护卫神·入侵防护系统

使用说明书

四川万象更新网络通信有限公司

目 录

第一部分 软件简介

1、主要功能

护卫神·入侵防护系统用于加强服务器信息安全，保护网站服务器、数据库服务器，防止黑客入侵带来的危害。

软件主要模块为：网页木马查杀、远程登录监控、系统用户监控、文件监控、进程限制、IIS 辅助功能、系统安全检测模块等。

2、技术特点

护卫神·入侵防护系统从应用层和驱动层，结合 WEB 网站，对黑客入侵的每一个渠道都进行过滤处理，更全面的保护服务器的安全。

3、适用对象

适用于有服务器信息安全需求的个人及企业事业单位。

第二部分 软件运行环境

1、硬件环境

护卫神·入侵防护系统最低支持如下硬件环境：

- CPU 为单核 1.6GHz 及以上
- 内存为 512MB 及以上
- 硬盘为 40G 及以上

注：配置越高性能越强。

2、软件环境

护卫神·入侵防护系统支持主流的 Windows Server + IIS 平台，包括：

Windows Server 2003 + IIS6.0
Windows Server 2008 + IIS7.0
Windows Server 2008 R2 + IIS7.5
Windows Server 2012 R2 + IIS8.5 等。

第三部分 软件的安装及卸载

1、软件安装

软件的下载：打开护卫神官方网站（http://www.huweishen.com），下载护卫神·入侵防护系统文件并解压缩，双击“护卫神·入侵防护系统 v3.2.0.exe”启动安装主界面后，安装开始：

A）护卫神·入侵防护系统安装向导启动，点击【下一步】开始安装：

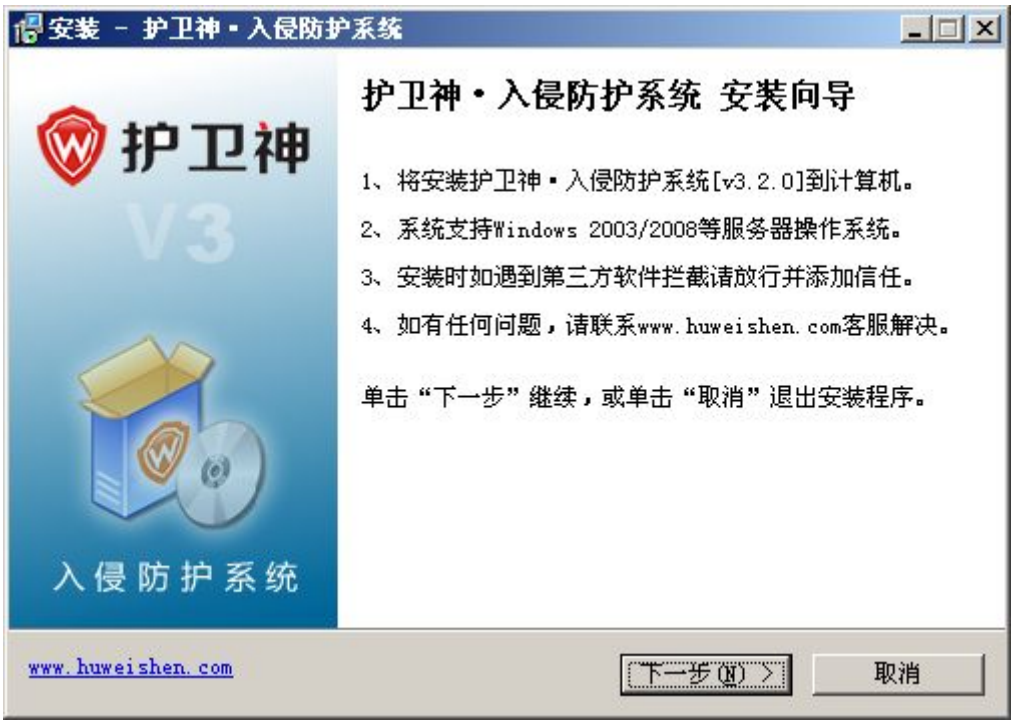

图 1 - 护卫神·入侵防护系统安装向导

B）许可协议，点击【下一步】继续：

图 2 - 护卫神·入侵防护系统安装许可协议

C）输入卸载密码：

图 3 - 护卫神·入侵防护系统输入卸载密码

说明：

卸载密码，为了防止黑客轻易将软件卸载而设计；安装时候如果设置了卸载密码，请牢记，卸载的时候会提示输入该密码，否则无法卸载。

D）选择安装目录，推荐默认目录，选择好后，点击【下一步】继续安装：

图 4 - 护卫神·入侵防护系统安装路径选择

E）安装完成，查看自述文件并启动系统：

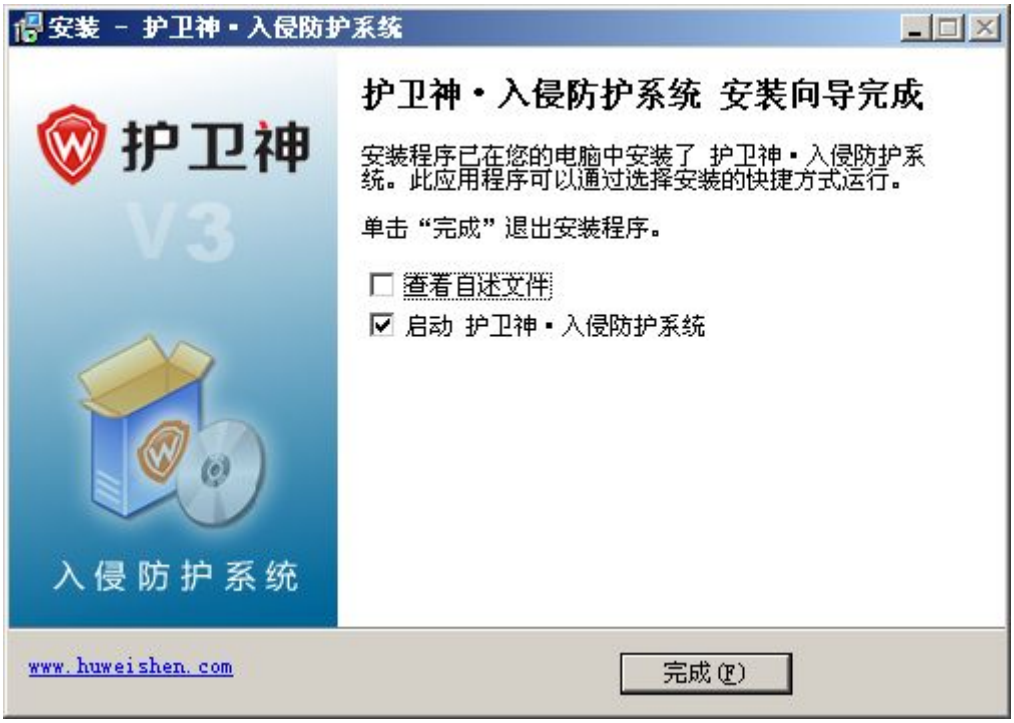

图 5 - 护卫神·入侵防护系统安装完成

说明：

1、点击【完成】按钮完成安装。

2、至此，护卫神·入侵防护系统安装完成。

注意：

1、默认情况下，安装程序会自动设置安装目录的权限，以确保系统能正常工作并生成日志。

2、安装完成后，系统会在桌面生成一个打开软件的快捷方式，每次运行双击打开即可，或者在开始菜单中打开也可。

3、安装后系统没有开启任何防护功能，需要用户在软件注册后设置开启。

2、软件卸载

卸载流程：

A）在操作系统中，点击开始菜单→所有程序→护卫神软件→入侵防护系统→卸载 护卫神·入侵防护系统，即开始卸载：

图 6 - 护卫神·入侵防护系统安装向导

B）如果安装时设置了卸载密码，需要在此输入卸载密码才能继续卸载：

图 7 - 护卫神·入侵防护系统卸载时要求输入卸载密码

C）弹出提示对话框，选择【是】:

