
中安恶意代码辅助检测系统

（主机版） V3.0

用户手册

北京中安兴坤科技有限公司
版权所有 翻版必究

版权声明

北京中安兴坤科技有限公司（以下简称“中安兴坤”）
©2012~2027 版权所有，保留一切权力。

未经中安兴坤书面同意不得擅自拷贝、传播、复制、泄露或复写本文档的全部或部分内容。本文档中的信息归北京中安兴坤科技有限公司所有并受中国知识产权法和国际公约的保护。

信息更新

本文档及其相关计算机程序仅用于为最终用户提供信息，并且随时可由中安兴坤更改或撤回。

免责条款

根据适用法律的许可范围，中安兴坤按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性 or 无侵害性。在任何情况下，中安兴坤都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使中安兴坤明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。

本文档中所有引用产品的使用及本文档均受最终用户可适用的特许协议约束。

目录

一、产品功能概述	1
二、系统结构	2
三、产品支持环境	2
3.1 支持操作系统	2
3.2 最小硬件要求	2
四、软件安装卸载	3
4.1 软件安装	3
4.2 软件卸载	7
五、系统登录	10
六、系统管理员登录操作	11
6.1 密码修改	11
6.2 软件激活	12
6.3 木马库更新	15
七、安全保密管理员登录操作	18
7.1 密码修改	18
7.2 木马扫描	18
7.2.1 快速扫描	19
7.2.2 全盘扫描	21
7.2.3 自定义扫描	22
7.3 安全检查	24
7.3.1 基本信息	24
7.3.2 辅助检测	28
7.4 动态检测	32
7.5 进程信息	33
7.6 样本分析	35
7.7 日志管理	37
7.8 系统设置	39
7.8.1 安全设置	40
7.8.2 存储设置	40
7.8.3 扫描设置	40
7.8.4 进程设置	41
7.8.5 域名设置	41
7.8.6 IP 设置	42
7.8.7 端口设置	42
7.9 统计分析	43
7.10 操作日志	44
7.11 综合报告导出	44
八、安全审计员登录操作	45
8.1 密码修改	45
8.2 操作日志	45
九、三员通用操作	46
9.1 关于	46
9.2 帮助	46
9.3 切换用户	46
9.4 重置密码	47
十、技术支持	48

一、产品功能概述

近年来，“特洛伊木马”（以下简称木马）数量迅速增加，而且种类较多，在各类非法程序中已经占到了极大的比重，由木马所造成的破坏和损失也越来越严重，

我国的互联网正处在一个普及阶段的大规模扩张时期，当前的网络安全虽然已经做了不少努力，但总体而言还比较脆弱，且安全意识比较薄弱。尤其是在我国保密要害部门均发现有木马攻击案例，目前木马的技术发展极其迅速，且隐蔽性较强，有些甚至能破坏常见杀毒引擎而绕过检测，而传统病毒防护系统对很多木马无法准确检测，专业化反木马的研究已成为信息安全保密领域的一个热点和重点。

中安恶意代码辅助检测系统是由北京中安兴坤科技有限公司针对目前我国现阶段信息化建设过程中计算机系统中木马猖獗且发生众多泄密事件而研制开发的专业级木马等恶意代码辅助检测系统，并能够全程监测木马等恶意软件活动并进行全方位监控，是我国各级政府、军工企业等保密要害部门信息化建设过程中必不可少的工具。

中安恶意代码辅助检测系统是专业级木马恶意代码检测工具，系统适用于 Windows NT 系列操作系统（Windows 2000/XP/2003/Vista/Win7/Win10/Win11 等）以及主流的国产操作系统（银河麒麟桌面操作系统、统信桌面操作系统、中科方德桌面操作系统等），支持多种 CPU 平台类型（amd64、arm64、mips64el、loongarch64），系统能够对系统中的木马进行准确检查，区别于传统的病毒查杀类软件，可深度检测当前系统中包含敏感隐藏区域是否存在各类可疑行为，并根据系统策略要求做出响应，协助安全保密管理员彻底清除系统中恶意木马程序，同时系统可通过各类行为分析等方式对木马行踪进

行跟踪定位，如：端口、进程、服务、网络连接状态等。

二、系统结构

系统的运行环境基于 Windows 平台或国产 CPU 平台，包含：木马特载数据库，木马检测引擎，调度管理引擎，管理控制模块，辅助检测工具等。

木马特征数据库：这是整个系统的基础，系统收集有最新的木马数据库，而且由专业团队跟踪分析当前最新木马发展情况，保持数据库更新的高效，准确。

木马检测引擎：负责调度检测木马，该模块的设计既要满足稳定，快速的检测，而且也考虑到了对系统资源的合理使用问题。

调度管理引擎：负责根据设置调度扫描任务。

管理控制模块：提供管理窗口进行系统的配置，使用等。

辅助检测工具：提供一些高级分析工具，用于分析系统可能潜在的危险，方便用户进行人工判断。

三、产品支持环境

3.1 支持操作系统

- Windows XP 及以后所有 Windows 系统
- 银河麒麟桌面操作系统
- 统信桌面操作系统
- 中科方德桌面操作系统
- 中标麒麟桌面操作系统

3.2 最小硬件要求

- 大于 Intel Pentium CPU 1.2 GHz
- 国产 CPU：最低龙芯 3A3000

- 国产 CPU：最低飞腾 1500
- 国产 CPU：最低兆芯 ZX-C4610
- 国产 CPU：最低鲲鹏 920
- 国产 CPU：最低麒麟 9006C
- 100 MB 磁盘空间（用于安装，不包含系统运行中产生的数据空间）
- 2GB 以上 RAM 内存

四、软件安装卸载

4.1 软件安装

（1）Windows 系统软件安装

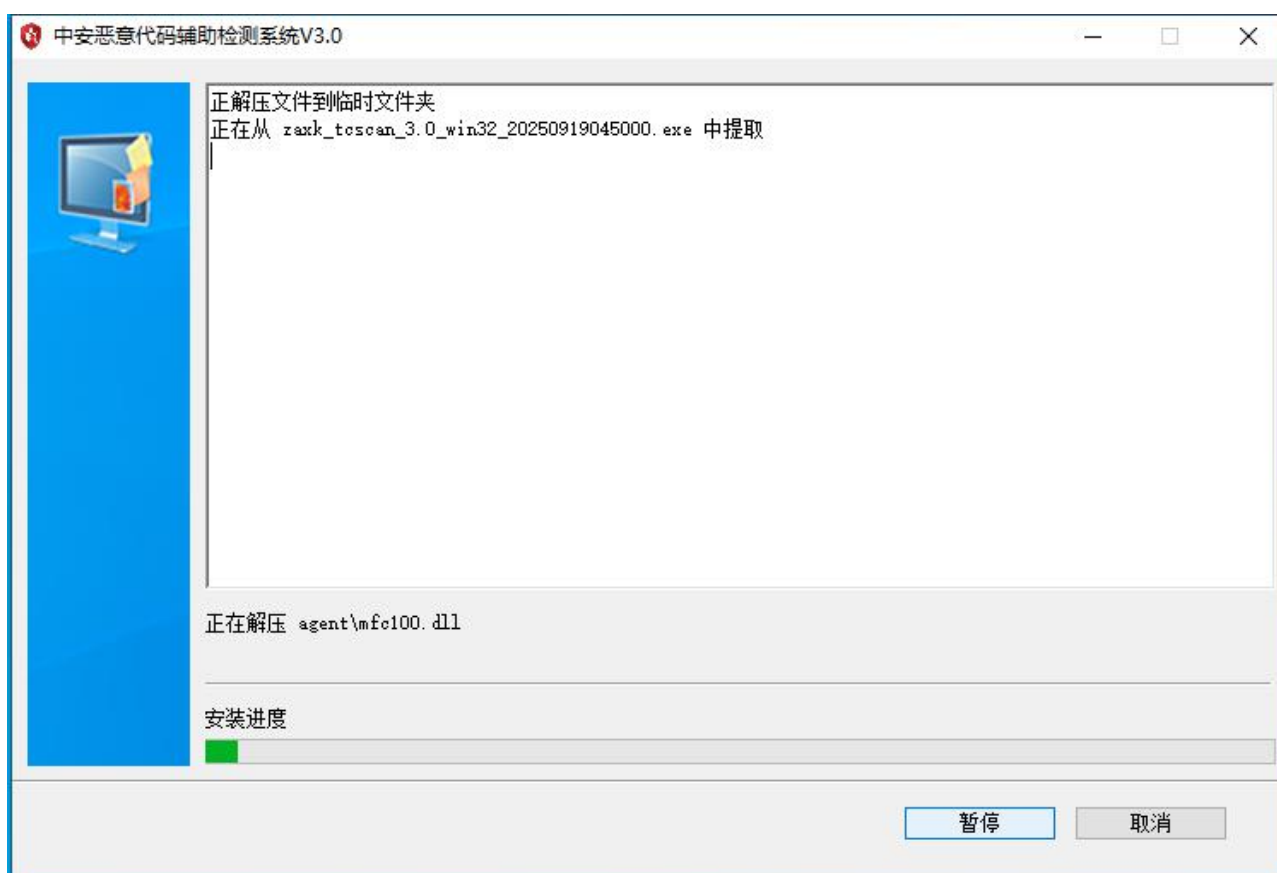
双击后缀为 exe 的安装程序，点击“接受”用户许可协议；

名称

-  signed_hm_tcscan_3.0_amd64_20241206.deb
-  signed_hm_tcscan_3.0_arm64_20241206.deb
-  signed_hm_tcscan_3.0_loongarch64_20241206.deb
-  signed_hm_tcscan_3.0_mips64el_20241206.deb
-  signed_hm_tcscan_3.0_win32_20241211.exe 双击安装



程序释放到临时文件夹中,等待进度完成;



点击“开始安装”按钮后,点击“确定”,软件开始安装;



软件安装完成后，勾选“立即重启”按钮后，点击“安装完成”重启电脑。

特别说明：软件安装完成后必须重启操作系统，否则无法正常打开软件。



(2) 国产系统软件安装

所有国产系统的软件安装包均为 deb 格式，双击对应的 deb 安装包就行。

一般 Intel、AMD、兆芯和海光处理器选择 amd64 的 deb 安装包安装，飞腾、鲲鹏、麒麟等处理器选择 arm64 的 deb 安装包安装，龙芯 3A5000 的处理器选择 loongaarch64 的 deb 安装包安装，龙芯 3A3000 和 3A4000 的处理器选择 mips64el 的 deb 安装包进行安装。



点击“一键安装”，输入系统登录的开机密码后，点击“授权按钮”；



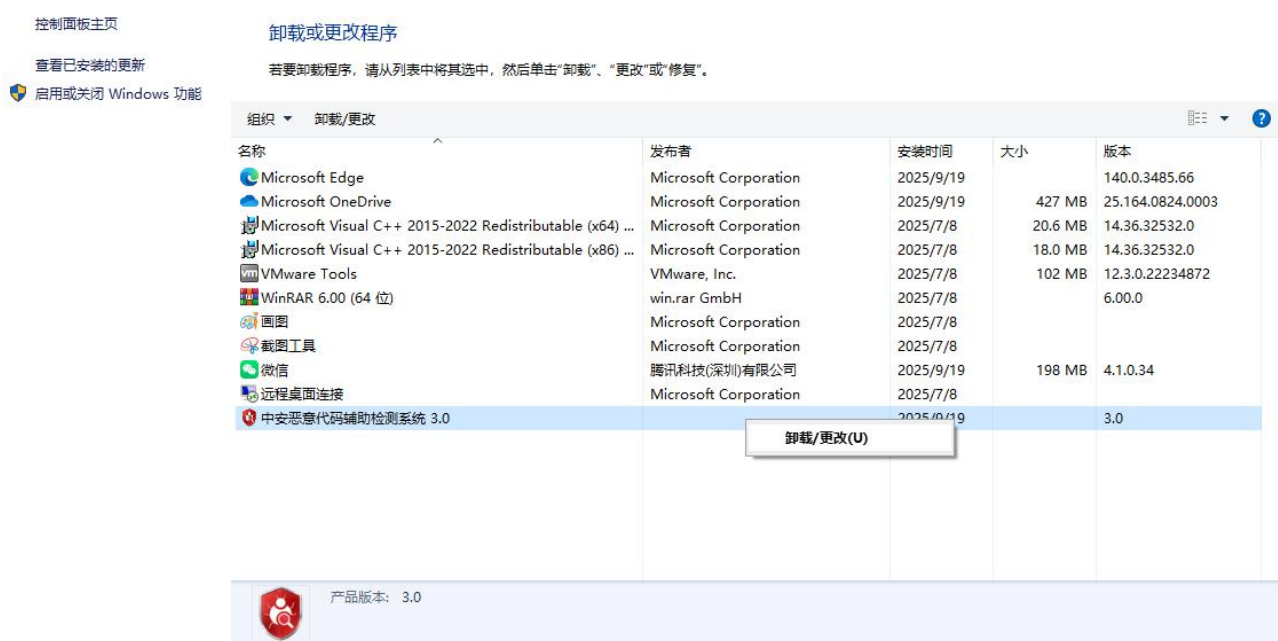
安装程序正在安装中，稍等片刻提示安装完成。



4.2 软件卸载

(1) Windows 系统软件卸载

方法一：在控制面板中找到软件后鼠标右键点击“卸载/更改”；



点击“立即卸载”，提示需要输入卸载密码，使用 sysadmin 账户登录点击“卸载”获取卸载密码或者向厂家获取卸载码后输入进去点击“下一步”即可完成卸载。



方法二：使用 sysadmin 账户登录软件，点击“卸载”；



勾选“直接卸载”复选框，最后点击“确定”按钮；在弹出的“确认直接卸载”对话框中点击“确定”，完成软件卸载。



(2) 国产系统软件卸载

方法一：单击左下角按钮，找到软件名称后点击鼠标右键，点击“卸载”；在弹窗中点击“卸载”。



输入管理员系统登录密码后点击“授权”，软件正在卸载中，稍等片刻软件卸载完成。



方法二：右键桌面空白地方，点击“打开终端”，在终端窗口中输入命令 `sudo dpkg -P tcscan` 后回车，输入管理员账户登录密码后回车，稍等片刻软件卸载完成。



五、系统登录

Windows 系统或国产系统直接双击桌面软件图标打开程序，程序登录主界面如下图所示。

系统内置 3 个用户，对应的用户名和默认密码如下：

- | | | |
|--------------|----------|-------------|
| (1) 系统管理员： | sysadmin | sysadmin001 |
| (2) 安全保密管理员： | secadmin | secadmin001 |
| (3) 安全审计员： | audadmin | audadmin001 |