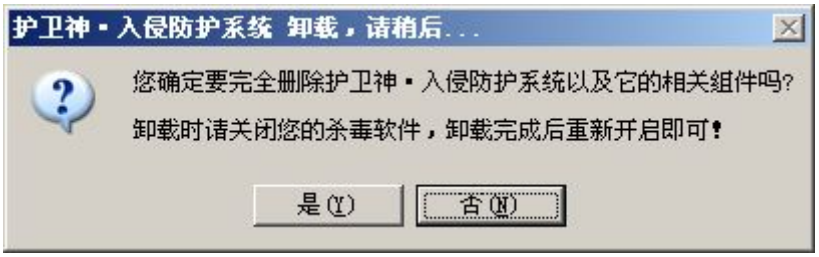

图 8 - 护卫神·入侵防护系统开始卸载确认框

D）系统会自动重新启动 IIS，完成卸载：

图 9 - 护卫神·入侵防护系统卸载完成提示框

E）至此，护卫神·入侵防护系统卸载完成。

注：出于安全角度，卸载时保留了隔离文件和日志文件，不需要的用户可以打开安装目录手动删除。

第四部分 软件注册

1、首次安装注册

第一次安装护卫神·入侵防护系统后，打开软件会提示输入注册信息，此时输入官方提供的软件账号和授权密码，即可完成注册：

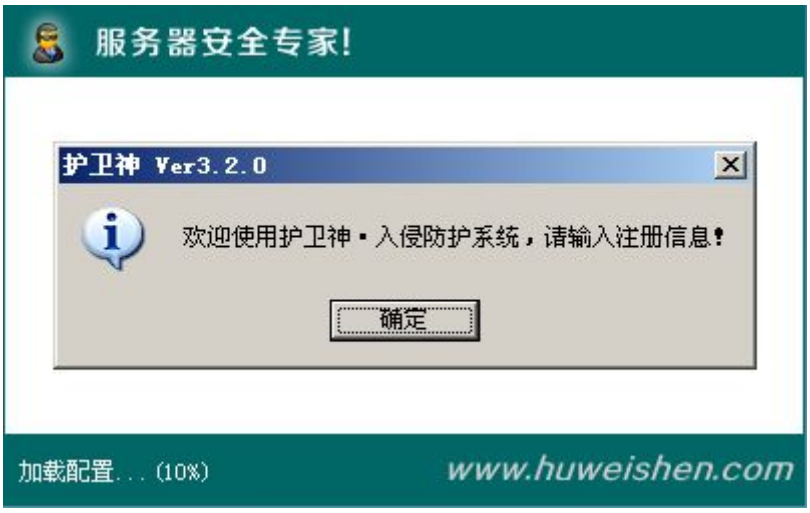

图 10 - 护卫神·入侵防护系统首次安装要求输入注册信息提示

输入软件授权账号和授权密码，完成注册：

图 11 - 护卫神·入侵防护系统输入授权账号和授权密码

2、注册后变更序列号

安装注册完成后，需要更换新的软件授权账号，请参见第三部分第一节系统设置的授权升级说明。

3、软件转移服务器

安装软件后，如果需要将软件转移到其他服务器上安装使用，则可以通过以下 3 种方式完成：

A）登录护卫神网站用户管理中心：

找到护卫神入侵防护系统对应的订单管理，点击按钮【调整为未启用】后，就可以在新的服务器上安装使用了。

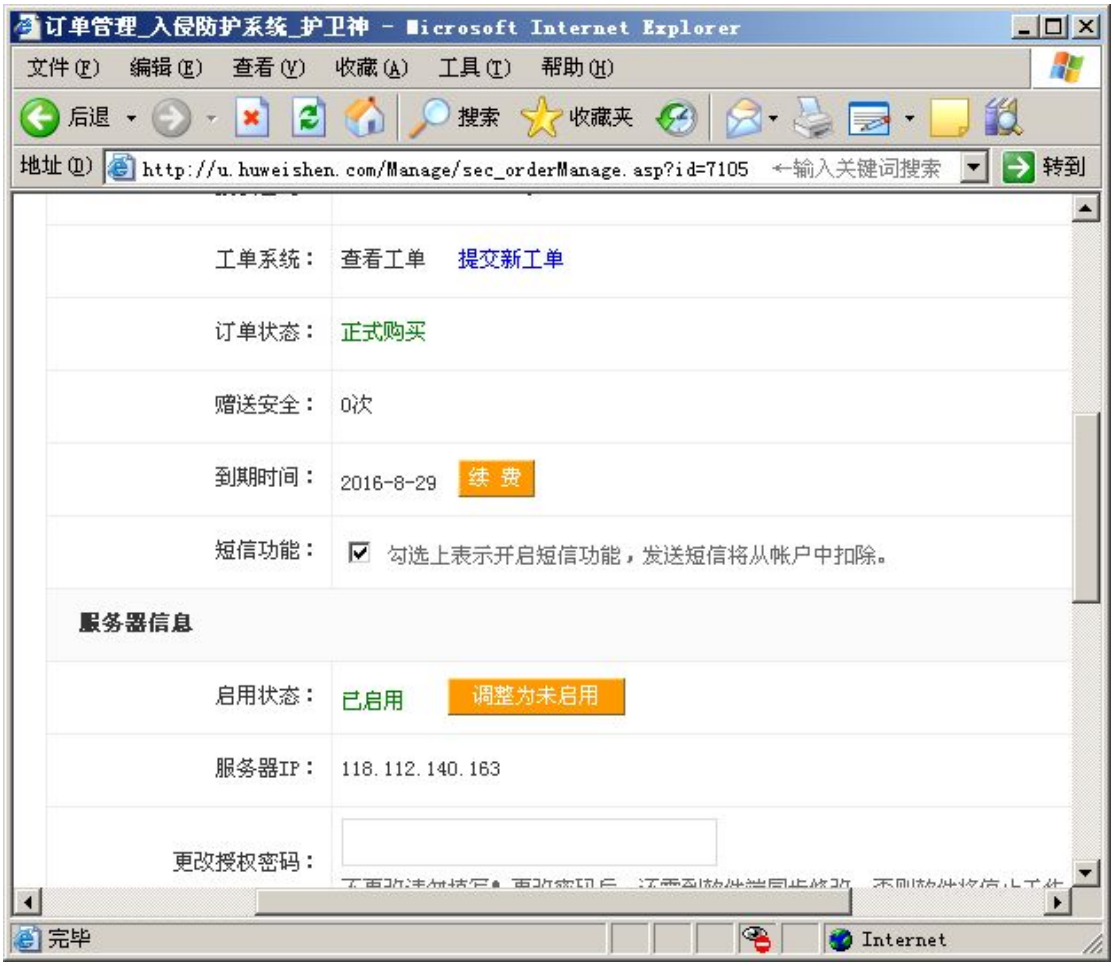

图 12 - 在护卫神网站管理中心设置软件为未启用示意图

B）登录软件独立控制面板：

登录如下网址，通过软件授权账户和授权密码登录，如图：

图 13 - 登录护卫神·入侵防护系统的独立控制面板

登录成功后，点击按钮【调整为未启用】，就可以在新的服务器上安装使用了，如下图：

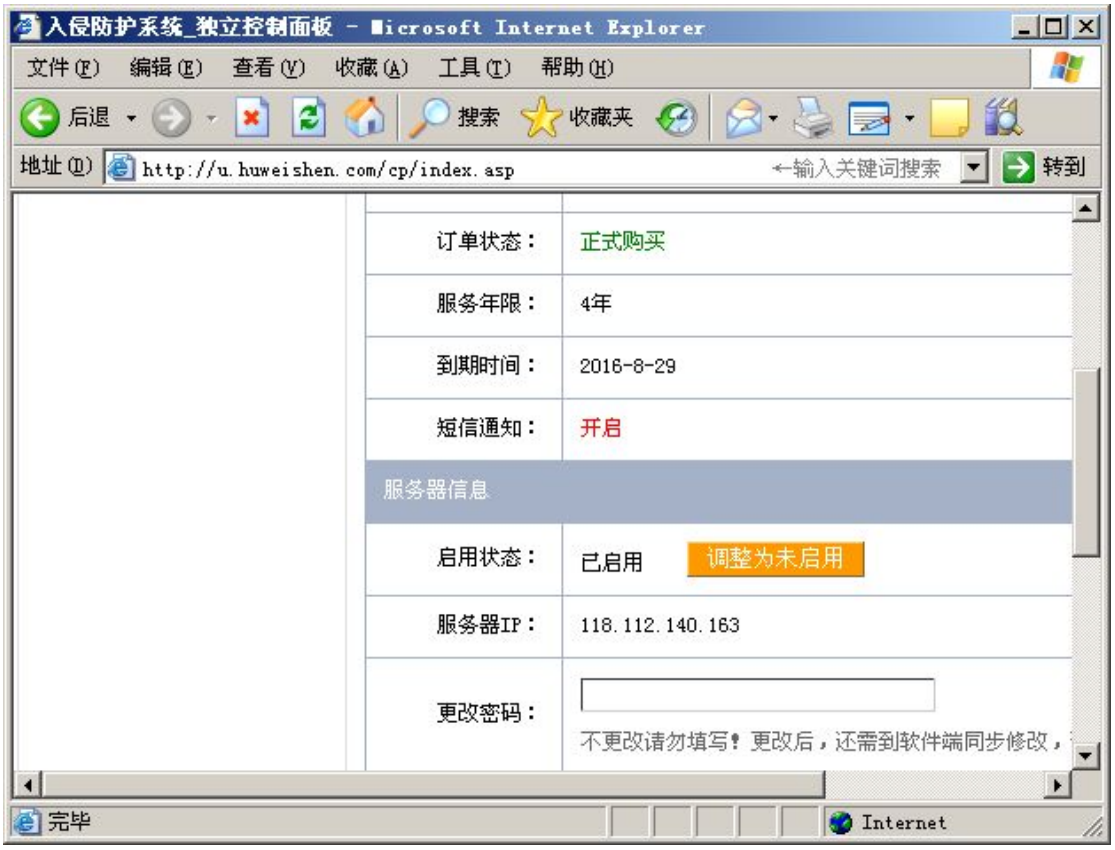

图 14 - 在护卫神独立控制面板设置软件为未启用示意图

C）通过 QQ 联系护卫神网站客服人员调整处理。

第五部分 功能设置

1、系统设置

（1）系统概况

软件注册后，打开护卫神·入侵防护系统，系统会自动定位到系统设置的系统概况页面，如图：

图 15 - 在护卫神·入侵防护系统软件主页面

说明：

这一栏总体显示软件功能的使用情况，如：软件的开启与关闭、是否显示托盘图标、重新启动护卫神等。

1、入侵防护系统运行中：表示系统已经开启，呈绿色；若显示入侵防护系统关闭中，呈红色，则表示系统已经关闭，关闭后所有功能均不生效。

2、开启显示托盘图标后，会在右下角托盘区显示护卫神·入侵防护系统的状态托盘，用于指示当前软件的状态。

：表示正常运行中且状态空闲；：表示系统正在执行任务。

3、鼠标放到托盘图标上，会有相应的状态提示，双击该图标将打开管理界面。

4、点击【木马查杀】，会启动网页木马查杀模块，自动对指定目录或所有网站目录的网页木马进行查杀，具体详见第四部分：木马查杀模块。

5、点击【安全检测】，会启动系统安全检测模块，用于检测当前服务器的基本安全状况，具体详见第

五部分：安全检测模块。

6、【重启软件】：重新启动护卫神·入侵防护系统服务程序，重新应用配置。

（2）系统管理

点击【系统设置】的【系统管理】选项卡，进入系统管理，如图：

图 16 - 在护卫神·入侵防护系统系统管理

说明：

这一栏主要设置软件打开密码，配置数据保存，是否开启自我保护等功能：

1、密码管理：设置好了管理密码之后，下次打开软件就需要输入这个密码才能进行正常管理操作，因此请牢记管理密码；

以下是设置管理密码之后，再次打开软件提示需要输入密码的界面：

图 17 - 打开软件要求输入软件密码

2、上传配置到官网：将目前的配置信息上传到护卫神管理中心，方便重装系统后直接下载软件配置信息。

3、下载配置到本地：将上次上传的配置信息下载到本地，如果之前没有上传配置，则下载不成功。另外，下载后，请检查下哪些配置不是自己需要的，注意更改。

4、查看配置文件备份：打开本地由系统自动备份的配置文件目录。

5、修复软件：如果系统工作异常，可以用修复软件功能进行修复。包括添加右键菜单、设置软件自身权限、设置 IIS 组件等。

6、开启系统自我保护：防止软件被人为破坏后自动恢复。

7、系统启动 5 分钟后启动内核：为了防止软件带来的异常导致服务器故障，在特殊情况下可以选中此项，正常情况无需选择，推荐不选。

8、不记录 Explorer.exe 内核操作日志：避免记录太多的资源管理器日志，因此推荐选中此项。

（3）短信设置

点击【系统设置】的【短信设置】选项卡，进入短信设置，如图：

图 18 - 短信设置模块截图

说明：

1、开启短信发送：要使用短信功能，需要先选中此项才能开启。

2、设置对应的手机号码，系统可以将您关心的事件第一时间发送到您的手机上，若有多个手机需要接收短信，请用“|”分隔多个手机号码。

3、通道检查：设置好手机之后，点击【通道检查】，则会发送一条测试短信到指定手机，如果收到短信，表名通道正常。

4、接收选项：可以设置 4 项关心的内容：在用户远程登录成功时发送、在用户远程登录失败时发送、在拦截创建用户时发送、在发现网页木马时发送，用户可以根据情况选择。

5、发送频率，最多不超过 N 分钟发送一条（软件重启后将会重新开始计时），避免短信太多，最低设置为 3。

6、屏蔽的字符串：如果短信中包含了这些字符串，将不会发送该短信，以便用户屏蔽不想接收的短

信。

注：短信通道采用第三方通道，有时可能稍微有一些延迟属正常。

下图为手机收到的取消账户 aspx 提权为 Administrators 组时被护卫神 •入侵防护系统拦截的提示短信：

图 19 - 收到的入侵拦截短信截图

（4）授权升级

点击【系统设置】的【授权升级】选项卡，进入授权升级，如图：

图 20 - 授权升级模块截图

说明：

1、软件授权账户：显示当前软件正在使用的授权序列号。

2、软件授权密码：当前软件正在使用的授权密码（*不显示）。

3、更换授权：如果需要更换序列号，可以将新序列号和授权密码输入，然后点击【更换授权】按钮，即可在该服务器上使用新的授权序列号和授权密码。

4、升级检查：检查获取当前软件是否有新版发布。

5、下载软件：打开护卫神·入侵防护系统软件下载网页，下载软件。

6、保存设置：保存软件账户和授权密码。

7、用户管理中心登录：打开护卫神用户管理中心网页，可以用会员账号和密码登录管理。

8、独立控制面板登录：打开护卫神·入侵防护系统软件管理页面，可以用软件授权账户和授权密码登录管理软件。

（5）在线服务

点击【系统设置】的【在线服务】选项卡，打开在线服务，如图：

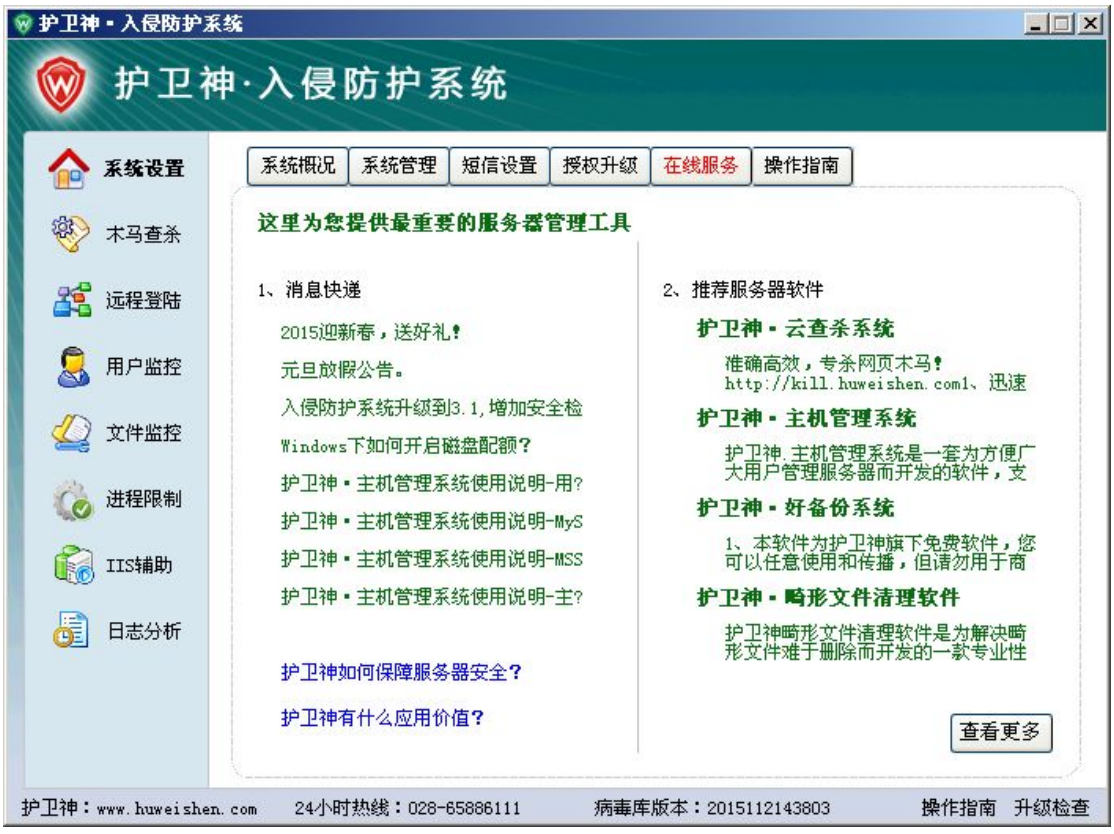

图 21 - 在线服务模块截图

说明：

在线服务：主要提供一些官方最新动态以及推荐的服务器相关软件，点击对应链接即可打开对应网页。

（6）操作指南

操作指南：点击链接到护卫神管理中心网络帮助文档： http://www.huweishen.com/help/tutorial，方便用户更好的使用软件。

2、木马查杀

点击左侧【木马查杀】菜单，进入木马查杀模块。该模块主要实时监控网页文件一举一动，发现木马文件立即处理。

（1）实时监控

进入木马查杀模块，默认显示实时监控画面，如图：

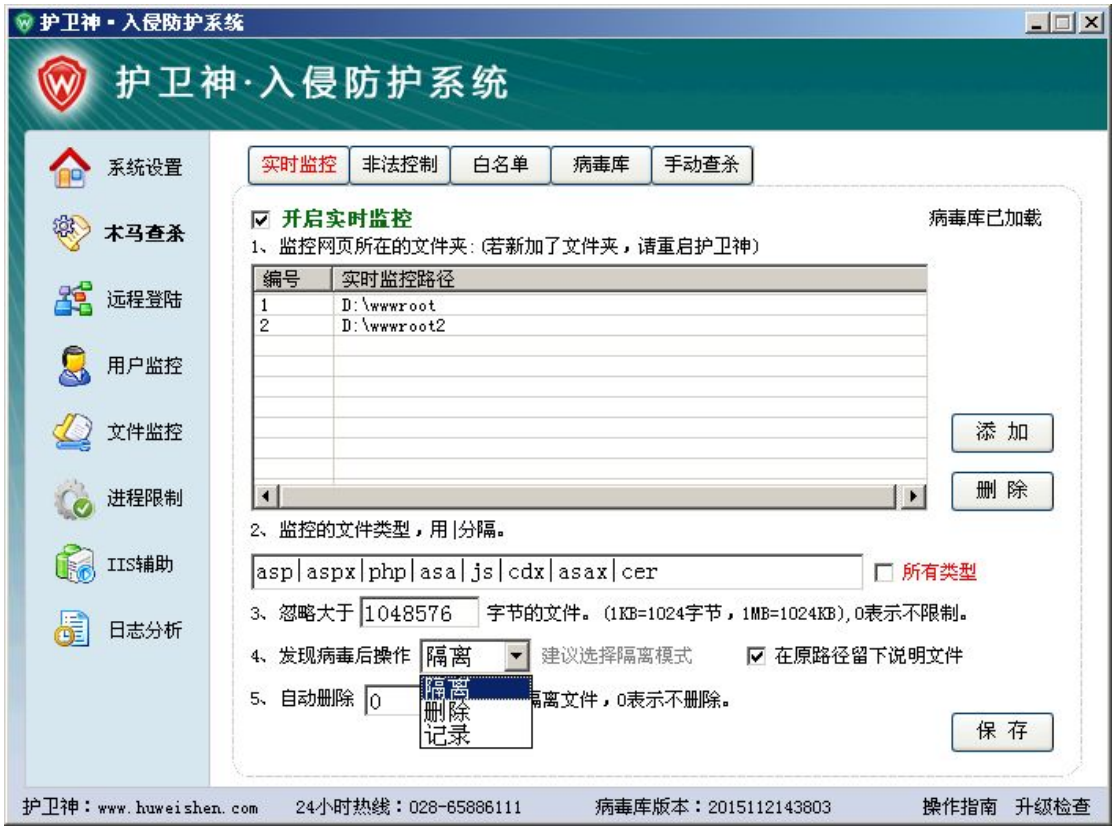

图 22 - 实时监控模块截图

说明：

1、开启实时监控：选中后，该模块功能有效，不选择则无效。

2、监控网页所在的文件夹列表：一般选择网页所在的文件夹。如果该文件夹包含了子目录，那么，只需要选择父目录即可，不需要逐个选择子目录。支持鼠标拖放，不建议设置太多的路径。

3、监控的文件类型：一般设置动态网页脚本文件即可，如：asp|aspx|php|asa| js|cdx|asax|cer 等，用中竖线“|”分隔多种类型，如果不限类型，请选择【所有类型】复选框。

4、忽略最大文件：如果某些文件太大，则对其进行忽略，目的是避免处理单个大文件造成 CPU 消耗过高。

5、发现病毒后操作：分为 隔离、删除、记录 三种。

(1)隔离：将木马文件隔离到系统目录，方便后期找回复原操作，推荐选择此方式；

(2)删除：将木马直接删除掉，注意此方式不能从回收站回收；

(3)记录：只对木马文件进行记录，不进行任何处理，木马依旧可以产生危害。

6、在源路径留下说明文件：此项，在发现木马文件的目录，留下“文件名”+ “.log”命名的文件，记录被隔离的原因，方便最终用户查找原因，可根据情况采用。

7、自动删除隔离文件：避免隔离文件太多占用磁盘空间，可以设置自动删除。0 表示不限制。建议 60 天（2 个月）以上。注意隔离文件删除后，就无法找回被删除的隔离文件了。

注意：如果增加或删除了监控目录，请点击【重启软件】才能生效。

（2）非法控制

点击【木马查杀】的【非法控制】选项卡，进入非法控制模块；该功能可以根据非法词库，拦截批量

生成指定文件类型的垃圾文件，如图：

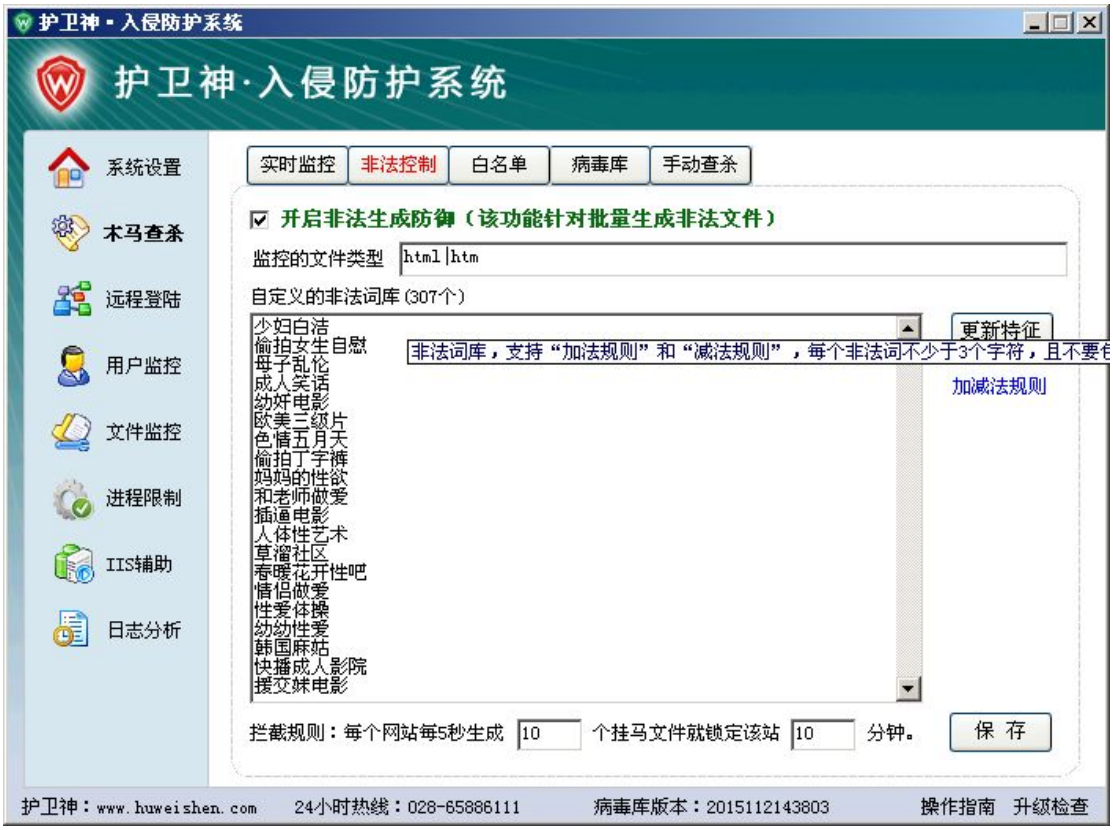

图 23 - 非法控制模块截图

说明：

1、开启非法生成防御：选中表示开启，不选中表示关闭此功能。

2、监控的文件类型：一般非法批量生成，都是生成 .html 和.htm 静态网页文件，因此通常只需要设置这 2 种文件类型即可。

3、自定义的非法词库：可以自行设置自认为需要判断的敏感词汇，支持“加减法规则”，加减法规则参见附录。

4、更新特征：可以从护卫神官方获取内置非法词库特征码。

5、拦截规则：根据自身情况设置，默认每个网站每 5 秒生成 10 个挂马文件，则锁定该站 10 分钟不能写入任何监控类型的文件。

（3）白名单

点击【木马查杀】的【白名单】选项卡，进入白名单页面；该部分主要设置在木马查杀中例外的目录和文件内容，如图：

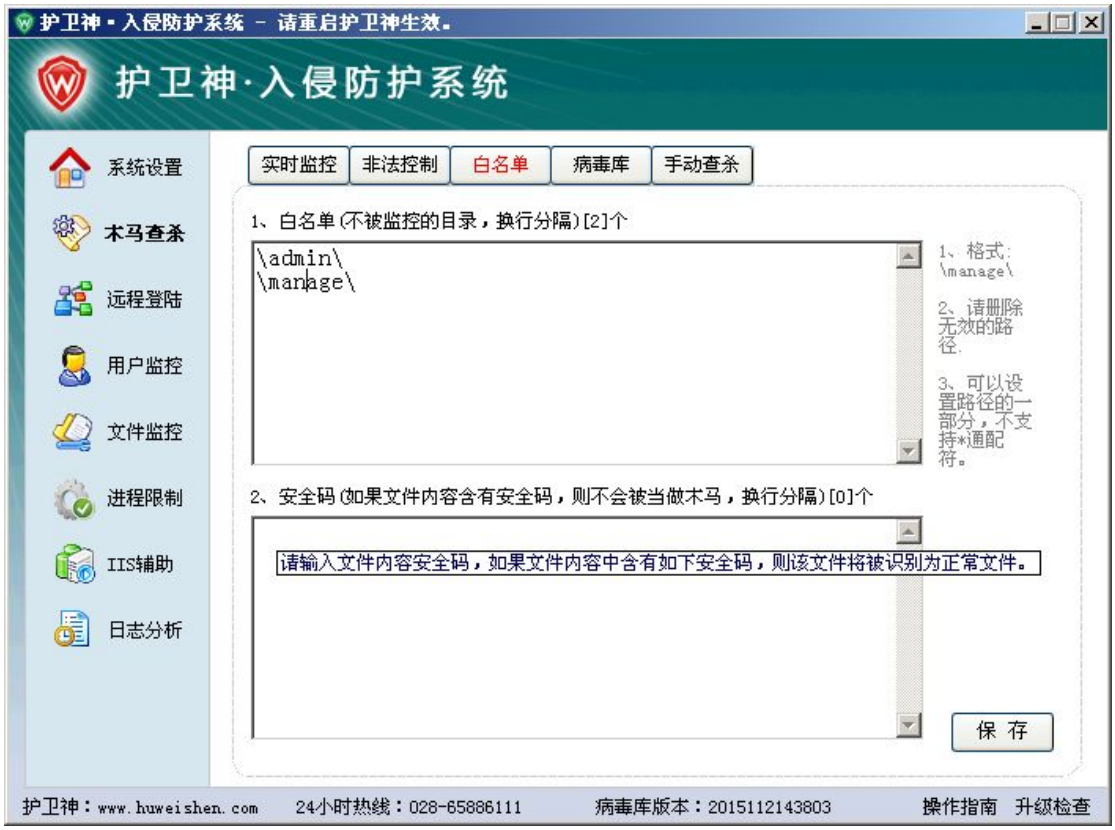

图 24 - 白名单模块截图

说明：

1、白名单：信任的目录，比如某些特殊非木马文件，会被护卫神误杀，就可以将文件路径的全部或部分设置到白名单。格式是 Windows 资源管理器路径格式，多个请换行分隔。