注意：密码连续输入 5 次错误后系统自动锁定，系统锁定时间为十分钟。



六、系统管理员登录操作

6.1 密码修改

使用系统管理员 sysadmin 账户登录系统后，在主界面右上角点击“系统管理员”或旁边的图标，可以修改账户登录密码。

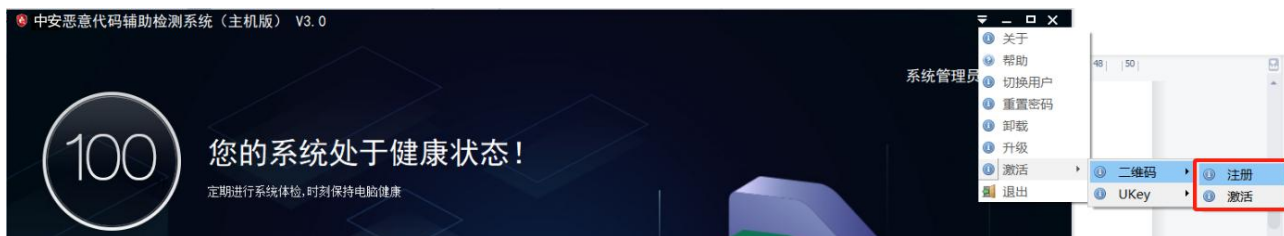


6.2 软件激活

软件激活有 2 种方式，可以通过二维码或授权 key 的方式，在主界面点击倒三角按钮，点击“激活”。



(1) 二维码激活



先点击“注册”按钮，出现如下图所示界面，输入单位名称、地址、联系人、电话和邮箱后点击“确定”，服务期限默认为 3 年（1095 天）。



点击确定后，出现如下图所示的二维码，将二维码或字符串发送给经销商，

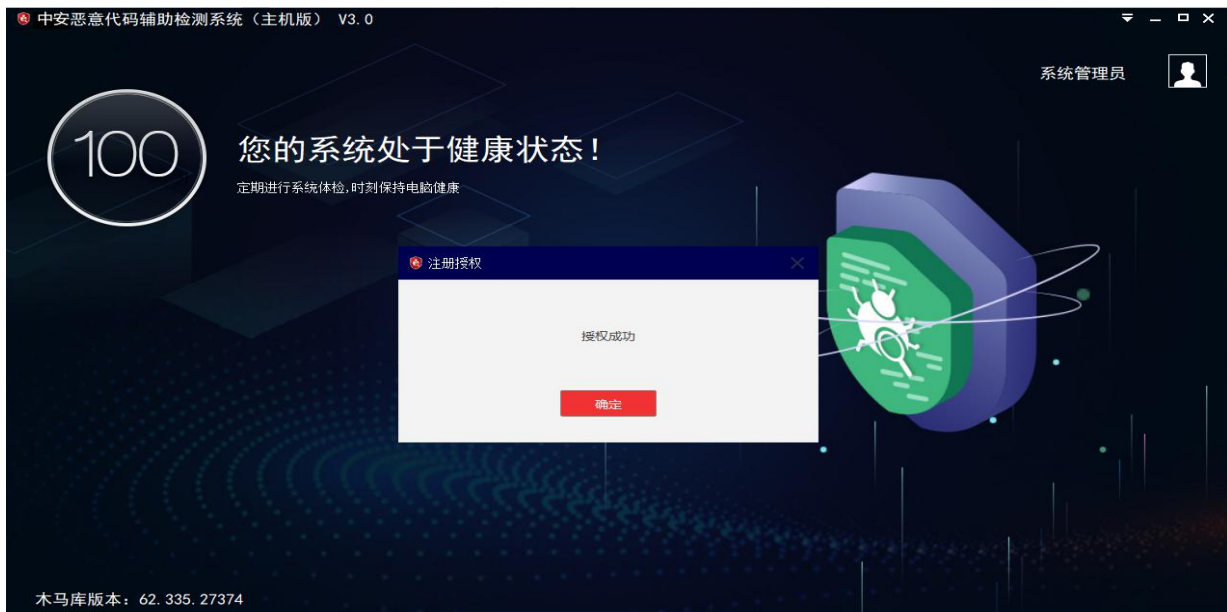
经销商会提供一串位授权码。



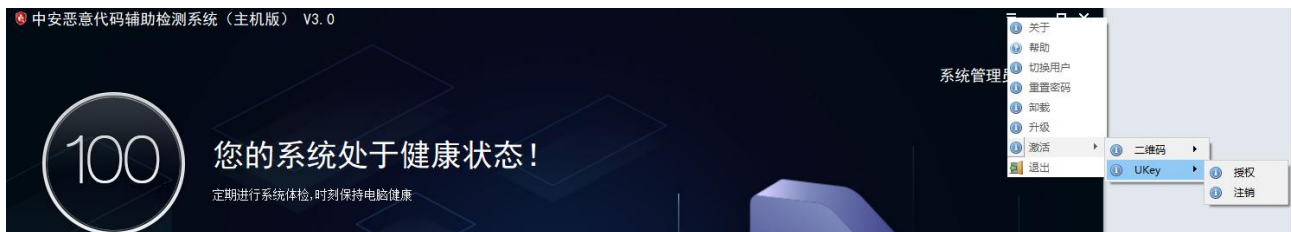
再次点击“激活”——“二维码”——“激活”，在弹出的注册窗口输入 8 位授权码后点击“确定”，完成软件激活。



软件授权成功后，“试用版”字样变成木马库版本。



(2) UKey 激活



插入软件授权 UKey，然后点击“激活”---“UKey”---“授权”，最后点击“确定”按钮完成软件激活。



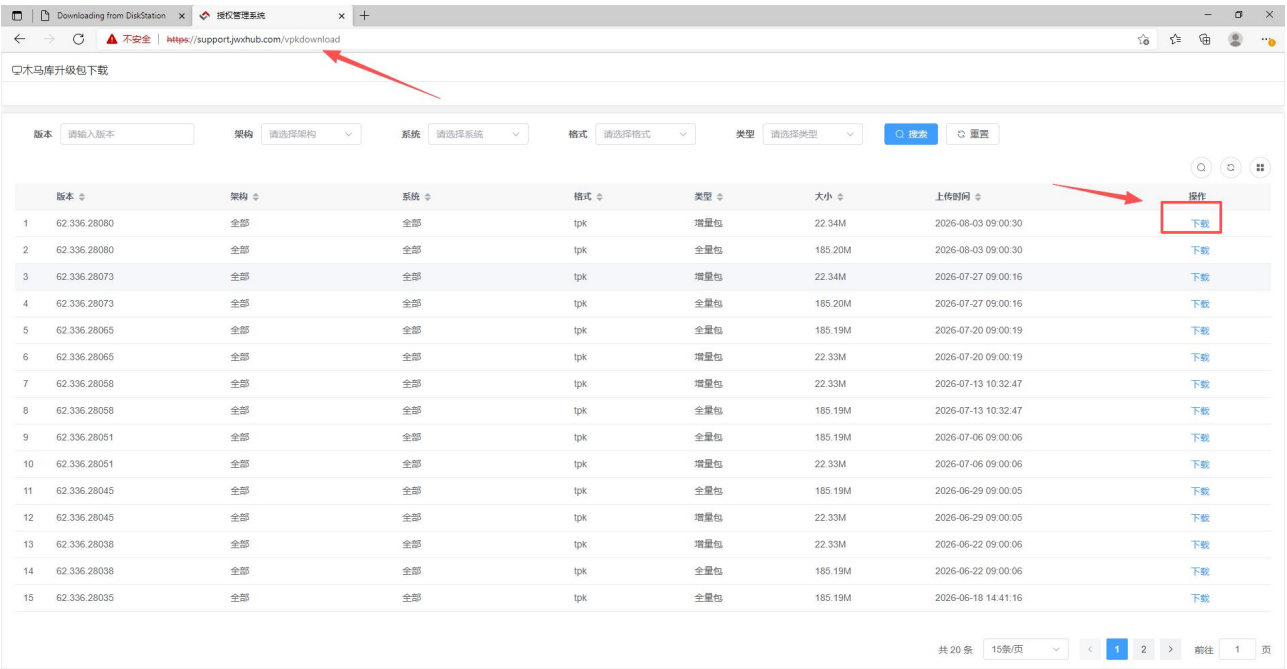
插入软件授权 UKey，然后点击“激活”---“UKey”---“注销”，最后点

击“确定”按钮完成软件授权回收。



6.3 木马库更新

在浏览器中输入 <https://support.jwxhub.com/vpkdownload> 在浏览器中下载最新的木马库。



在主界面点击“升级”；

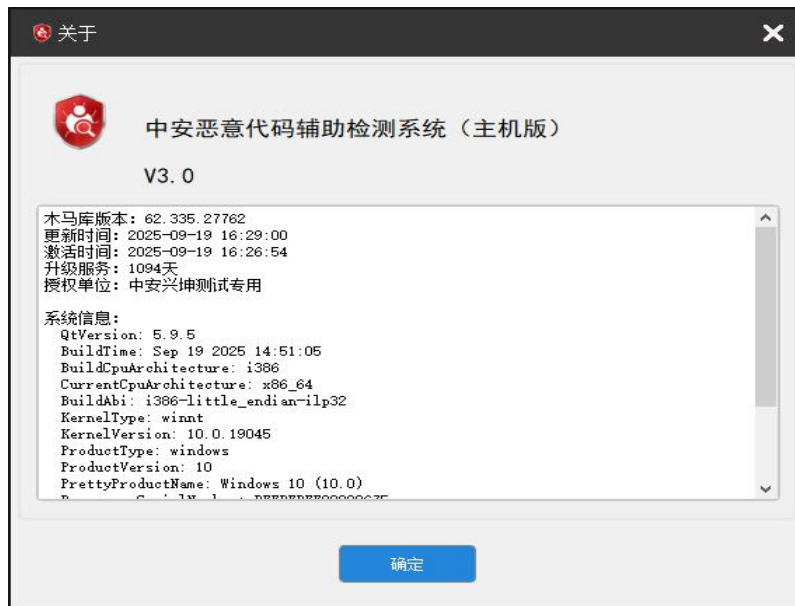


选择下载的最新的木马库，点击“确定”完成木马库升级更新。



升级完成点击“确定”重新登录软件，点击“关于”可查看木马库版本。





七、安全保密管理员登录操作

7.1 密码修改

使用安全保密管理员 secadmin 账户登录系统后，在主界面右上角点击“安全保密管理员”或旁边的图标，可以修改账户登录密码。



7.2 木马扫描

点击主界面中的“木马扫描”，可进行“快速扫描”、“全盘扫描”和“自定义扫描”。



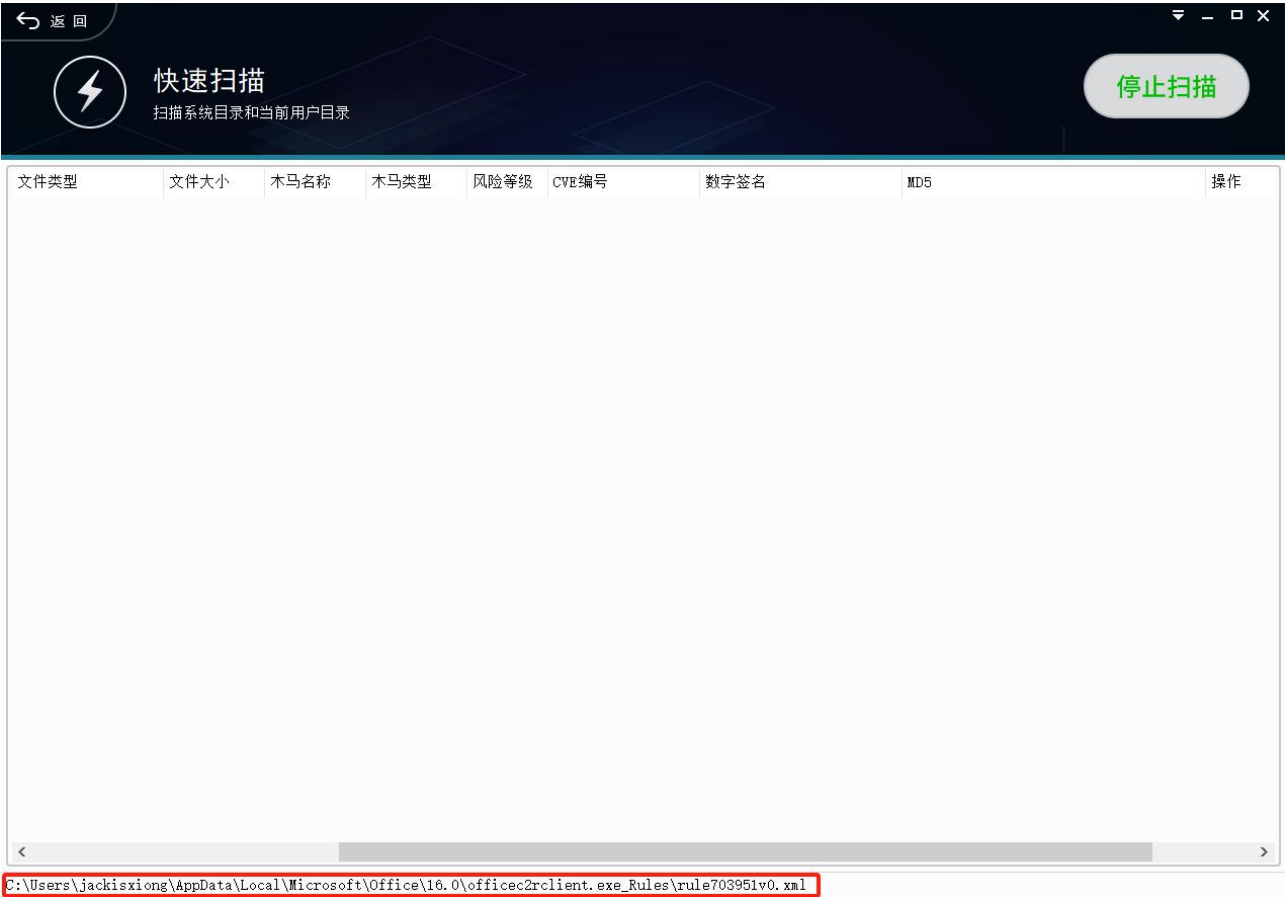
7.2.1 快速扫描

点击“木马扫描”主界面右上角的“立即扫描”或者点击“快速扫描”后跳转到“快速扫描”界面点击右上角的“立即扫描”。

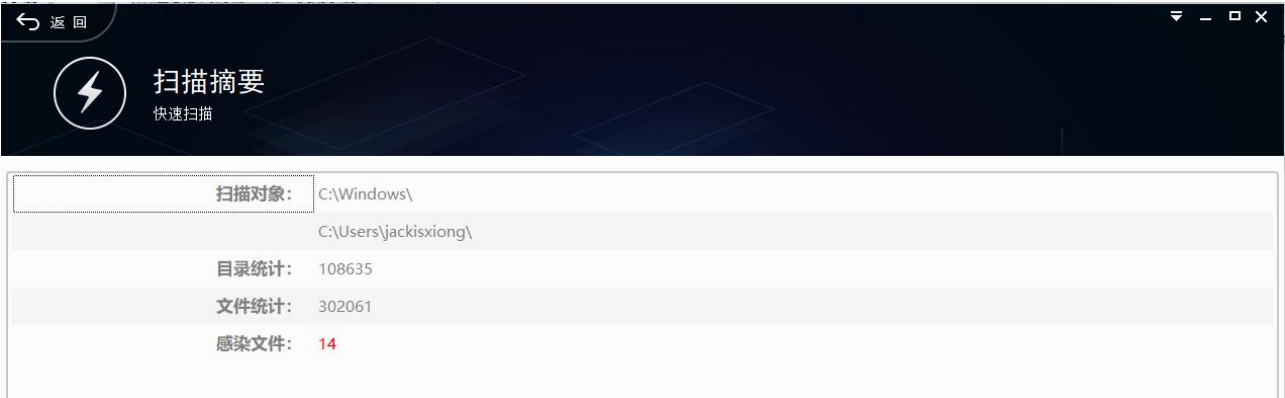


快速扫描可以扫描系统目录和当前用户目录文件，可以查看文件名、文件类型、文件大小、木马名称、木马类型、风险等级、CVE 编号、数字签名、MD5、操作。

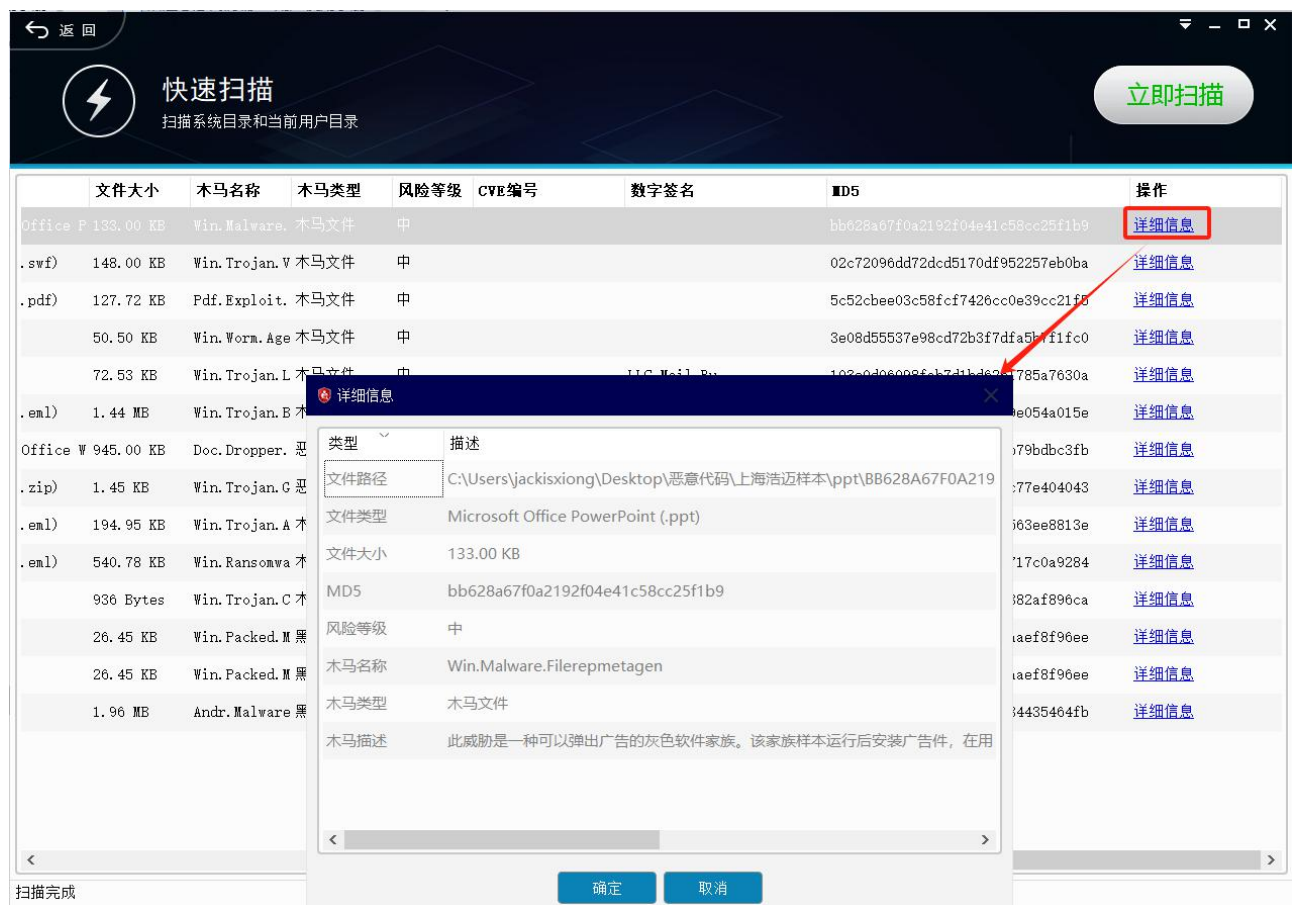