2、安全码：如果某些文件确认正常，但是被护卫神隔离，那么就可以提取该文件部分内容，作为安全码，那么护卫神将不再对其隔离处理。

（4）病毒库

点击【木马查杀】的【病毒库】选项卡，进入病毒库页面；该部分主要管理护卫神 • 入侵防护系统内置和自定义的木马特征，如图：

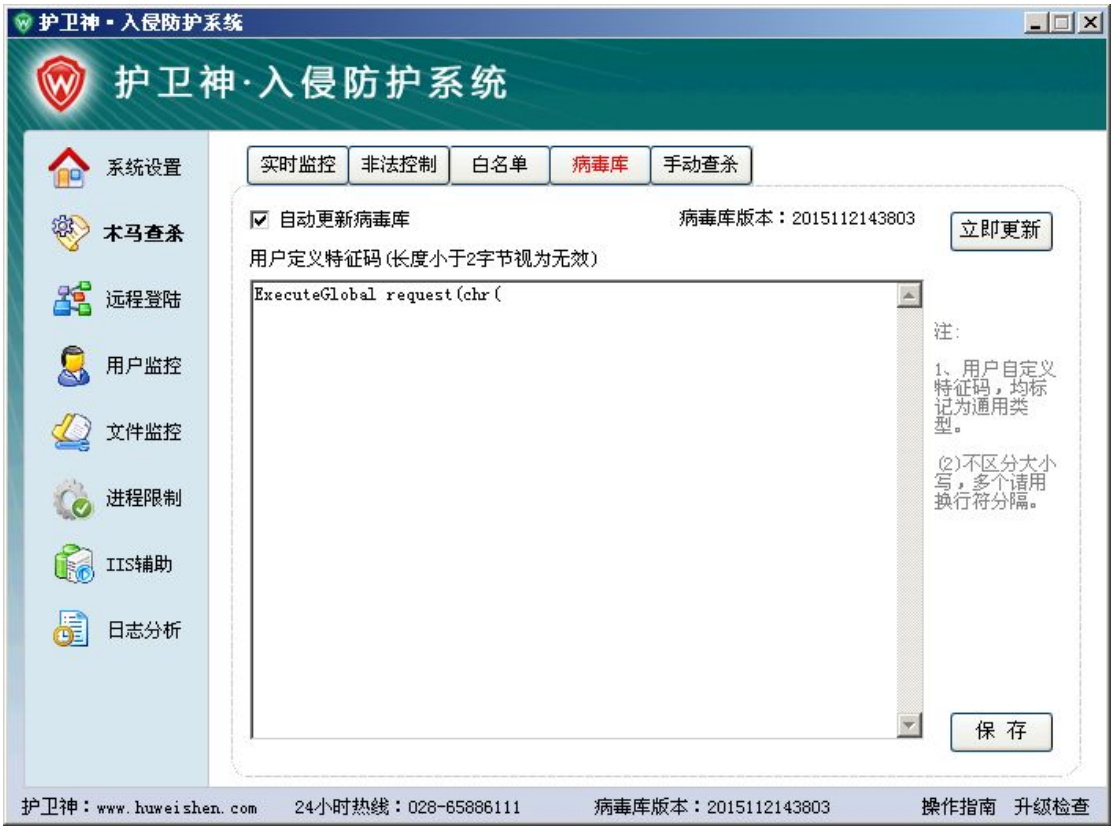

图 25 - 病毒库模块截图

说明：

1、自动更新病毒库：选择后，系统会定期查询病毒库是否有更新，如果有更新，就会自动下载到本地，保障了对新木马的及时识别，建议选择。

2、用户定义特征码：如果用户不希望包含某些内容的文件出现，那么可以设置特征码，设置了之后，系统会将含有特征码的文件识别为网页木马并进行处理，注意不要低于 2 个字节。

3、【立即更新】病毒库，立即从护卫神官方更新病毒库，以便查杀最新木马文件。

4、【保存】：保存当前设置的规则。

（5）手动查杀

关于手动查杀模块，请参见第四部分 木马查杀模块。

3、远程登录

该部分功能，通过终端计算机名或终端 IP 地址，以及登录使用的服务器账户，验证远程桌面终端的登录信息，只有通过认证的终端设备才能连接上服务器，保障服务器远程桌面安全。

（1）远程登录设置

1、计算机名认证

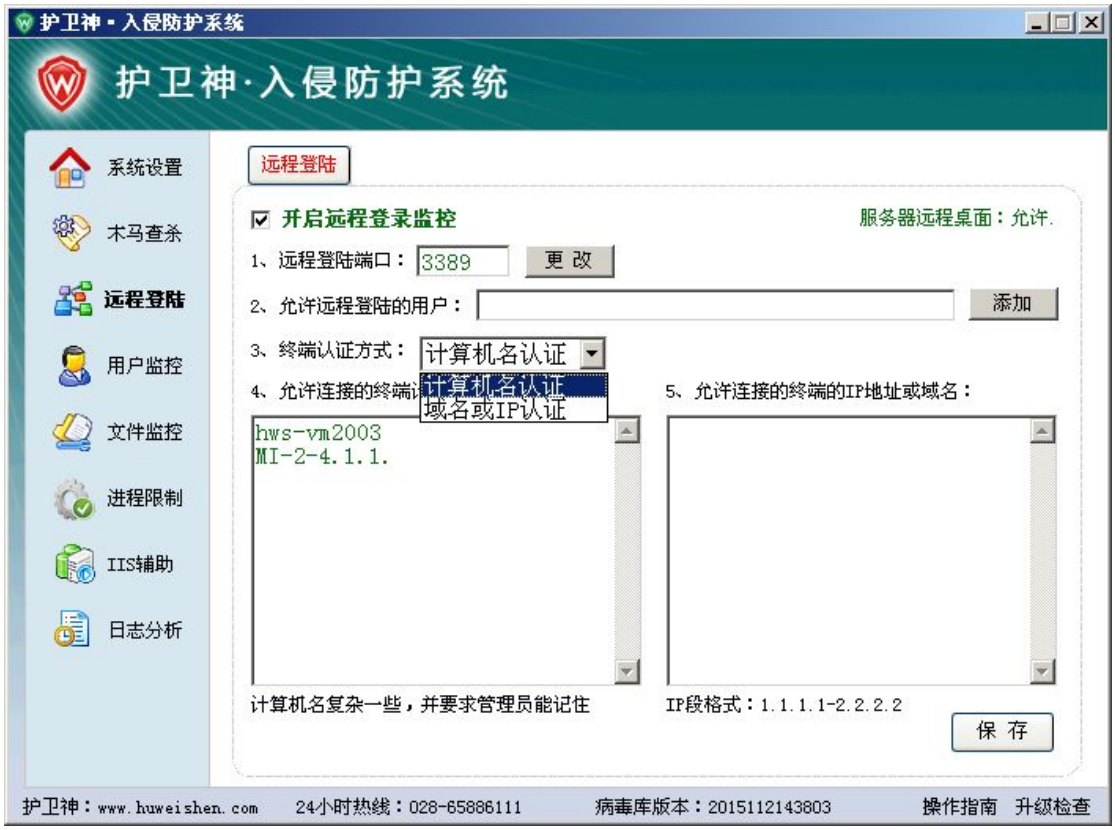

图 26 - 远程登录模块设置计算机名认证截图

2、域名或 IP 认证

图 27 - 远程登录模块设置域名或 IP 认证截图

说明：

1、远程登录端口：默认 3389，可以通过旁边的按钮【更改】为一个您想要的端口，更改后，能相对默认的 3389 较安全，建议更改，更改后需要牢记新端口。

2、允许远程登录的用户：指定服务器已经存在的用户，点击【添加】将默认添加管理员组用户。只有在该用户列表中的用户才有远程登录服务器的权限，否则将会被拦截，不设置表示不限制用户名。（注：该功能可以解决因为提权而导致的用户被远程。）

3、注意：如果需要修改管理员用户名，则需要先在这里添加上新的管理员名， 然后再修改，避免被拦截在远程桌面外。

4、终端认证方式：

(1)计算机名认证：假设您拥有 1 台电脑 A，1 台服务器 B，通过 A 对 B 进行远程管理，B 安装有护卫神，那么，就需要将 A 的计算机名输入到 B 的护卫神允许远程的计算机名中，可以换行分隔输入多个，设置后，只有终端计算机名在该列中的，才能对 B 进行远程管理，其他终端计算机名的计算机将会被拦截。

注意：1、必须是 A 的计算机名；2、您需要记住 A 的计算机名，否则如果 A 重装了系统忘记了计算机名，就会无法远程管理；3、建议设置多个终端名，但是不要设置太简短避免被猜测；4、如果机房需要管理，则需要添加机房管理的终端名；5、计算机名，请限制在 15 个字节以内。

(2)域名或 IP 认证：如果您拥有固定的 IP，您也可以采用 IP 或者域名的方式进行管理。

假设您拥有 1 台电脑 A，1 台服务器 B，B 安装有护卫神，则您需要将 A 的公网 IP 添加到 B 的护卫神的 IP 名单中，那么 A 就可以对 B 进行远程管理，其他 IP 的计算机均会被拦截。

您也可以用域名，用域名的原理：该域名在服务器上 ping 得的 IP，即为可信的终端 IP，因此，您可以搭配域名解析系统，如一些域名智能解析系统等。

注意：1、域名和 IP 可以混用；2、IP 段格式：1.1.1.1-1.1.1.255，闭区间，中间由中划线连接。

（2）拦截效果

1、设置允许终端连接的计算机名，在此列的终端计算机可以正常连接，除此之外的都被拦截，被拦截的示意图如下：

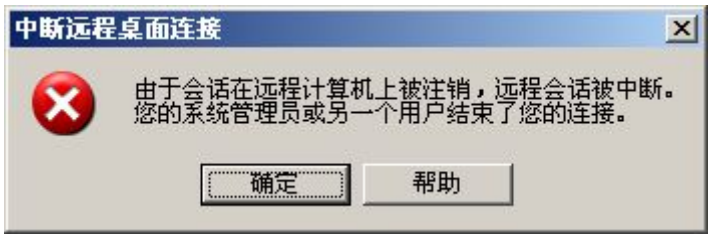

图 28 - 远程桌面被拦截效果图

2、设置 IP 段拦截效果与上图类似。

3、拦截日志：

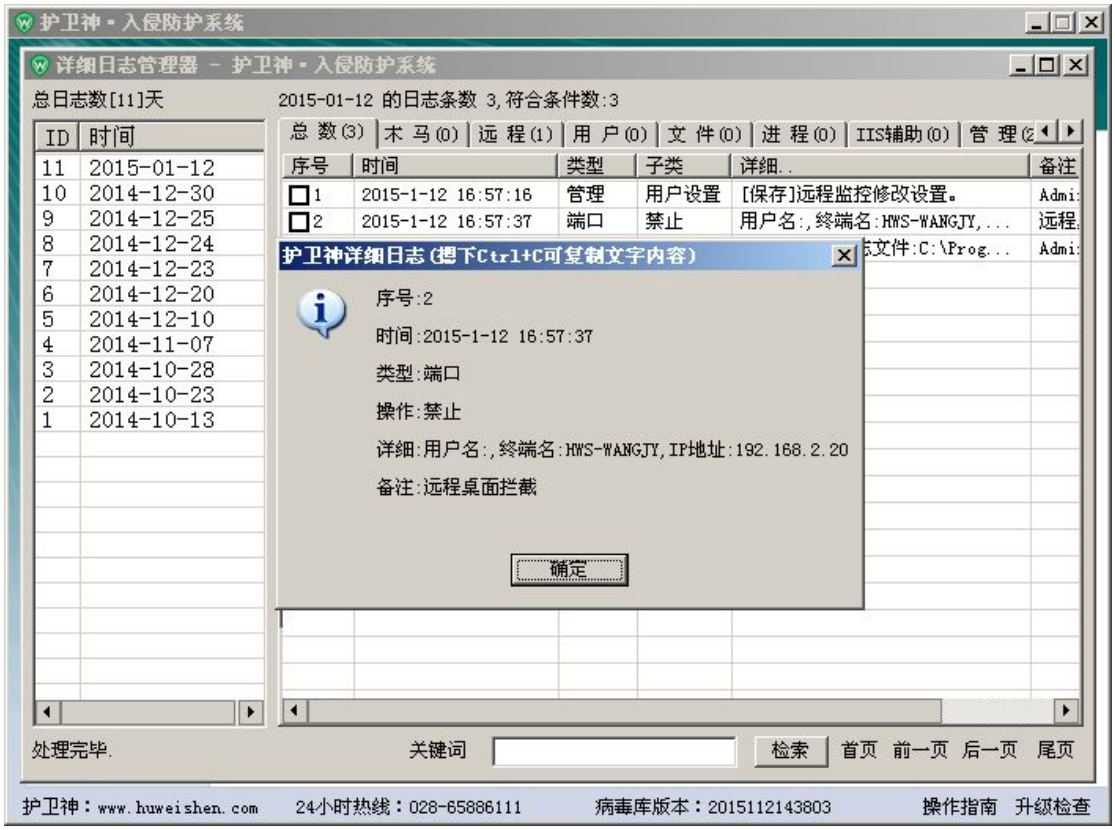

图 29 - 远程桌面拦截日志截图

说明：

日志中记录了详细的终端信息，包括终端计算机名，终端 IP 地址，方便查找来源。

4、用户监控

点击左侧【用户监控】按钮，即可进入用户监控模块；该部分主要监控服务器上的系统用户（账户），防止提权，及时发现处理克隆账户等。

（1）用户监控设置

进入用户监控，如下图：

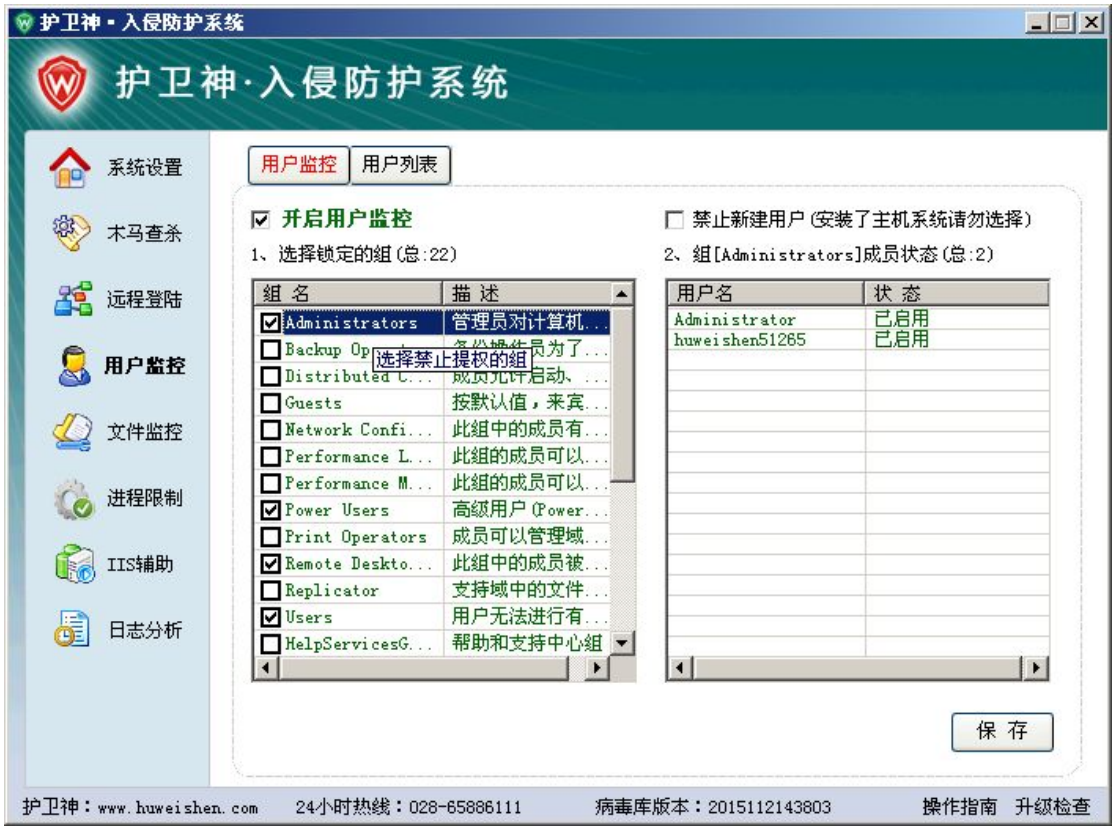

图 30 - 用户监控模块截图

说明：

1、开启用户监控：用户监控模块功能开关，选中表示开启，不选中表示不开启。

2、选择锁定的组：选定的组，将会禁止增加新用户，如果有用户往该组提权，将失败。一般选中权限最高的组，如 Administrators、Power Users、Remote Desktop 等即可。

3、禁止新建用户：选中后，新建用户将失败。注意：虚拟主机系统会自动创建新用户，选择会导致开设网站失败，因此虚拟主机用户请勿勾选此项。

（2）拦截效果

1、选中禁止新建用户：选中后，手动新建用户，提示如图：

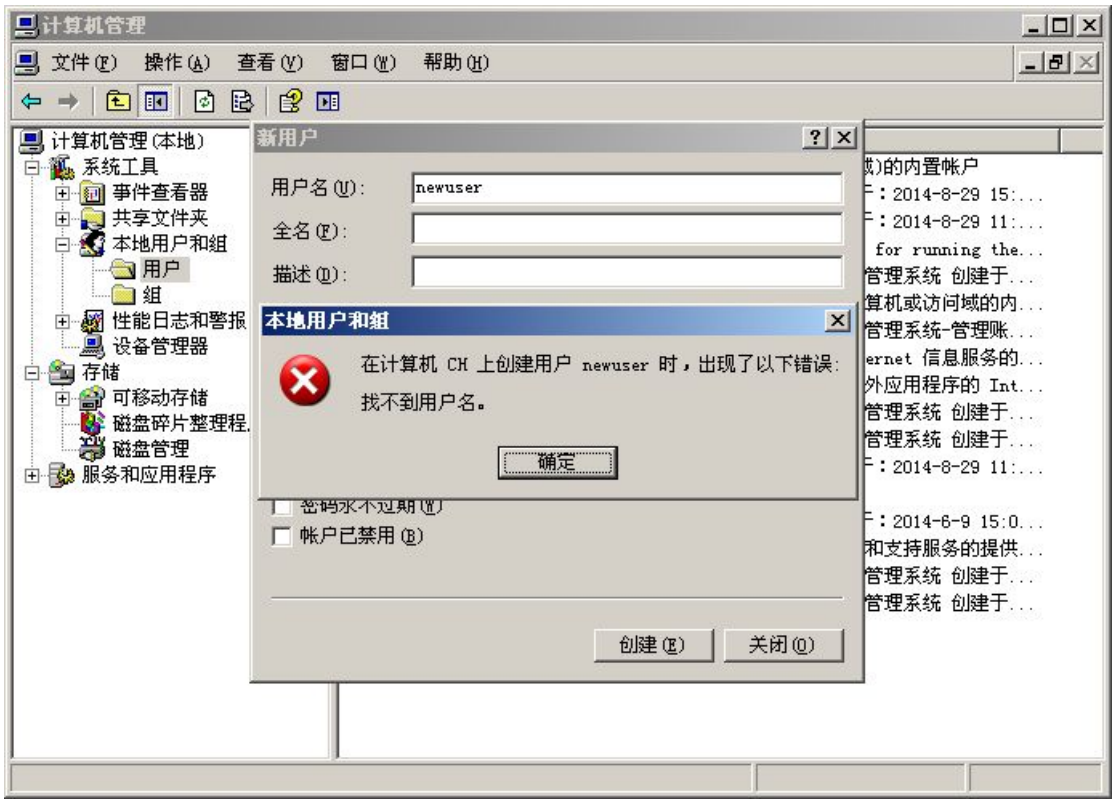

图 31 - 用户监控模块拦截用户创建效果截图

2、锁定组功能：假设选中 Administrators 组，如果将本来不属于这个组的用户，修改到隶属于该组，那么立刻会被护卫神取消权限。

3、如果您设置了短信提醒，那么您将立刻收到拦截账户的短信通知。

（3）拦截日志

1、以上操作的拦截日志如图：

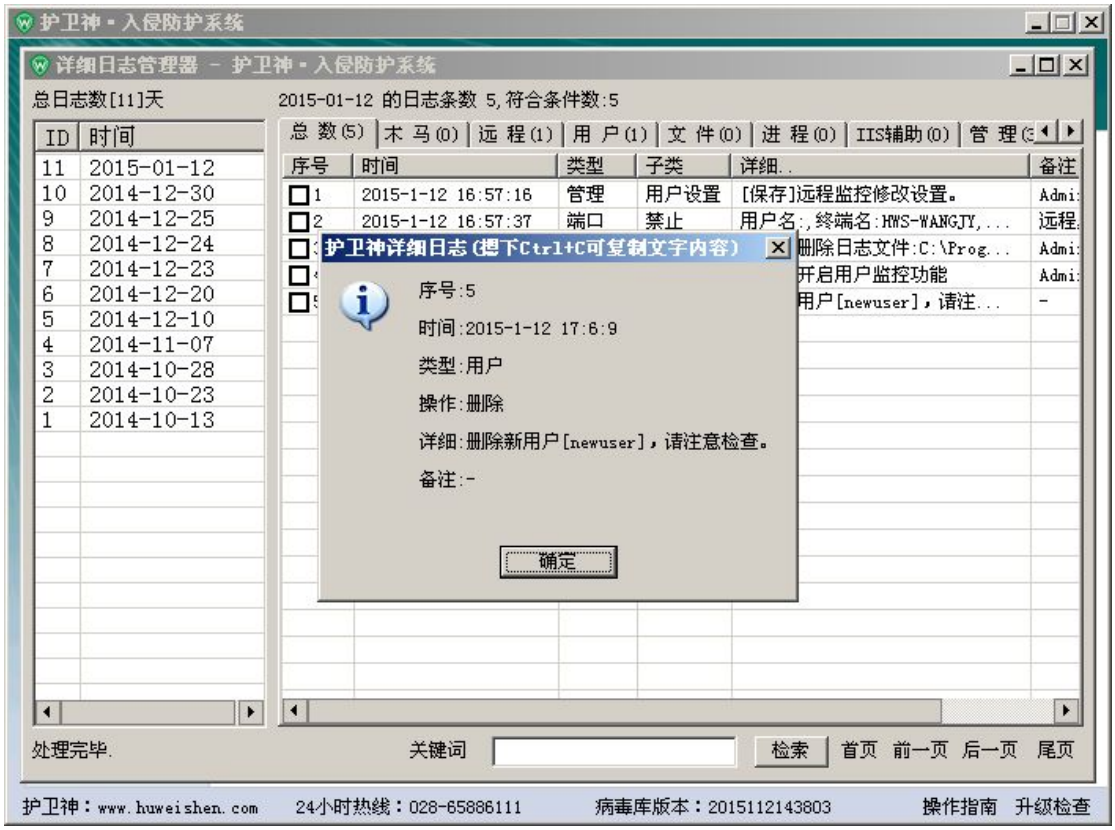

图 32 - 用户监控模块拦截用户创建日志截图

（4）用户列表

点击【用户监控】的【用户列表】选项卡，进入用户列表：

A）没有克隆账户，整个列表显示绿色：

图 33 - 用户列表模块截图

B）发现克隆账户后，护卫神 • 入侵防护系统会给出提示信息，并且整个列表显示红色，提醒用户：

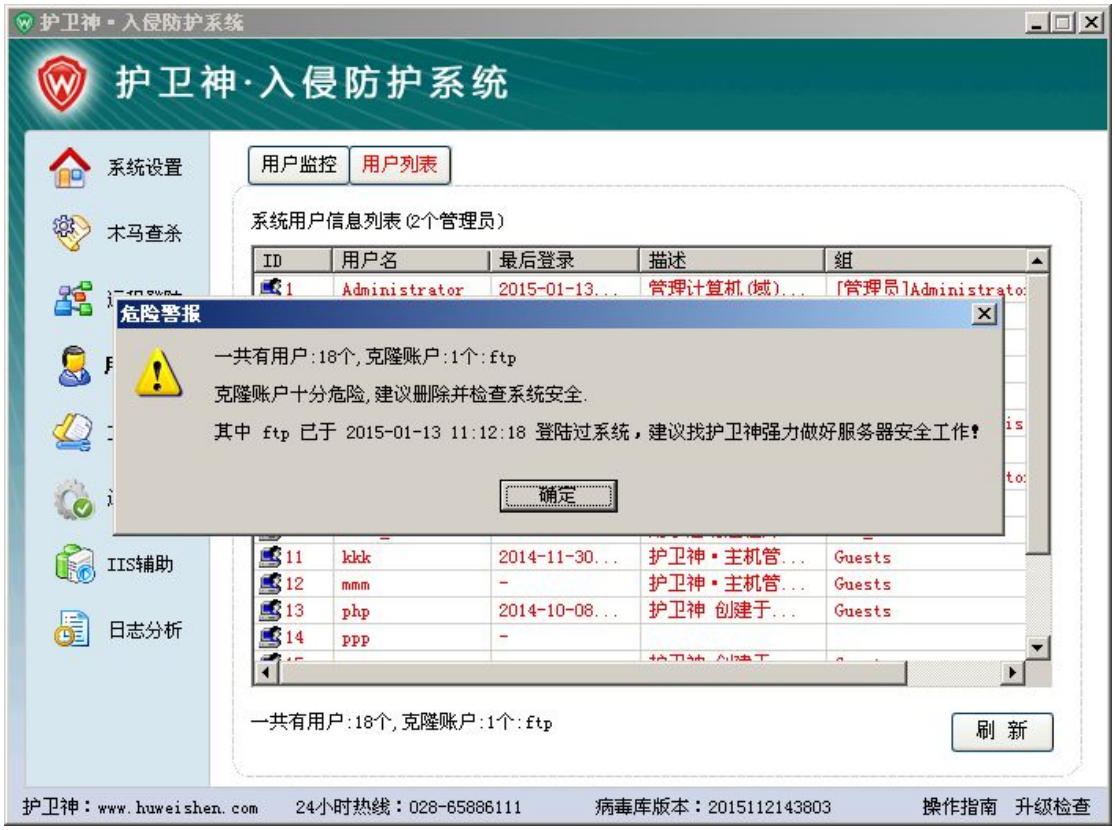

图 34 - 用户列表模块发现克隆账户提示截图

说明：

1、如果发现有克隆账户，表示服务器很可能被入侵了，管理员需要严格注意。

2、安装了护卫神·入侵防护系统之后，会自动检测克隆账户的创建，一旦有，则会立即删除并记录日志。

5、文件监控

点击左侧【文件监控】按钮，进入文件监控部分；该部分用于实时监控指定目录的文件，如防篡改、禁止执行、禁止生成畸形文件等。

（1）文件监控设置

文件监控界面如图：

图 35 - 文件监控模块截图

说明：

1、开启文件监控：选中即开启该功能。

2、点击右边按钮【新增】，或直接鼠标点击文件夹拖放进来，即加入新的监控路径。

3、点击右边按钮【修改】，或双击某项，则可以对该文件夹监控规则进行设置。

4、点击右边按钮【删除】，即删除对某个选中文件夹的监控。

5、如果监控路径有变化，则需要重新启动护卫神·入侵防护系统才能生效。

（2）文件监控常规设置

点击【新增】或【修改】按钮，默认进入文件监控详细常规设置画面：

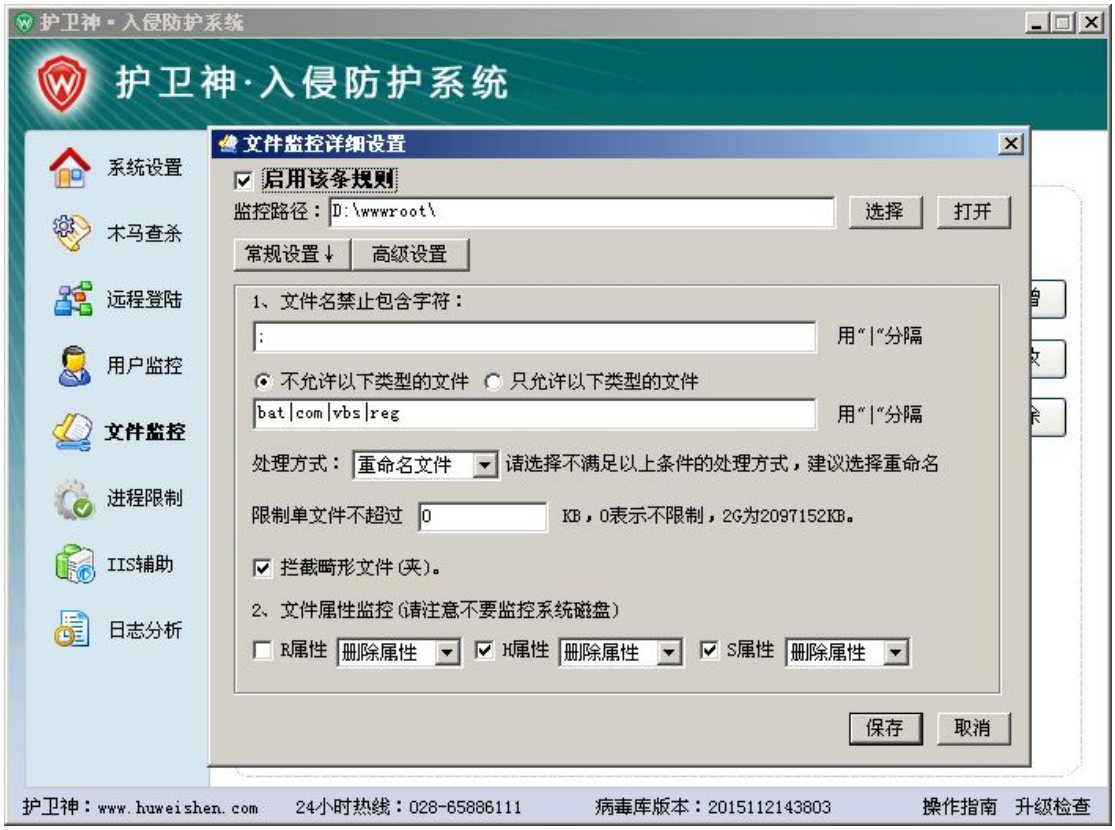

图 36 - 文件监控常规设置截图

说明：

1、启用该条规则：选择表示该条规则有效，不选表示无效。

2、监控路径：选择设置需要监控的目录，一般只需要设置网站文件所在目录。

3、文件名禁止包含的字符：如果文件(夹)名包含设置的字符，则系统自动进行处理，如分号“;”，很多 asp 文件利用 IIS 漏洞逃避检测并隐藏破坏。系统默认分号，不需要可以删除。

4、不允许/只允许 以下类型的文件：一般在网站中不会出现：vbs|bat|com|reg 等危险文件，如果不禁止则很危险，需要禁止该类文件。

5、处理方式：分为重命名和删除。重命名后，该文件类型将会失效，达到屏蔽危险的作用。一般选择重命名，如果删除，则不会经过回收站。

6、自动清理畸形文件：畸形文件，包括所谓的带点目录，小强文件，特殊文件名等，这类文件使用了 Windows 内部控制字符，导致在资源管理器中无法直接删除。选中此项后，护卫神会为您自动删除该类文件而不遗漏（建议在安装后手动扫描一次）。