在扫描过程中，用户可以通过扫描状态栏看到当前正在检测的位置，以及检测的实时信息。



扫描结束后自动跳转到状态栏并显示摘要，包括扫描对象、目录统计、文件统计、感染文件等。



点击“返回”按钮，可以查看文件感染木马详细信息。



7.2.2 全盘扫描

点击“木马扫描”主界面的“全盘扫描”后跳转到“全盘扫描”界面，再次点击右上角的“立即扫描”。



全盘扫描可以扫描系统所有硬盘分区文件，可以查看文件名、文件类型、文件大小、木马名称、木马类型、风险等级、CVE 编号、数字签名、MD5、操作。

时间	文件名	文件类型	文件大小	木马名称	木马类型	风险等级	CVE编号	数字签名
2024-12-13 13:10:52	C:\Users\jackisxiong\Desktop\恶意代码\PDF 文件 (.pdf)		127.72 KB	Pdf.Exploit.	木马文件	中		
2024-12-13 13:22:45	D:\驱动和补丁\打印机驱动\pantum_p3010_CL_TYPE_MSEXE	CL_TYPE_MSEXE	10.47 MB	Win.Worm.Aut	木马文件	中		温州市驱动
2024-12-13 13:28:57	E:\工作(参考)\已完成: 郑州航院保密档案\CL_TYPE_MSEXE	CL_TYPE_MSEXE	702.00 KB	Win.Trojan.F	木马文件	中		