7、文件属性监控：文件属性，分为三种，分别为：只读(R)、隐藏(H)、系统(S)，一般网页文件中应该禁止出现隐藏和系统属性的文件，建议用户选择让其原形毕露。

（3）文件监控高级设置

点击【高级设置】按钮，进入文件监控高级设置画面，如图：

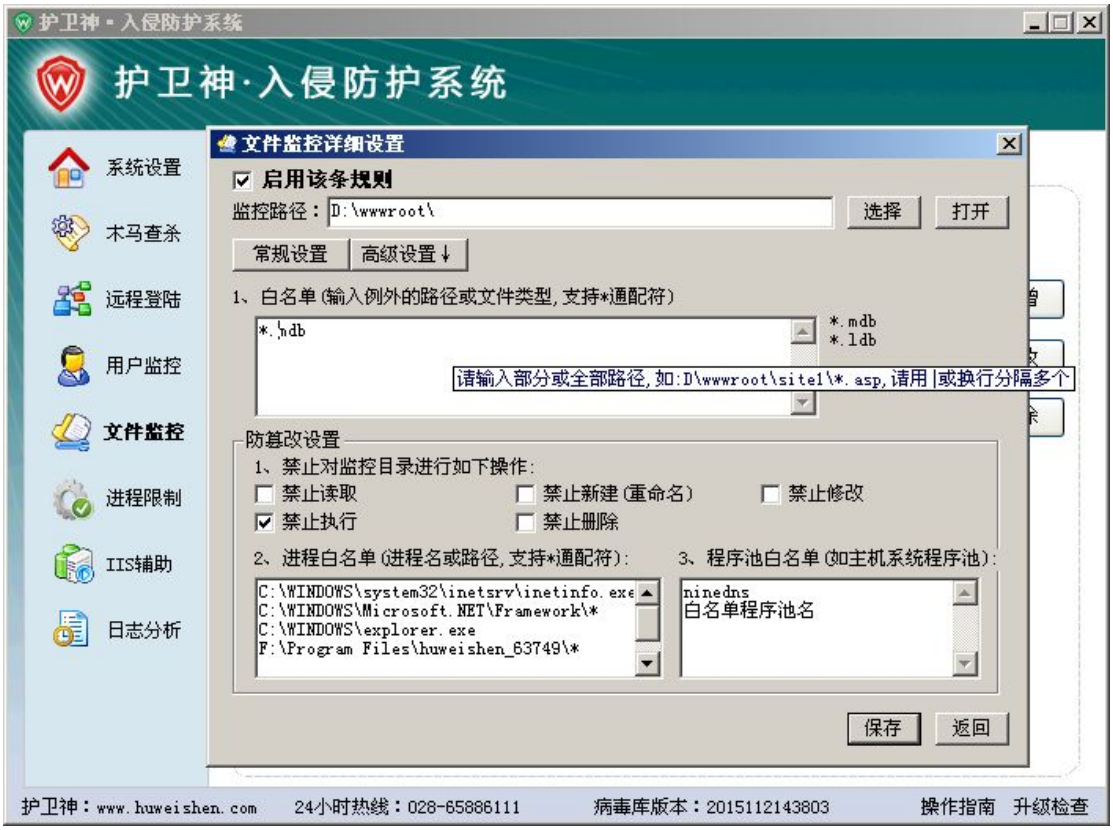

图 37 - 文件监控高级设置截图

说明：

1、白名单：监控目录下的部分目录或文件如果不需要监控，则设置到白名单即可。注意是这个路径的全部或部分目录，支持*通配符。多个请用换行分隔。

2、防篡改设置：

A）禁止读取：禁止除白名单外的进程读取监控目录下的文件。

B）禁止新建（重命名）：禁止除白名单外的进程新建/重命名监控目录下的文件。

C）禁止修改：禁止除白名单外的进程修改监控目录下的文件内容。

D）禁止执行：禁止除白名单外的进程执行监控目录下的文件。

E）禁止删除：禁止除白名单外的进程删除监控目录下的文件。

3、进程白名单：如果进程路径在白名单中，将不会受到防篡改设置的限制。

4、程序池白名单：例外的程序池，一般填写主机管理系统的程序池名。

（4）防篡改拦截效果

1、禁止读取的效果：

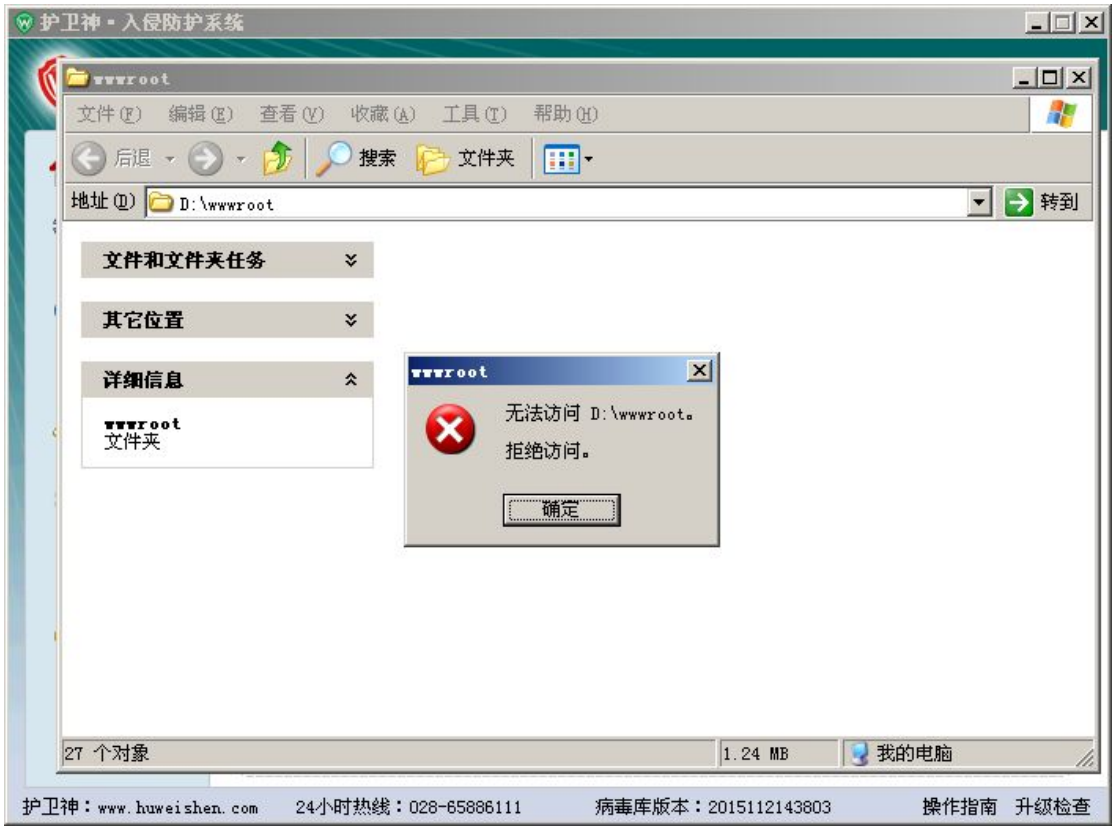

图 38 - 禁止读取拦截效果截图

2、禁止新建（重命名）的效果：

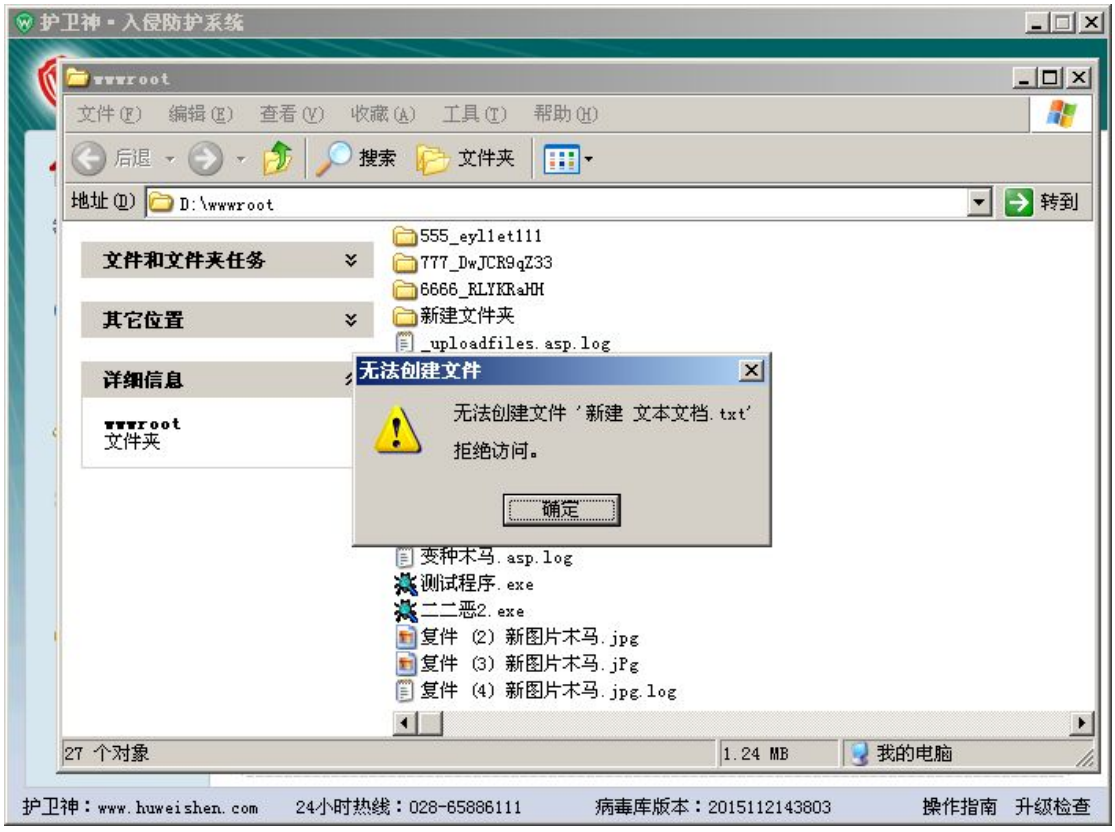

图 39 - 禁止创建文件拦截效果截图

3、禁止修改的效果：

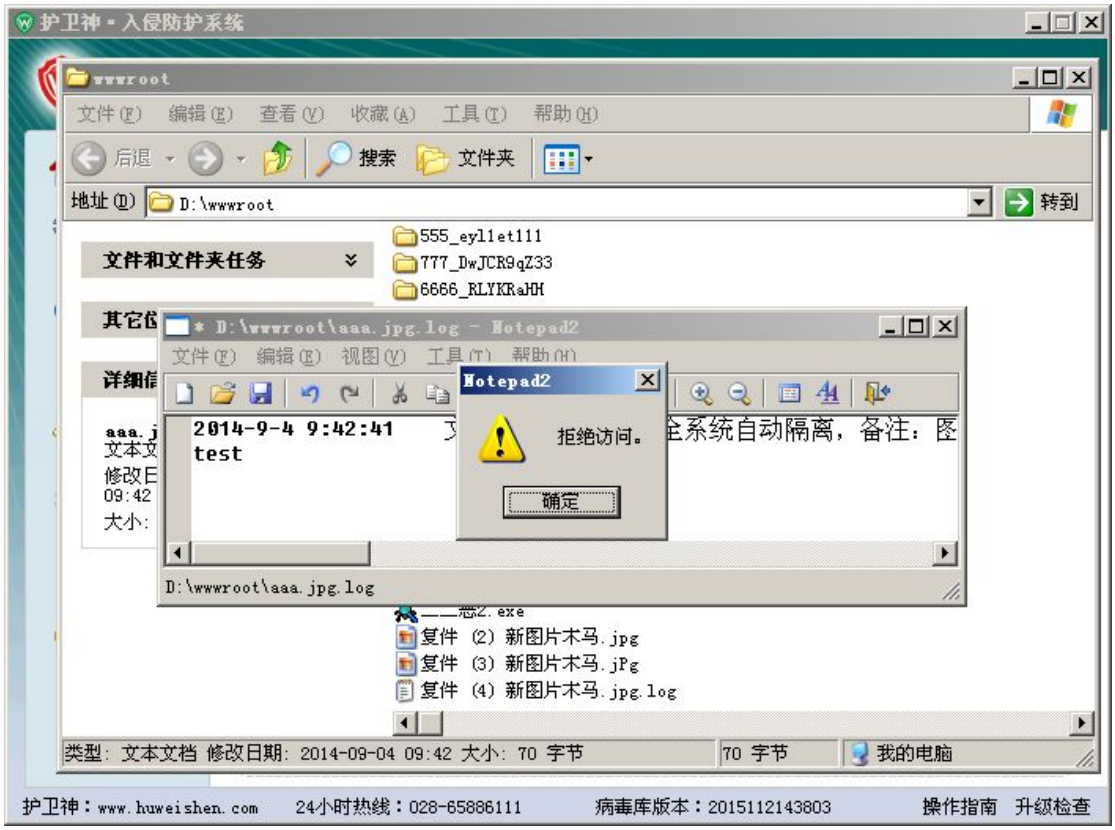

图 40 - 禁止修改文件拦截效果截图

4、禁止执行的效果：

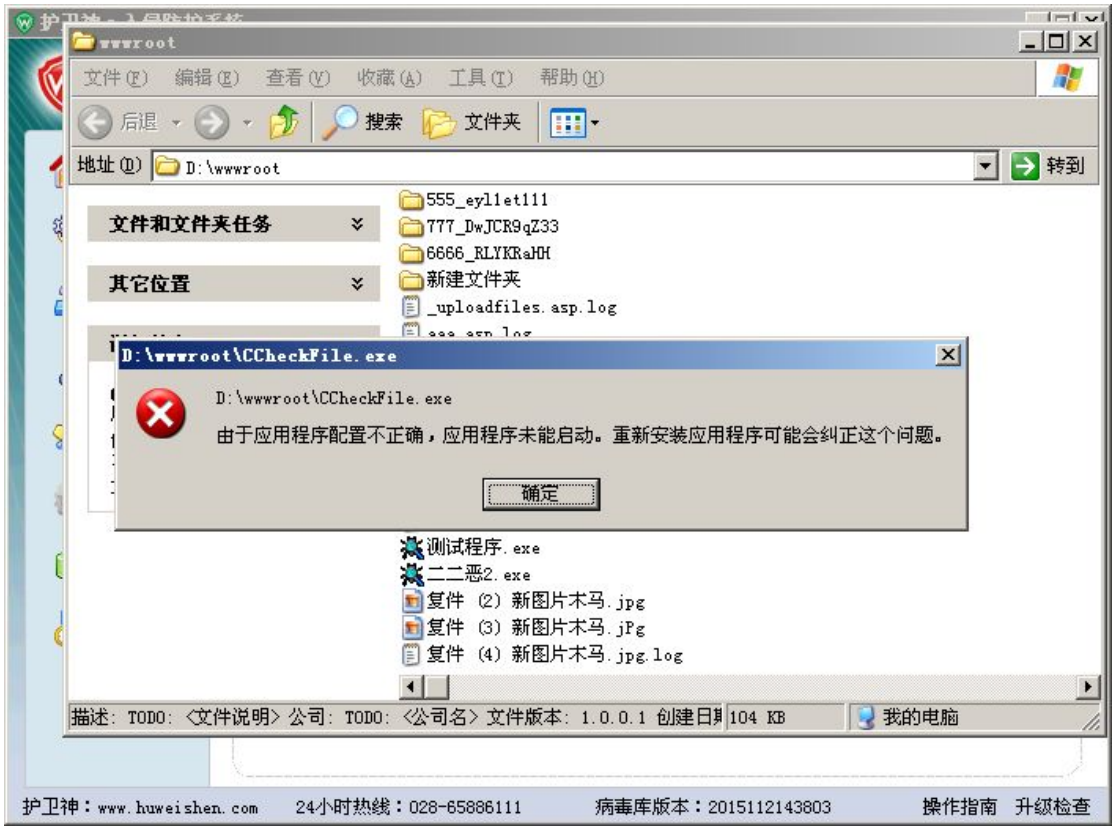

图 41 - 禁止执行文件拦截效果截图

5、禁止删除的效果：

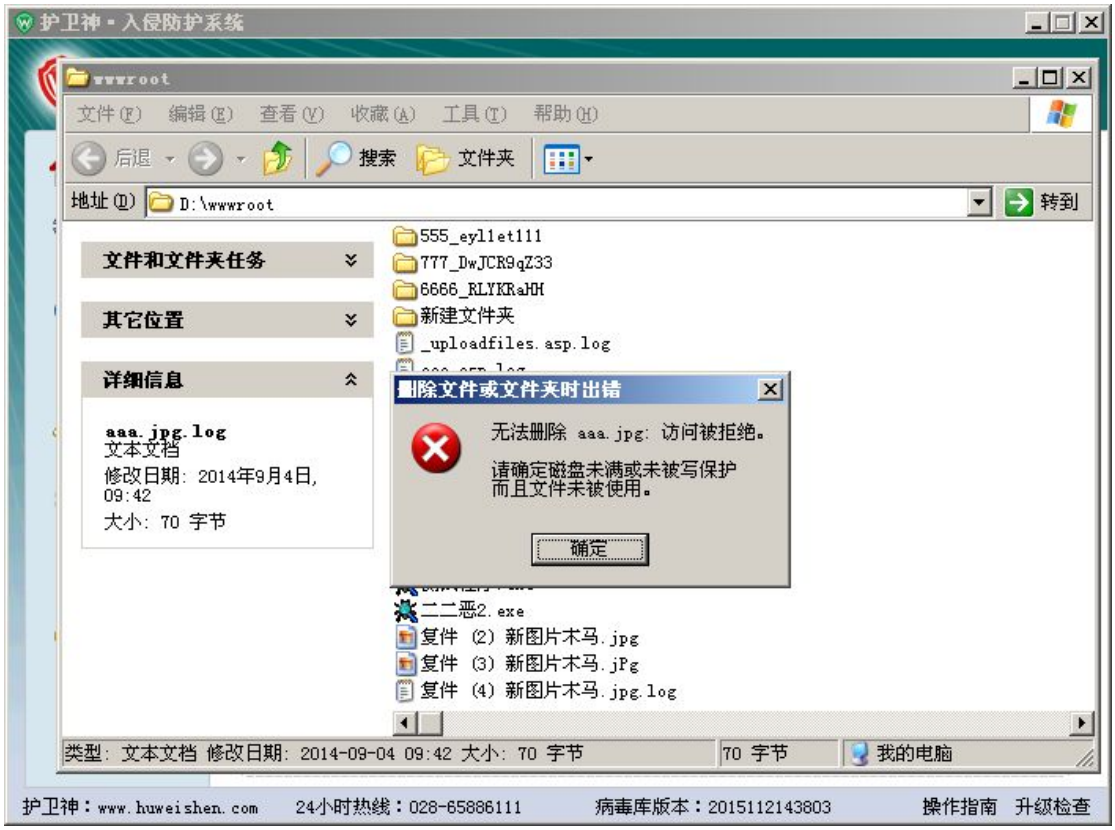

图 42 - 禁止删除文件拦截效果截图

（5）畸形扫描

点击【文件监控】的【畸形扫描】选项卡，打开畸形扫描模块；这是一个手动扫描畸形目录的功能，可以快速扫描指定目录下的畸形文件，并对扫描到的畸形文件强制删除，如图：

图 43 - 畸形扫描模块截图

说明：

1、首次安装护卫神·入侵防护系统，请用畸形扫描功能，扫描网站目录，清除隐藏在网页目录中的畸形文件。

2、扫描结束后，确认无误后点击右边删除所有，进行删除。

6、进程限制

点击左侧【进程限制】菜单，进入进程限制模块；进程限制是对针对指定进程，限制其执行其他进程或其本身被执行的功能。

（1）进程限制设置

进程限制设置如图：

图 44 - 进程限制模块截图

说明：

1、开启进程监控：选择则开启进程监控模块功能，不选择表示不开启。

2、监控的进程列表：所有监控的进程列表。

3、新增：新增一条进程监控项。

4、修改：修改列表中选中的项。

5、删除：删除列表中选中的项。

点击【新增】或【修改】按钮后，进入进程管理设置界面：

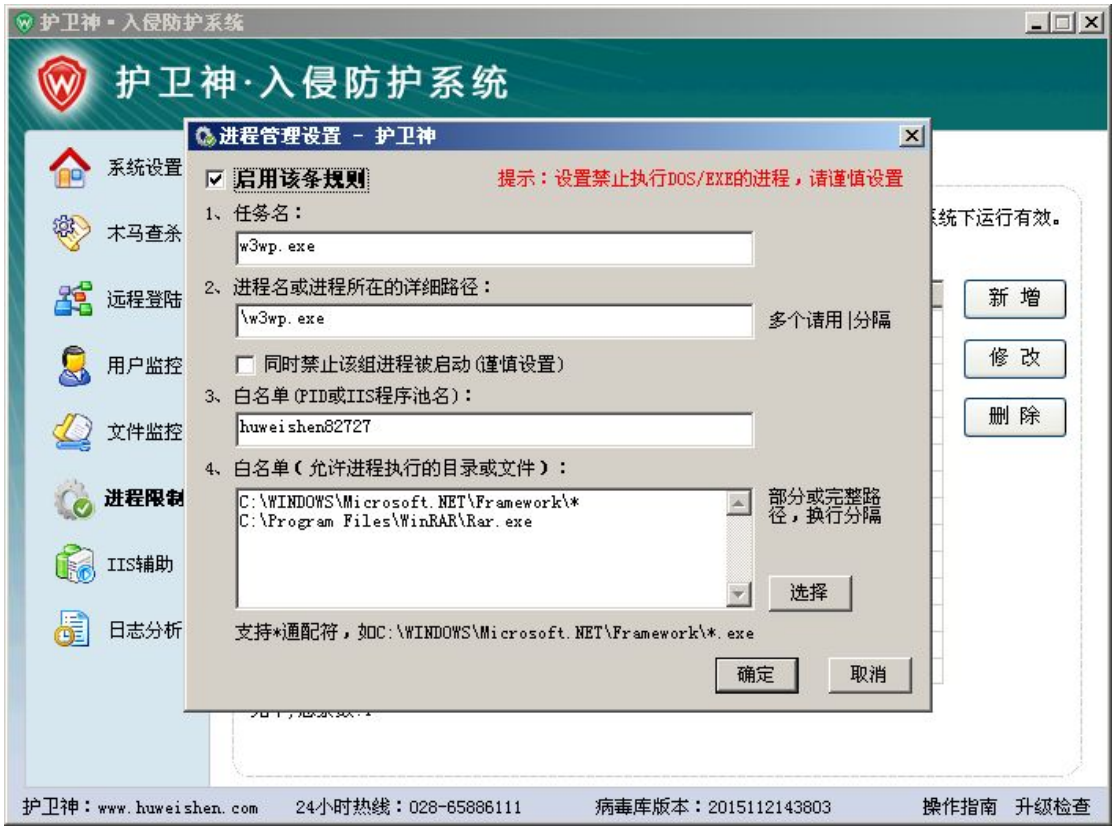

图 45 - 修改进程限制详细参数截图

说明：

1、启用该条规则：选中则表示启用该任务规则，不选中表示该规则无效。

2、任务名：该条进程监控的唯一名称，用于管理员识别。

3、进程名或进程所在的详细路径：任务实际监控的进程名，或详细到该进程的路径，如果多个进程，请用“|”分隔。

4、同事禁止该组进程被启动：选择后，当前监控的进程无法执行；若不选中，则当前监控进程本身可以执行。

5、白名单（PID 或 IIS 程序池名）：一般设置主机管理系统所在的程序池名。

6、白名单（允许进程执行的目录或文件）：白名单目录或文件，允许被监控的进程执行，规则支持*通配符，多条规则请用换行分隔。

（2）拦截效果

禁止进程被执行拦截效果图：

图 46 - 禁止进程被执行拦截效果截图

（3）进程列表

点击左侧【进程限制】菜单，再点击【进程列表】选项卡，打开进程列表，如图：

图 47 - 进程列表模块截图

说明：

1、进程列表：可以看到当前正在运行的所有进程、CPU 占用、路径等。

2、分类：可以筛选程序池和系统服务，如果选择程序池，则仅显示所有 w3wp.exe 进程信息；选择系统服务，则进现实所有系统服务进程运行信息。

3、刷新：重新加载所有进程列表信息。

4、双击列表可以打开 Windows 资源管理器，定位到该进程所在路径。

7、IIS 辅助

点击左侧【IIS 辅助】菜单，可以打开 IIS 辅助模块；该模块主要针对 Internet Information Services（互联网信息服务，简称 IIS）WEB 服务器网站进行安全防护。

（1）基本设置

进入 IIS 辅助，首先会看到基本设置模块，如图：

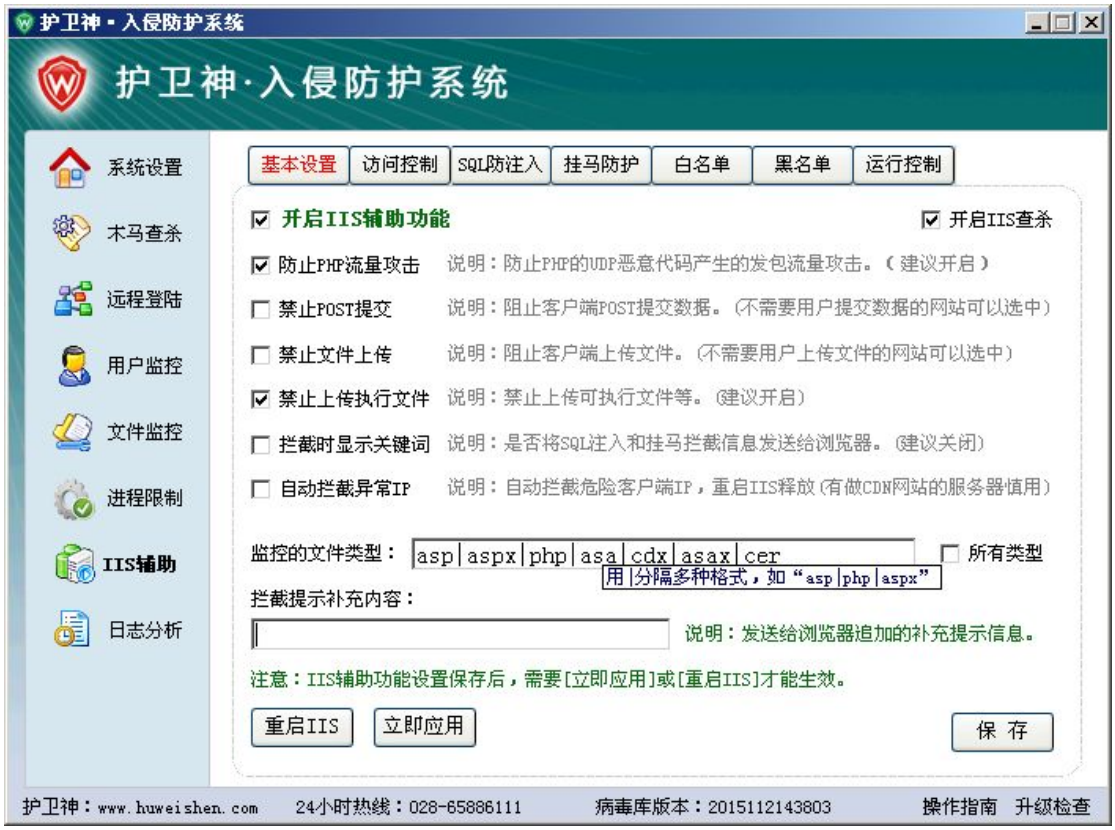

图 48 - IIS 辅助基本设置模块截图

说明：

1、开启 IIS 辅助功能：开启后，IIS 辅助功能生效，否则无效。

2、开启 IIS 查杀：在浏览器与服务器通信的数据流中检测危险数据，如果有，则进行阻断。

3、防止 PHP 流量攻击：防止 PHP 的 UDP 恶意流量上传攻击，建议开启。

4、禁止 POST 提交：阻止客户端 POST 提交数据。

5、禁止文件上传：阻止客户端上传文件。

6、禁止上传执行文件：禁止客户端上传可执行文件，如 exe/cmd 等。

7、拦截时显示关键词：是否将拦截关键词信息发送到浏览器，此功能是为了方便找到拦截的内容，但为了安全建议关闭。

8、自动拦截异常 IP：对试图尝试入侵服务器的 IP 进行拦截，在重启 IIS 后才会清除。注意，对于 CDN 节点的服务器建议不勾选。

9、监控的文件类型：一般需要监控动态脚本，如：asp|aspx|php|asa|cdx|asax|cer 等。选择所有类型，则将监控任何类型的文件。

10、拦截提示补充内容：您可以将自己的提示信息发送给被拦截的用户，如联系方式等。

11、重启 IIS：重新启动 w3svc 服务，重新应用 IIS 辅助设置，注，此功能需要先点击保存按钮保存配置信息。

12、立即应用：不用重启 IIS，直接让 IIS 配置信息生效，此功能需要先点击保存按钮保存配置信息。

13、保存：保存所有配置信息。

（2）访问控制

点击【IIS 辅助】的【访问控制】选项卡，打开访问控制功能，如图：

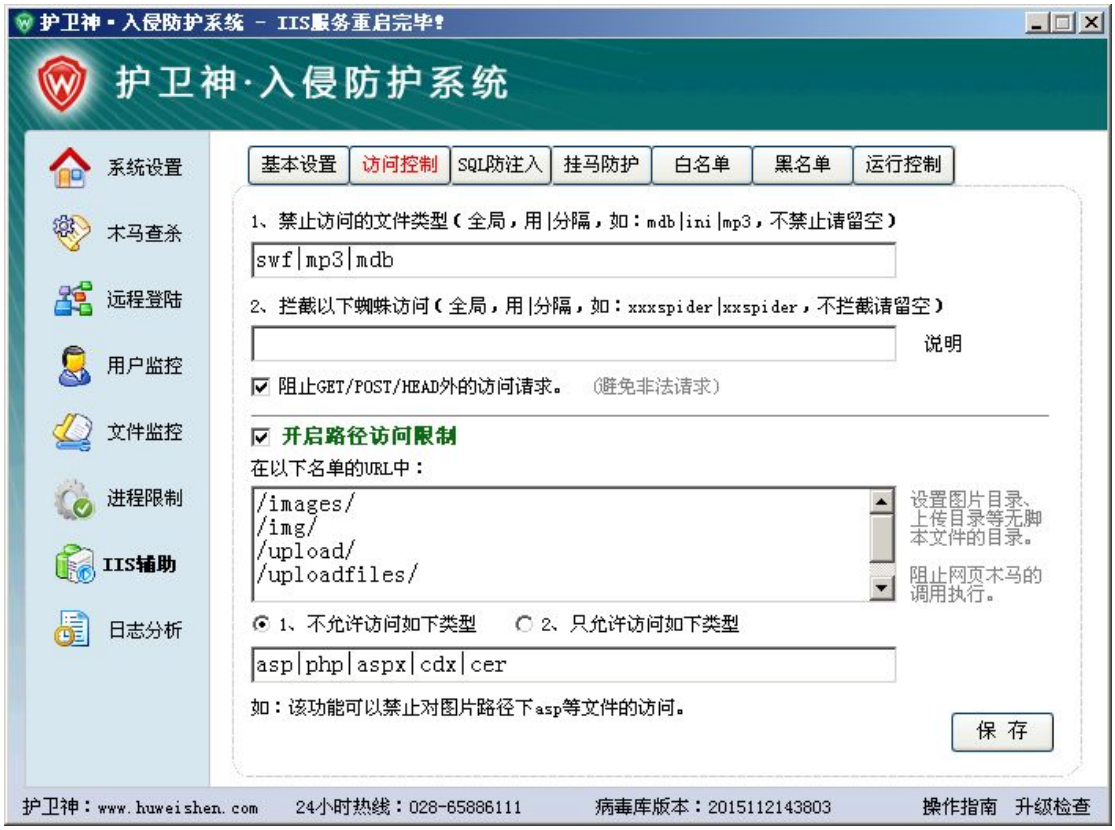

图 49 - IIS 辅助访问控制模块截图

说明：

1、禁止访问的文件类型：如设置 mdb|ini|mp3 等，可以禁止客户端浏览器访问下载这些文件，保护这些文件。

2、拦截以下蜘蛛访问：输入搜索引擎特征，拦截对应的蜘蛛爬虫抓取您的网页，详细设置请参见后边的【说明】。

3、阻止 GET/POST/HEAD 外的访问请求：禁止 GET/POST/HEAD 外的非法请求。

4、开启路径访问控制：选择表示开启 URL 路径访问控制功能，不选择表示关闭。

5、在以下名单的 URL 中：一般设置图片目录、上传目录等静态目录，不需要执行脚本的目录，如：“/images/”、“/uploadfiles/”等，禁止该目录下的脚本文件，如 asp 文件被访问。

6、不允许访问如下类型：在上述 URL 名单中，不允许含有指定的文件类型被访问。

7、只允许访问如下类型：在上述 URL 名单中，只允许含有指定的文件类型被访问。

8、保存：点击保存配置信息。

9、拦截效果如图：

图 50 - IIS 辅助访问控制拦截指定类型文件效果截图

10、路径访问控制拦截效果如图：

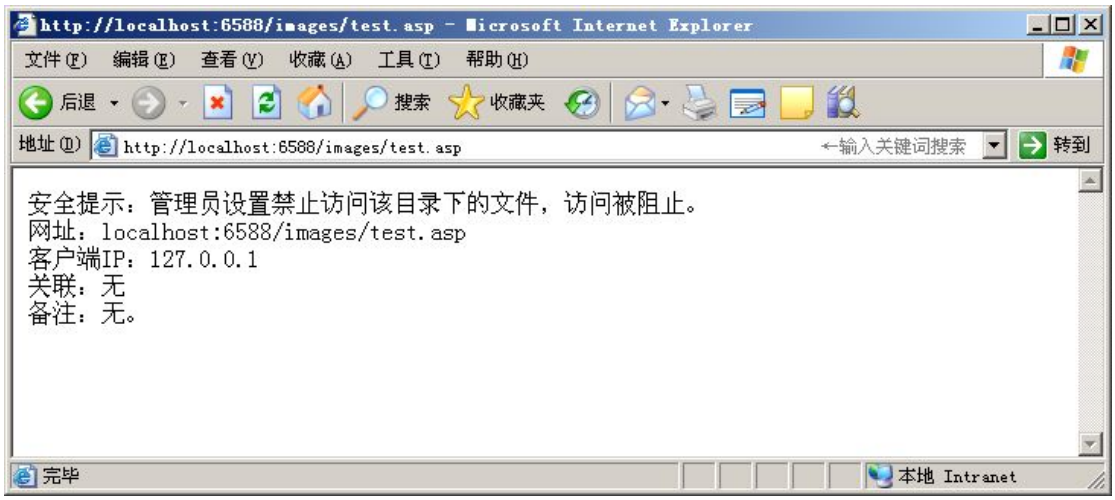

图 51 - IIS 辅助访问控制拦截指定目录下指定文件效果截图

（3）SQL 防注入

点击【IIS 辅助】的【SQL 防注入】选项卡，进入 SQL 防注入，如图：

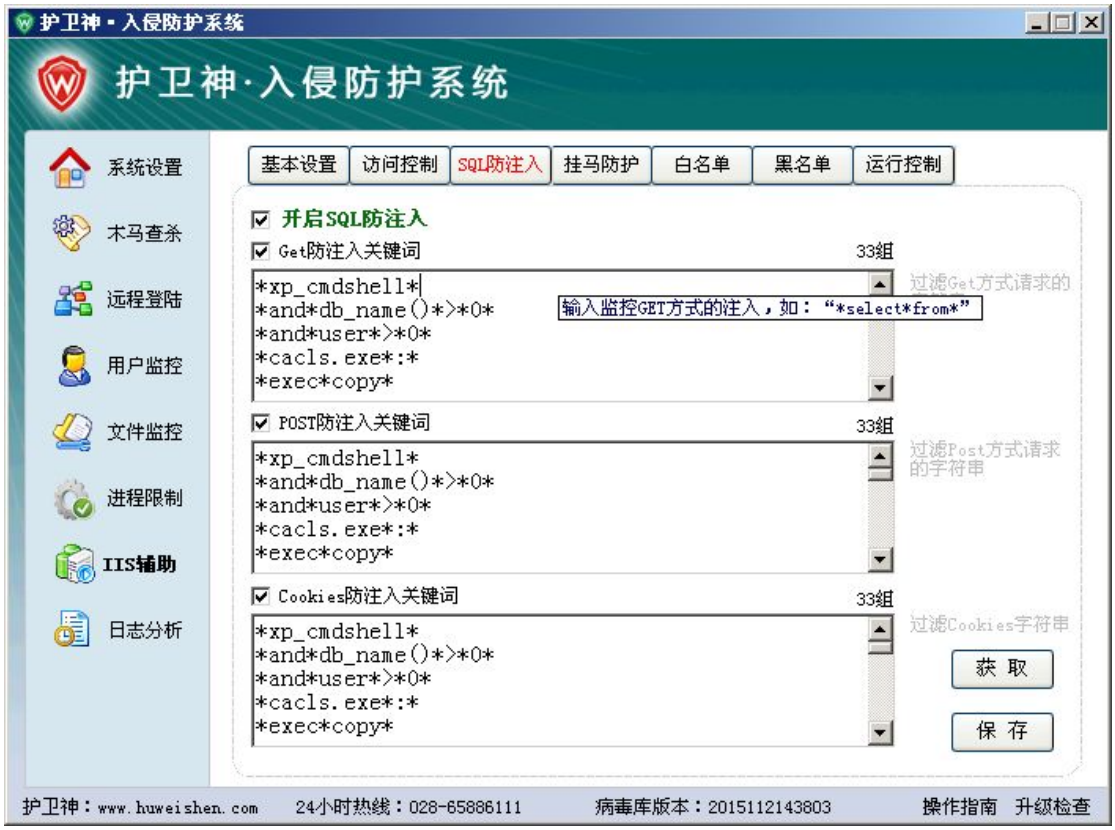

图 52 - IIS 辅助 SQL 防注入模块截图

说明：

1、开启 SQL 防注入：选中则开启 SQL 防注入功能，不选择表示不开启。

2、Get 防注入关键词：过滤 URL 中的字符串，包括通过 URL 编码的字符串。

3、POST 防注入关键词：过滤 POST 提交数据中的数据，包括通过 URL 编码的数据。

4、Cookies 防注入关键词：过滤 Cookies 中的数据，包括通过 URL 编码的数据。

5、【获取】按钮：获取护卫神官方内置的防注入关键词，比较完全，推荐采用。

6、如果需要开启某功能，请选择对应的选项，并保存。保存完毕之后，请重启 IIS 以便完成应用。

7、SQL 防注入拦截效果图：

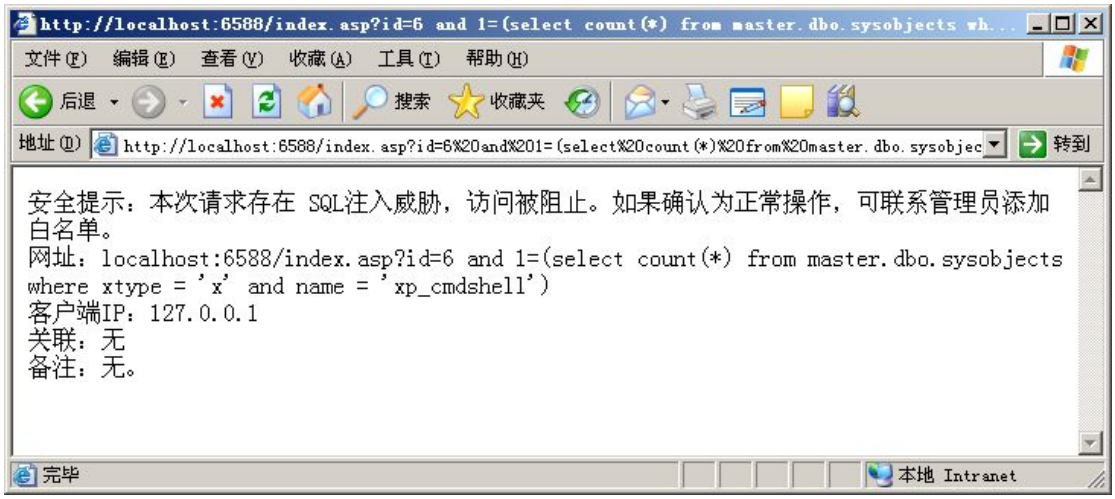

图 53 - IIS 辅助拦截 SQL 注入效果图

（4）挂马防护

点击【IIS 辅助】的【挂马防护】选项卡，进入挂马防护功能，如图：

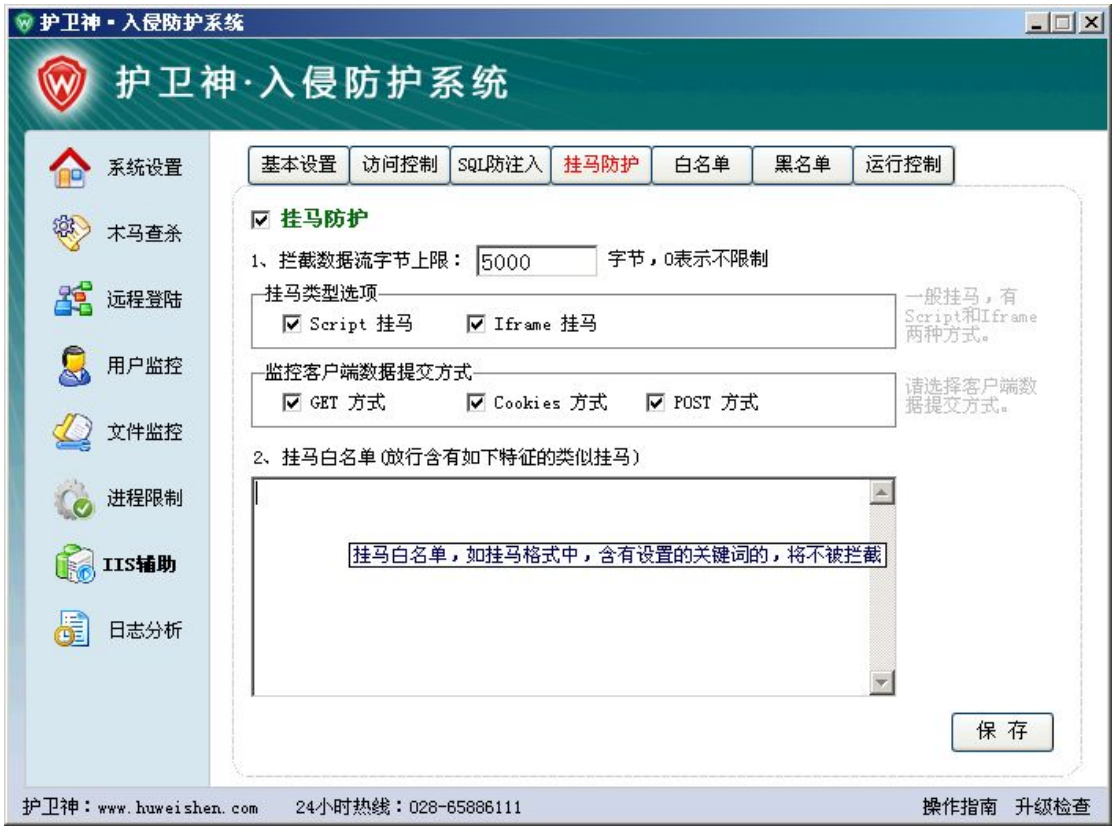

图 54 - IIS 辅助挂马防护截图

说明：

1、挂马防护：选择表示开启，不选择表示不开启。

2、拦截数据流字节上限：超过该设定字节长度的数据流，将不进行解析，默认 5000，用户可以自定义。

3、挂马类型选项：包括 Script/Iframe 挂马，选中可以拦截对应的挂马格式。

a) Script 格式如：<script src=http://www.aa.com/muma.js></script>；

b) Iframe 格式如：<Iframe src=http://www.aa.com; width='250'height='200' scrolling='no'frameborder='0'> </iframe> 。