E:\管理工具\4. 选装软件\AutoCAD2007简体中文版\Bin\acadFeui\Program Files\Root\csp16.dll

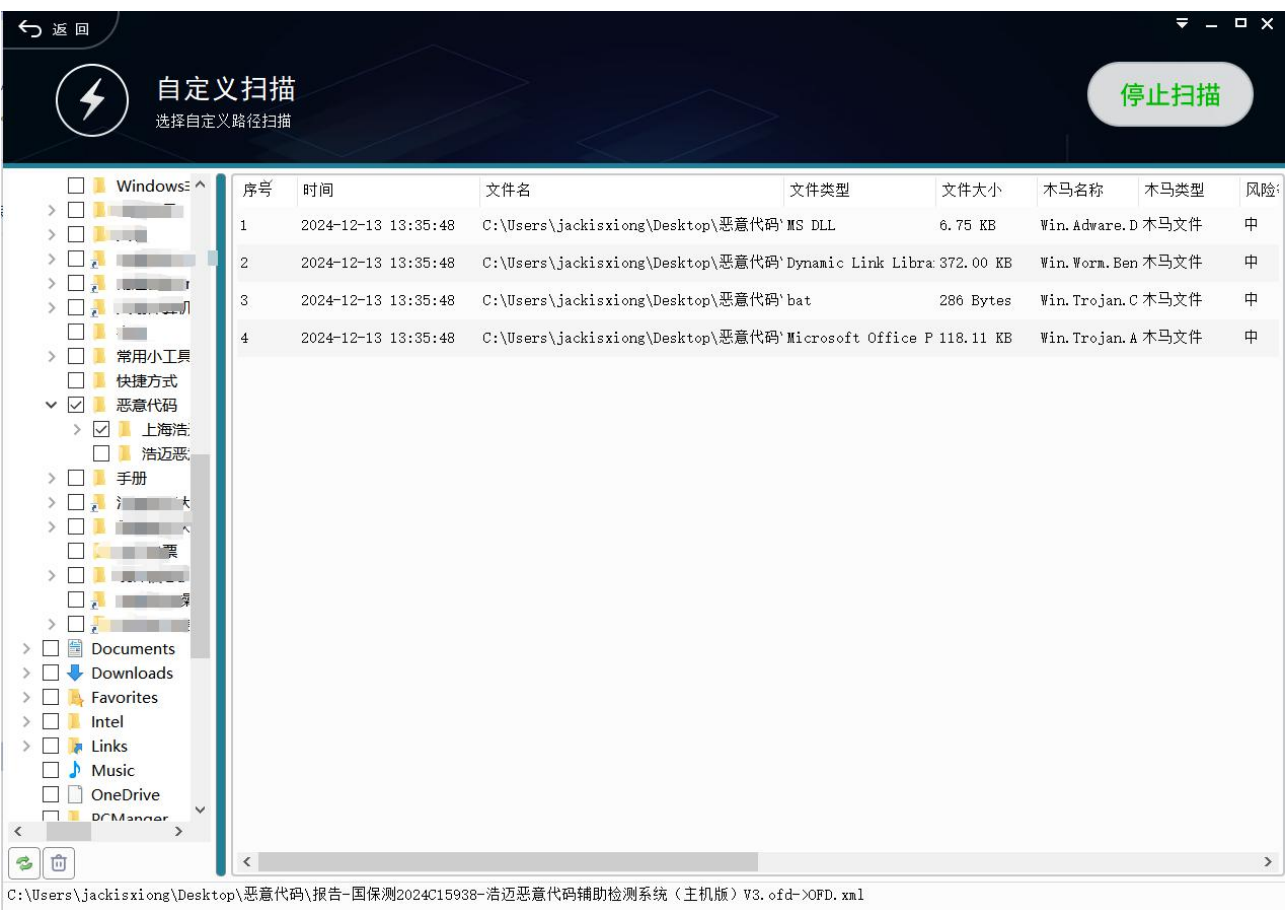
扫描结束后自动跳转到状态栏并显示摘要，包括扫描对象、目录统计、文件统计、感染文件等。

扫描对象:	C:\
	D:\
	E:\
	F:\
	G:\
	H:\
	I:\
目录统计:	180348
文件统计:	821589
感染文件:	4

7.2.3 自定义扫描

点击“木马扫描”主界面的“自定义扫描”后跳转到“自定义扫描”界面，选择左侧目录的带扫描文件或文件夹，再次点击右上角的“立即扫描”

开始自定义扫描。



扫描结束后自动跳转到状态栏并显示摘要，包括扫描对象、目录统计、文件统计、感染文件等。



7.3 安全检查

点击主界面中的“安全检查”，可查看“基本信息”和进行“辅助检测”。



7.3.1 基本信息

(1) 系统信息

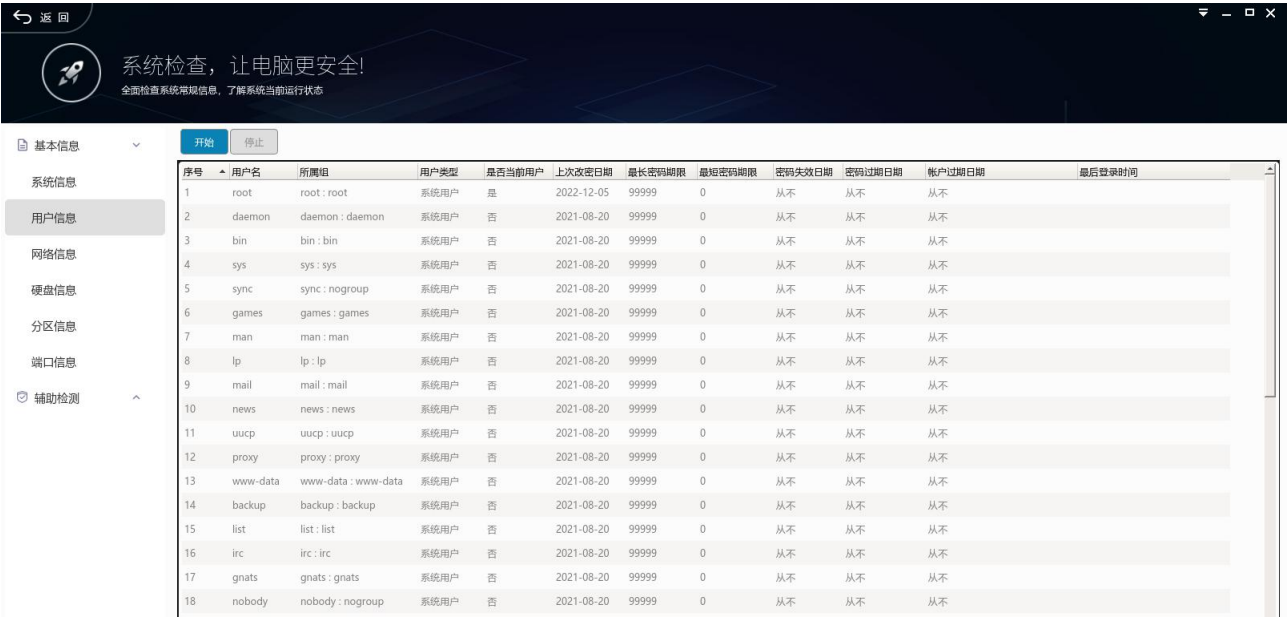
选中“系统信息”，点击“开始”可以查看系统名称、系统版本、内核版本、产品名、系统位数、计算机名、系统安装时间、安装路径、制造商和描述。