4、监控客户端数据提交方式：包括 Get/Post/Cookies 三种，建议都勾选。

5、挂马白名单，如含有某些认可的特征，如某些统计代码，则可以将这些代码中的关键部分提取到挂马白名单中，那么即使提交的数据含有挂马的特征，但是含有白名单特征码，因此不会被拦截。

6、挂马操作被拦截后的提示：

图 55 - IIS 辅助拦截挂马效果图

（5）白名单

点击【IIS 辅助】的【白名单】选项卡，进入白名单设置，如图：

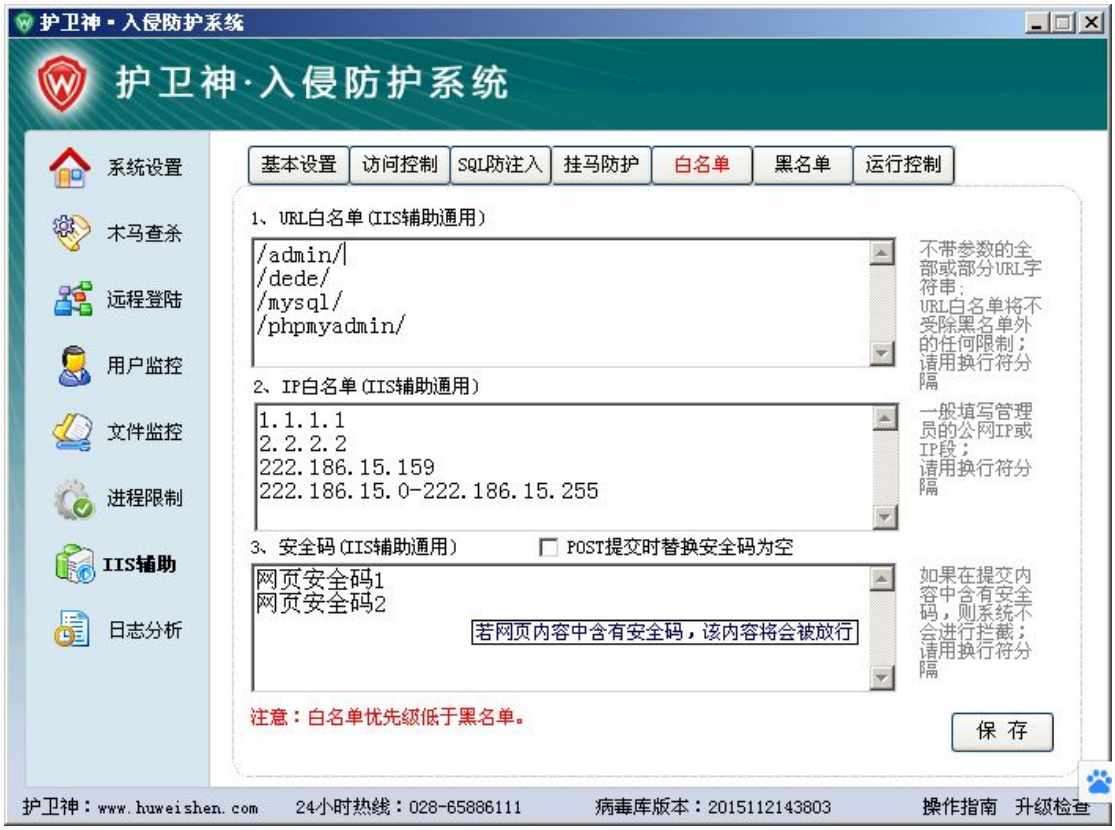

图 56 - IIS 辅助白名单模块截图

说明：

1、URL 白名单：设置信任的部分 URL 路径或完整路径 URL 路径，该目录下的文件将不受限制的访问。

2、IP 白名单：指定的客户端 IP(段)将不受限制的访问此服务器上的 WEB 站。

3、安全码：如果通过网页提交的内容包含了安全码特征，那么该次提交将不会被拦截。

4、注意：白名单优先级低于黑名单。

（6）黑名单

点击【IIS 辅助】的【黑名单】选项卡，进入黑名单设置，如图：

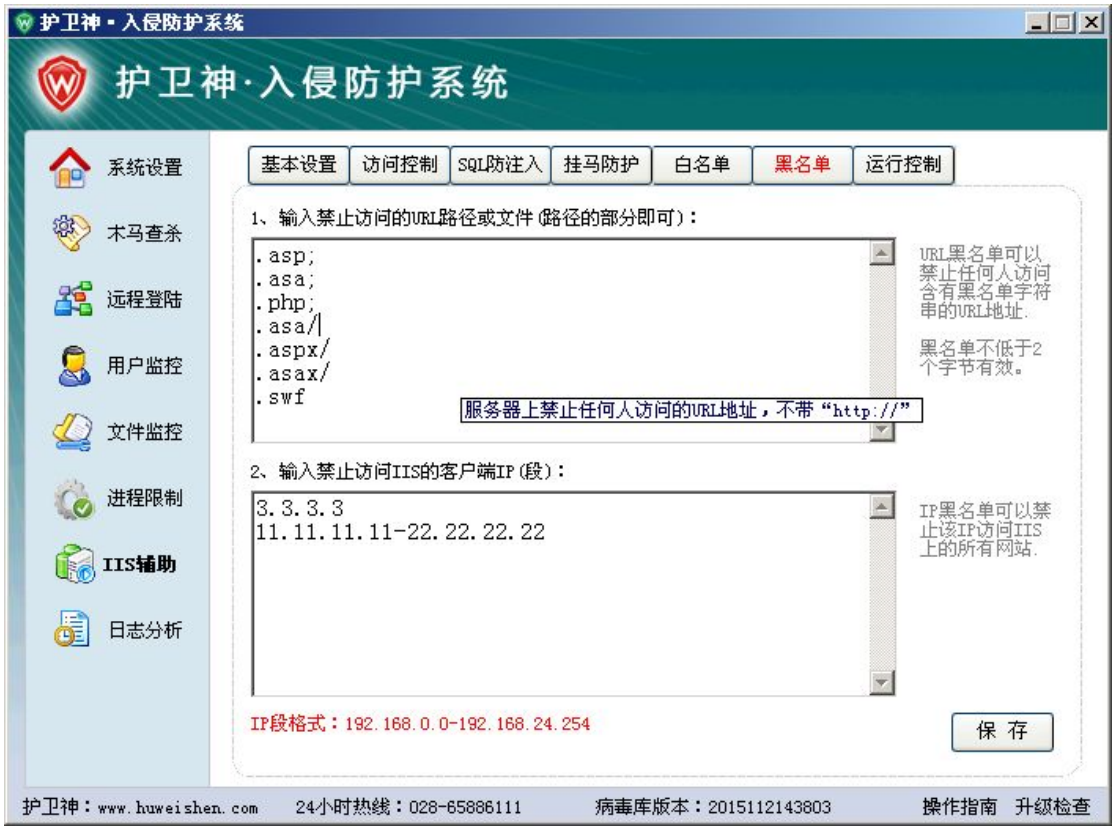

图 57 - IIS 辅助黑名单模块截图

说明：

1、禁止访问的 URL 路径或文件：如不希望某些目录或文件被访问，则可以设置到这里。

2、输入禁止访问的 IIS 的客户端 IP(段)：禁止该 IP 的客户端访问 IIS 上的网站。

3、保存：保存所设置的配置信息，重启 IIS 后立即生效。

4、注：黑名单优先级高于白名单。

5、URL 黑名单拦截效果如图：

图 58 - IIS 辅助 URL 黑名单拦截效果截图

6、IP 黑名单拦截效果如图：

图 59 - IIS 辅助 IP 黑名单拦截效果截图

（7）运行控制

点击【IIS 辅助】的【运行控制】选项卡，进入运行控制设置，如图：

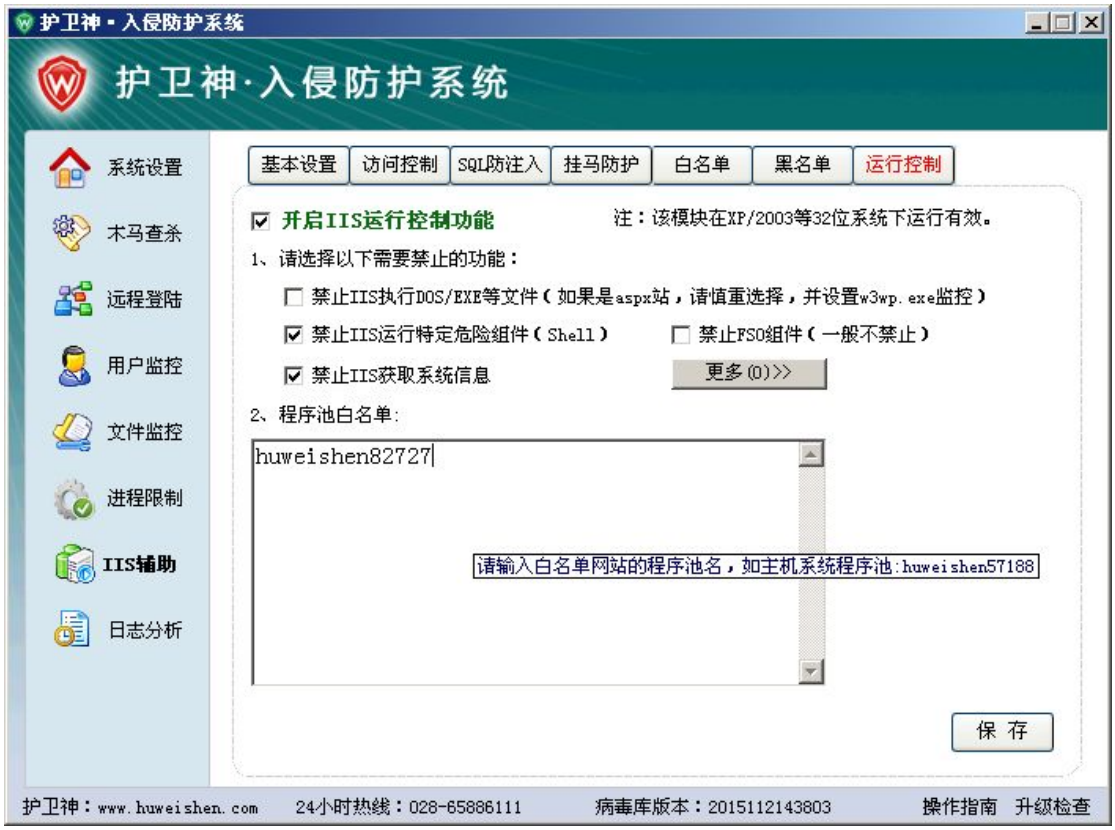

图 60 - IIS 辅助运行控制模块截图

说明：

1、开启 IIS 运行控制功能：选择表示开启运行控制功能，不选表示不开启。

2、禁止 IIS 执行 DOS/EXE 等文件：选择后，将禁止 w3wp.exe 进程执行其他可执行文件。

3、禁止 IIS 运行特定危险组件：选择后，将禁止 w3wp.exe 进程运行其他危险组件，如 Shell。

4、禁止 FSO 组件：选择后，将禁止 w3wp.exe 创建文件系统对象（FSO），选择后会导致许多需要 fso 的正常组件运行失败，请根据自身需要设置。

5、禁止 IIS 获取系统信息：主要禁止 w3wp.exe 获取 Windows 计算机硬件信息、IIS 网站账户信息等

敏感信息。

6、程序池白名单：一般设置主机管理系统所在程序池名，白名单中的程序池将不受运行控制限制。

7、更多：可以自定义更多需要拦截的组件（CLSID 或 TypeLib），如下图：

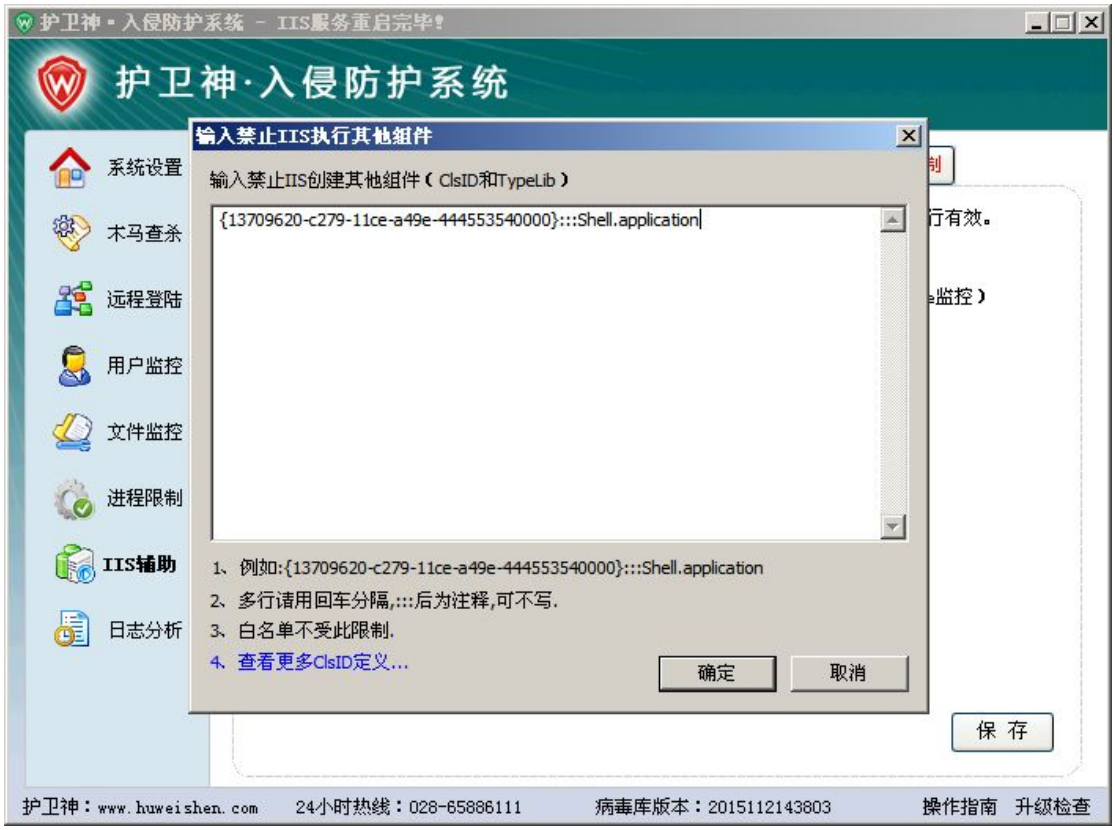

图 61 - IIS 辅助挂马防护截图

8、保存：保存所设置的配置信息，重启 IIS 后立即生效。

9、拦截效果（以创建 FSO 对象为例）

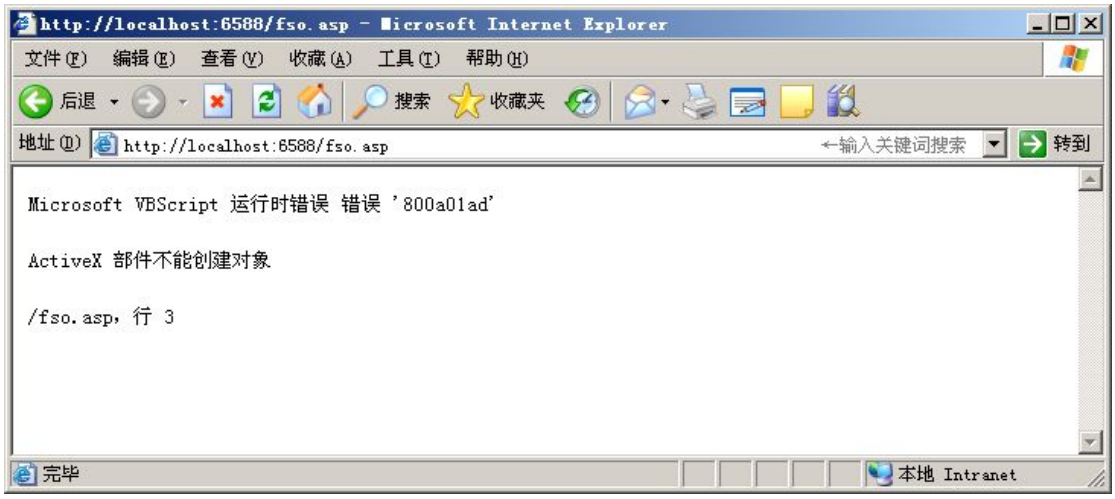

图 62 - IIS 辅助拦截 FSO 对象创建效果截图

（8）拦截日志

IIS 辅助拦截日志示意图

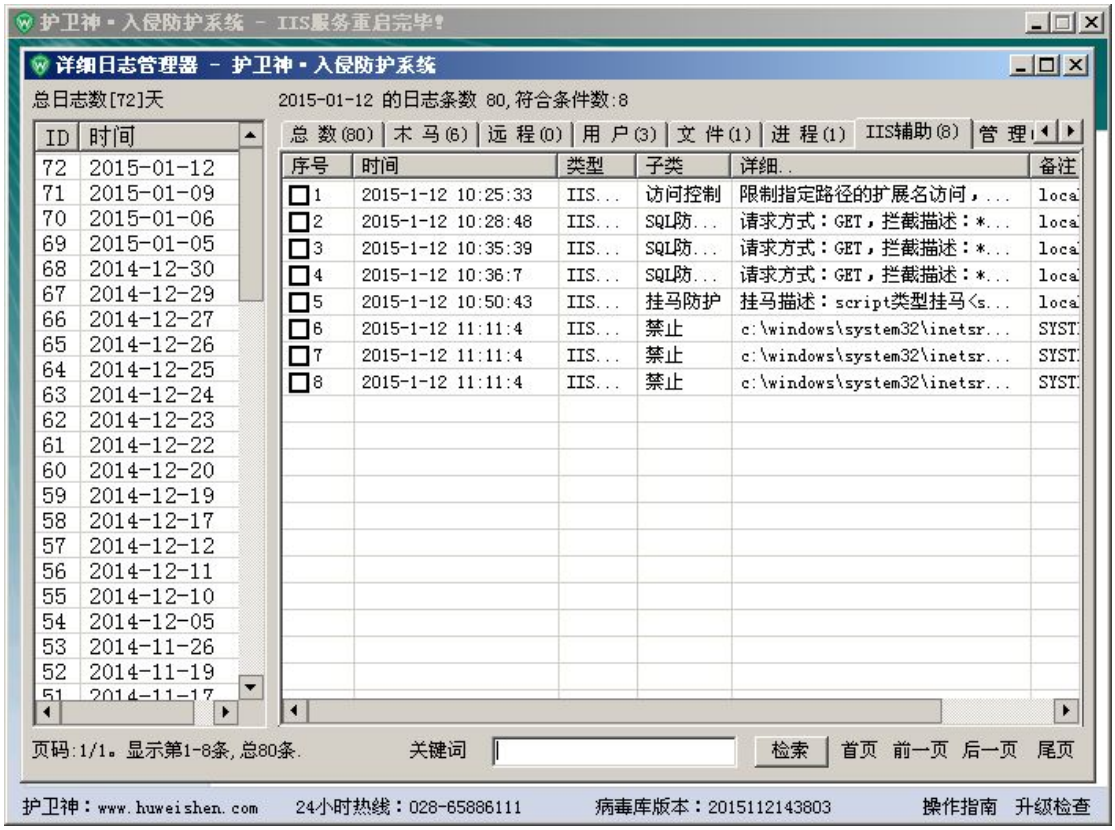

图 63 - IIS 辅助拦截日志截图

（9）IIS 辅助注意事项

1、仅限于采用 IIS 做 WEB 服务器的服务器使用，Apache 用户无法使用。

2、修改设置后，请保存，并重启 IIS 才会立即生效。

3、为了提高效率，系统记录的日志并不是实时记录，如果您想立刻查看日志，请重启 IIS，否则，护卫神·入侵防护系统会根据时间和日志条数写日志。

8、日志分析

护卫神日志，主要有【日志记录】和【隔离文件】两个模块。

（1）日志记录

点击左侧【日志分析】菜单，就可以进入日志记录页面；日志记录记录了软件手动和自动处理的详细日志，便于管理人员分析，如图：

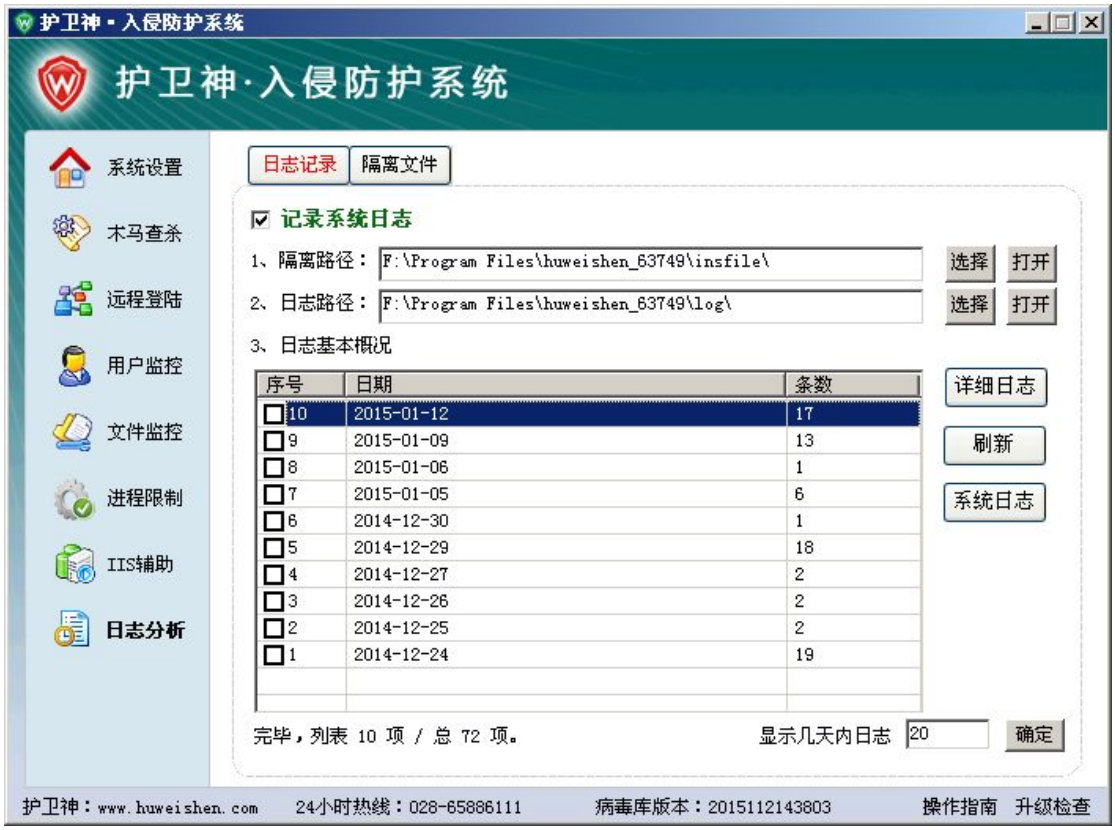

图 64 - 日志记录截图

说明：

1、记录系统日志：如不选择，则系统不会记录日志，建议选中。

2、隔离路径：存放隔离文件的目录。

3、日志路径：存放日志文件的目录。

4、双击列表中某天日志，即可打开详细的日志分析画面，如下图：

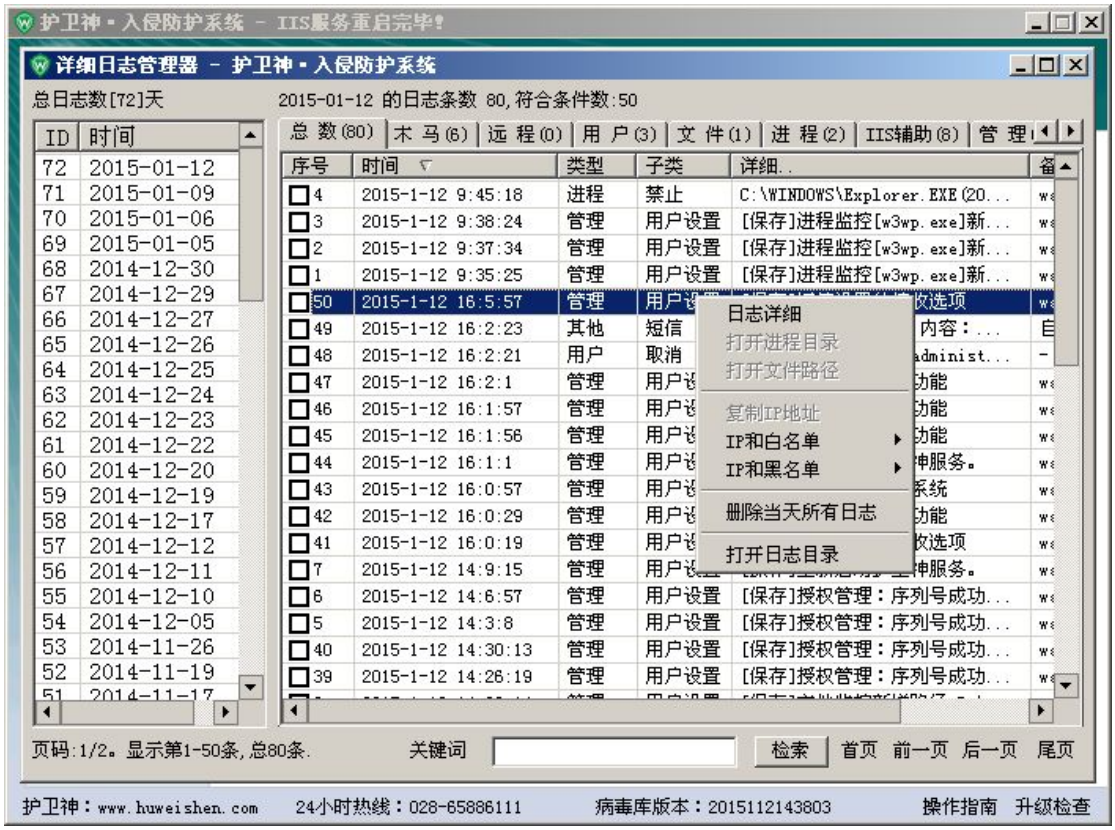

图 65 - 详细日志管理器截图

说明:

在日志详细分析画面中,您可以对日志进行随意处理,可以使用键盘方向键进行翻页、使用 Ctrl + A 全选等。

(2)隔离文件

如果文件被隔离了,可以打开隔离文件管理器进行管理,包括还原和删除。

图 66 - 隔离文件管理器截图

说明：

1、查看详细：查看该记录详细的信息。

2、打开文件：用记事本打开文件，查看该文件具体内容。

3、打开当前目录：打开文件被隔离后的目录，并选中该文件。

4、打开源目录：打开被隔离文件之前的目录。

5、全选：选择所有。

6、反选：将未选中的选中，已选中的取消选中。

7、删除当前项：删除鼠标当前选中的某一条，删除后无法恢复。

8、删除选中项：选中所有勾选的项目，删除后无法恢复。

9、删除所有项：删除所有已勾选和未勾选的项，删除后无法恢复。

10、还原当前项：还原鼠标点击的某一项到之前的位置，如果已经存在，则提供会询问。

11、还原选中项：还原所有勾选的项目到各自之前对应的位置。

12、还原所有项：还原所有已勾选和未勾选的项到各自之前对应的位置。

13、注意：该操作需要与后台服务程序协调操作才能完成，因此您需要确保护卫神正常运行。

第六部分 木马查杀模块

木马查杀模块为手动查杀服务器存在的网页木马，准确性高，查杀速度快，建议在首次安装使用此模块对所有网页文件进行全面查杀。

1、启动方式