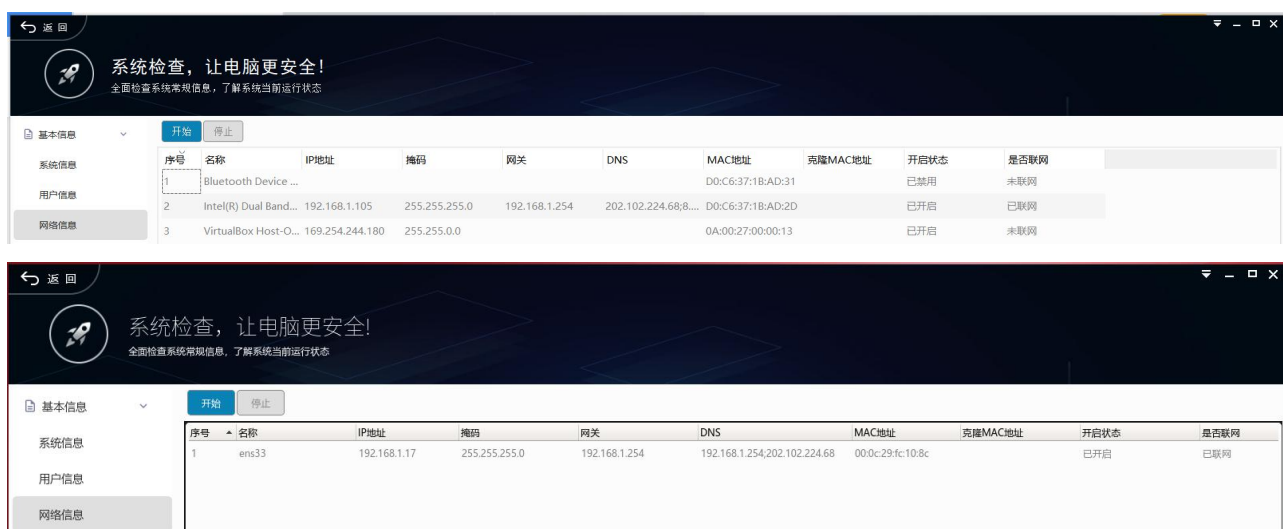
(2) 用户信息

选中“用户信息”，点击“开始”可以检查主机的用户名、所属组、用户类型、是否当前用户、上次改密日期、最长密码期限、最短密码期限、密码警告期限、密码失效日期、密码过期日期、帐户过期日期、最后登录时间。



(3) 网络信息

选中“网络信息”，点击“开始”可以检查主机网卡的名称、IP 地址、掩码、网关、DNS、MAC 地址、克隆 MAC 地址、开启状态和是否联网。



(4) 网络信息

选中“网络信息”，点击“开始”可以检查主机磁盘的名称、序列号、容量大小、厂商、型号、是否可移动、是否只读、启动次数、累计使用时间（小时）和状态。



(5) 分区信息

选中“分区信息”，点击“开始”可以检查主机的硬盘信息，包括：硬盘、分区、文件系统、标签名、大小、是否可移动、是否只读、挂载点和分区类型（正常分区、隐藏分区、加密分区或虚拟分区等）。

系统检查，让电脑更安全！ 全面检查系统常规信息，了解系统当前运行状态									
返回 系统检查，让电脑更安全！ 全面检查系统常规信息，了解系统当前运行状态 基本信息 开始 停止									
序号	硬盘	分区	文件系统	标签名	大小	是否可移动	是否只读	分区类型	
1	aigo NVMe SSD P7000Z 2TB	C:\	NTFS	Win10	407.00 GB	否	否	正常分区	
2	aigo NVMe SSD P7000Z 2TB	D:\	NTFS	软件	300.00 GB	否	否	正常分区	
3	aigo NVMe SSD P7000Z 2TB	E:\	NTFS	军工保密	300.00 GB	否	否	正常分区	
4	aigo NVMe SSD P7000Z 2TB	F:\	NTFS	资质申请	200.00 GB	否	否	正常分区	
5	aigo NVMe SSD P7000Z 2TB	H:\	NTFS	国产化	400.42 GB	否	否	正常分区	
6	aigo NVMe SSD P7000Z 2TB	G:\	NTFS	其他	299.00 GB	否	否	正常分区	
7	aigo NVMe SSD P7000Z 2TB	I:\			1.00 GB	否	否	加密分区	
8	aigo NVMe SSD P7000Z 2TB				300.00 MB			隐藏分区	
9	aigo NVMe SSD P7000Z 2TB				16.00 MB			隐藏分区	

系统检查，让电脑更安全！ 全面检查系统常规信息，了解系统当前运行状态									
返回 系统检查，让电脑更安全！ 全面检查系统常规信息，了解系统当前运行状态 基本信息 开始 停止									
序号	硬盘	分区	文件系统	标签名	大小	是否可移动	是否只读	分区类型	
1	sda	sda1	ext4	SYSBOOT	1G	否	否	正常分区	
2	sda	sda2			1K	否	否	扩展分区	
3	sda	sda5	ext4	SYSROOT	100G	否	否	正常分区	
4	sda	sda6	ext4	KYLIN-BACKUP	22.2G	否	否	隐藏分区	
5	sda	sda7	ext4	DATA	69.7G	否	否	正常分区	
6	sda	sda8	swap	SWAP	7.1G	否	否	隐藏分区	

(6) 端口信息

选中“端口信息”，点击“开始”可以检查系统端口的协议、本地 IP、本地端口、远程 IP、远程端口、端口状态、进程 ID、进程名称、进程路径和发行商。

返回

系统检查，让电脑更安全！
全面检查系统常规信息，了解系统当前运行状态

基本信息

开始

停止

系统信息

用户信息

网络信息

硬盘信息

分区信息

端口信息

辅助检测

序号	协议	本地IP	本地端口	远程IP	远程端口	端口状态	进程ID	进程名	进程路径	发行商
1	TCP	0.0.0.0	135	0.0.0.0	0	侦听	1256			
2	TCP	0.0.0.0	445	0.0.0.0	0	侦听	4			
3	TCP	0.0.0.0	902	0.0.0.0	0	侦听	6896	vmware-authd.exe	D:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe	VMware, Inc.
4	TCP	0.0.0.0	912	0.0.0.0	0	侦听	6896	vmware-authd.exe	D:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe	VMware, Inc.
5	TCP	0.0.0.0	1688	0.0.0.0	0	侦听	6788	kms-renewal.exe	C:\Windows\system32\kms-renewal.exe	
6	TCP	0.0.0.0	3306	0.0.0.0	0	侦听	6292			
7	TCP	0.0.0.0	3389	0.0.0.0	0	侦听	1636			
8	TCP	0.0.0.0	5040	0.0.0.0	0	侦听	10728			
9	TCP	0.0.0.0	7880	0.0.0.0	0	侦听	12060			
10	TCP	0.0.0.0	47546	0.0.0.0	0	侦听	5124			
11	TCP	0.0.0.0	49664	0.0.0.0	0	侦听	1000			
12	TCP	0.0.0.0	49665	0.0.0.0	0	侦听	924			
13	TCP	0.0.0.0	49666	0.0.0.0	0	侦听	1028			
14	TCP	0.0.0.0	49667	0.0.0.0	0	侦听	1996			
15	TCP	0.0.0.0	49668	0.0.0.0	0	侦听	3208			
16	TCP	0.0.0.0	49669	0.0.0.0	0	侦听	5124			
17	TCP	0.0.0.0	49696	0.0.0.0	0	侦听	992			
18	TCP	127.0.0.1	1001	0.0.0.0	0	侦听	4			
19	TCP	127.0.0.1	3443	0.0.0.0	0	侦听	6660			
20	TCP	127.0.0.1	5283	0.0.0.0	0	侦听	2196	SGTool.exe	D:\Program Files (x86)\Sogou\input\14.10.0.1161\SGTool.exe	Sogou.com

返回

系统检查，让电脑更安全!