1、点击【系统设置】的【系统概况】选项卡，点击【木马查杀】按钮，则可以启动木马查杀模块。

2、双击安装目录下的“HwsKill.exe”，也可以启动木马查杀模块。

3、在文件(夹)上点击右键，选择“使用[护卫神]快速扫描网页木马(K)”，即可启动木马查杀模块，如下图：

图 67 - 在文件夹上点击鼠标右键启动网页木马查杀模块示意图

2、操作介绍

网页木马查杀主界面：

图 68 - 网页木马查杀模块截图

说明：

1、查杀路径：当前正在查杀的路径，可以支持鼠标拖放路径到此。

2、所有网站：选择后，系统自动搜索当前服务器上所有网站，并列表到左侧。

3、自定义路径：选择后，自动默认获取当前设置监控的网站路径，并列表到左侧；如果手动拖放路径，也会自动添加到左侧列表。

4、选择：选择需要查杀的路径，一般选择网页文件所在目录即可。

5、开始：开始对选择路径的网页木马进行扫描；开始后按钮会转变为暂停，此时可以继续扫描。

6、设置：设置扫描规则，如扫描文件类型等，详见第四部分第 3 节系统设置。

7、停止：停止扫描。

8、退出：退出网页木马查杀模块。

右键快捷菜单说明：

1、打开文件：用系统自带的记事本打开该文本文件，方便查看内容分析。

2、打开文件路径：打开该木马路径，方便确认具体位置。

3、打开日志路径：打开护卫神的日志目录，方便查看日志。

4、隔离当前文件：对鼠标选择的某项文件进行隔离，隔离后，可以在入侵防护系统的隔离文件管理中找到并处理，如还原。

5、隔离选中文件：隔离所有选择的项目，支持快捷键 Ctrl + A 全选。

6、隔离所有文件：将所有文件，包括未选中的文件，进行隔离。

7、删除当前文件：对鼠标选择的某项文件进行删除，注意删除后无法从回收站中撤销。

8、删除选中文件：删除所有选择的项目，未选中的不进行处理。

9、删除所有文件：删除所有项目，包括未选中的项目。

10、全选：全部选中，支持 Ctrl + A 快捷键。

11、反选：对已选的项目进行取消，对未选择的项目进行选择。

12、清空记录：清空列表，不会对列表中的文件进行处理。

13、查看木马说明：对鼠标选择的项的木马进行解释，以便对该木马进行进一步的了解。

3、系统设置

点击【设置】按钮，打开规则设置，如图：

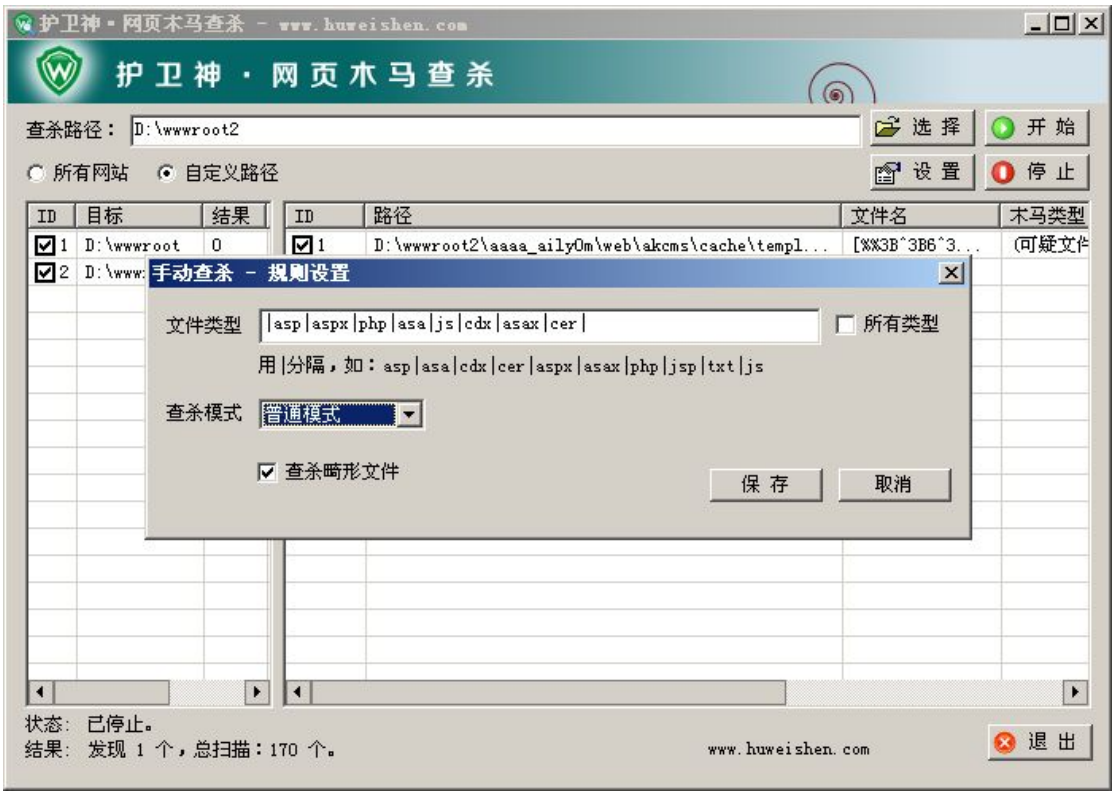

图 69 - 网页木马查杀规则设置界面截图

说明：

1、文件类型：设置扫描的网页文件类型，一般设置动态脚本后缀，如：|asp|aspx|php|asa |cdx|asax|cer|等。

2、所有类型：选中后不限制扫描类型，所有类型的文件均要被扫描，如图片。

3、查杀模式：

a) 普通模式：正常查杀算法，效率高，准确率高，一般推荐用此。

b) 极限模式：比较严格的查杀算法，查杀比较彻底，能查出很多变种木马，但是会存在一定程度的误杀，用此模式杀出来的木马文件，需要辨别后再做处理。

c) 非法生成扫描：采用系统的非法生成词库，扫描网页文件，看看是否被挂马。

4、查杀畸形文件：查杀扫描目录中存在的畸形文件，很多木马文件利用此方式影藏自己，并且在 Windows 资源管理器中无法删除，因此建议选中。

5、保存：点击保存设置并关闭界面。

6、取消：点击取消设置并关闭界面。

第七部分 安全检测模块

1、启动方式

1、点击【系统设置】的【系统概况】选项卡，点击【安全检测】按钮，可以启动系统安全检测模块。

2、双击安装目录下的“HwsCheck.exe”，也可以启动系统安全检测模块。

2、功能介绍

图 70 - 安全检测模块截图

说明：

1、开始检测：点击后，软件会开始对服务器安全项目进行扫描，并将结果显示在列表。

2、导出报告：点击后，可以将检测的结果导出到指定路径的文件中。

3、强化安全：点击后链接到护卫神官网服务中心，获取解决方案。

4、检测项目：分为系统账户检测、重点软件检测、磁盘权限检测、网站权限检测、重点服务检测；这些都是必要的安全措施。

第八部分 软件维护常见问题

1、杀软阻止

由于护卫神安装，要在启动项添加系统托盘，要添加服务项，以及要访问官方网站，因此可能会被部分杀毒软件阻止或者报不安全，此种情况，请放行即可，软件是安全的。

2、网页文件被误杀

如果有正常用户的文件被当成病毒查杀了，您可以从【系统日志】→【隔离文件】中，找到 该文件，进行还原即可；还原后的文件会被自动添加到木马查杀的白名单。

为从根源解决此问题，请及时向我们在线客服反馈此情况，或者提取该类文件的部分内容，放到【木马查杀】→【白名单】→【安全码】中。

3、CPU 消耗偏高

如果您在使用过程中，实时监控目录中文件的变化十分频繁，可能导致护卫神进程 hws.exe 占用的 CPU 资源偏高。如果持续很长时间，请联系我们的在线客服。

4、进程 hws.exe 不能自启动

造成此种情况的原因，很可能是由于某些进程阻止了护卫神·入侵防护系统的服务自动启动操作。您可以按照这样的步骤进行修复：【系统管理】→【修复软件】；在这个菜单中，您还可以修复 IIS 中 ISAPI 的注册被其他因素删除的问题。

第九部分 附录

1、关键词加减法规则

（1）加法规则

1、格式：关键词 1+关键词 2，关键词 1+关键词 2+关键词 3+…+关键词 N，支持连续加号；
2、若在一个字符串中，加号连接的所有关键词均能找到，则表示匹配成功，否则匹配失败。

（2）减法规则

1、格式：关键词 1-关键词 2，关键词 1-关键词 2-关键词 3-…-关键词 N；
2、减法规则支持连续减法，但只允许一个被减数，允许多个关键词连续相减；
3、减法表达式中，若只出现关键词 1，但是关键词 2 以及后续的关键词均未出现，则表示匹配成功；
4、若出现关键词 1，同时也出现了关键词 2 以及以后的任何一个关键词，则表示匹配失败。

第十部分 致谢

感谢您选择护卫神·入侵防护系统！

更强的技术、更好的服务、更实用的软件，专注服务器入侵安全！

公司名称：四川万象更新网络通信有限公司
公司地址：四川成都市二环路东五段万达广场3单元2004号

护卫神官网（www.huweishen.com）
2015-01-15