全面检查系统规范信息，了解系统当前运行状态

基本信息

系统信息

用户信息

网络信息

硬盘信息

分区信息

端口信息

辅助检测

开始

停止

序号	协议	本地IP	本地端口	远程IP	远程端口	端口状态	进程ID	进程名	进程路径	发行商
1	tcp	0.0.0.0	445	0.0.0.0	0	侦听	1354	smbd		
2	tcp	0.0.0.0	139	0.0.0.0	0	侦听	1354	smbd		
3	tcp	0.0.0.0	8751	0.0.0.0	0	侦听	785	kyseclogd		
4	tcp	127.0.0.53	53	0.0.0.0	0	侦听	788	systemd-resolve		
5	tcp	0.0.0.0	22	0.0.0.0	0	侦听	1086	sshd: /usr/sbi		
6	tcp	127.0.0.1	631	0.0.0.0	0	侦听	820	cupsd		
7	udp	127.0.0.53	53	0.0.0.0	0		788	systemd-resolve		
8	udp	192.168.1.255	137	0.0.0.0	0		1002	nmbd		
9	udp	192.168.1.17	137	0.0.0.0	0		1002	nmbd		
10	udp	0.0.0.0	137	0.0.0.0	0		1002	nmbd		
11	udp	192.168.1.255	138	0.0.0.0	0		1002	nmbd		
12	udp	192.168.1.17	138	0.0.0.0	0		1002	nmbd		
13	udp	0.0.0.0	138	0.0.0.0	0		1002	nmbd		
14	udp	0.0.0.0	4500	0.0.0.0	0		1107	charon		
15	udp	0.0.0.0	500	0.0.0.0	0		1107	charon		
16	udp	0.0.0.0	55865	0.0.0.0	0		814	avahi-daemon: r		
17	udp	0.0.0.0	5353	0.0.0.0	0		814	avahi-daemon: r		
18	udp	0.0.0.0	1701	0.0.0.0	0		1115	xl2tpd		

7.3.2 辅助检测

(1) IE 加载项

选中“IE 加载项”，点击“开始”可以浏览器插件文件、产品名、版本和公司名。

返回

系统检查，让电脑更安全！
全面检查系统常规信息，了解系统当前运行状态

基本信息

辅助检测

IE加载项

SPI信息

计划任务

文件关联

Hosts检查

SSDT检查

开始

停止

序号	文件	产品名	版本	公司名
1	D:\软件\000常用软件\百度云破解下载限制\IDM v6.38.7.2 中文绿色特别版\IDM\IDMIECC.dll	Internet Download Manager Module	6, 38, 2, 1	Internet Download Manager, Tonec Inc.
2	C:\Windows\SysWow64\ABCCECom.ocx	ABCCECom.ocx	1, 0, 11, 222	Feitian Technologies Co., Ltd.
3	C:\Program Files (x86)\Microsoft\Edge\Application\131.0.2903.86\BHO\ie_to_edge_bho.dll	IEToEdge BHO	131.0.2903.86	Microsoft Corporation
4	C:\Windows\SysWow64\WebOA.ocx	iWebOA 插件	6.0.0.45	国泰新点软件股份有限公司
5	C:\Windows\SysWow64\Macromed\Flash\Flash32_34_0_0_282.ocx	Shockwave Flash	34,0,0,282	Adobe
6	C:\Users\jackson\AppData\Roaming\Tencent\QQ\QQAntiPhishing\AccountProtect.dll	QQ帐号保护	2.0.6.140	Tencent
7	D:\Program Files (x86)\Thunder Network\Thunder\Thunder BHO Platform\np_idieplat.dll	迅雷BHO平台	2.6.0.1046	深圳市迅雷网络技术有限公司
8	C:\Windows\Downloaded Program Files\JQGRID-1.OCX		1.1.0.50	
9	D:\软件\000常用软件\百度云破解下载限制\IDM v6.38.7.2 中文绿色特别版\IDM\IDMIECC.dll	Internet Download Manager Module	6, 38, 2, 1	Internet Download Manager, Tonec Inc.
10	C:\Windows\SysWow64\ABCCECom.ocx	ABCCECom.ocx	1, 0, 11, 222	Feitian Technologies Co., Ltd.
11	C:\Program Files (x86)\Microsoft\Edge\Application\131.0.2903.86\BHO\ie_to_edge_bho.dll	IEToEdge BHO	131.0.2903.86	Microsoft Corporation
12	C:\Windows\SysWow64\WebOA.ocx	iWebOA 插件	6.0.0.45	国泰新点软件股份有限公司
13	C:\Windows\SysWOW64\mshtml.dll	Internet Explorer	11.00.19041.2546 (WinB...	Microsoft Corporation
14	%SystemRoot%\System32\msxml3.dll			
15	C:\Program Files (x86)\BJCAClient\CertAppEnvV3.3.01.2144\Program\XTXAppCOM.dll	证书应用环境	3, 2, 0, 2	北京数字认证股份有限公司
16	D:\Program Files (x86)\Thunder Network\Thunder\BHO\ThunderAgent10.1.27.614.dll	迅雷	10, 1, 27, 614	深圳市迅雷网络技术有限公司
17	C:\Windows\SysWow64\abcPrintCtl4RA.dll	ABCPrintCtl4RA Module	1, 0, 0, 9	INFOSEC Tech. corp
18	C:\Windows\SysWow64\ABCCEBankSignCtrl.ocx	中国农业银行一代K宝签名控件	2.0.0.3	中国农业银行

(2) SPI 信息

选中“SPI 信息”，点击“开始”可以列出 SPI 服务的协议、文件、产品名、版本和公司名。

SPI 栏列举出检查到的系统中的网络服务,因为服务可能被用作进程木马。

序号	协议	文件	产品名	版本	公司名
1	MSAFD Tcpip [TCP/IP]	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
2	MSAFD Tcpip [UDP/IP]	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
3	MSAFD Tcpip [TCP/IPv6]	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
4	MSAFD Tcpip [UDP/IPv6]	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
5	AF_UNIX	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
6	RSVP TCPv6 服务提供商	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
7	RSVP TCP 服务提供商	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
8	RSVP UDPv6 服务提供商	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
9	RSVP UDP 服务提供商	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
10	Hyper-V RAW	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
11	MSAFD L2CAP [Bluetooth]	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
12	MSAFD RfComm [Bluetooth]	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
13	vSockets DGRAM	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation
14	vSockets STREAM	C:\Windows\system32\mswsock.dll	Microsoft? Windows? Operating System	10.0.19041.4522 (WinBuild.160101.0800)	Microsoft Corporation

注意: 正常 Windows 系统只有两个不同 DLL: mswsock.dll 和 rsvpsp.dll。

SPI (Service Provider Interface) 服务提供者接口是 Winsock 系统组件提供的面向系统底层的编程接口。所有 Windows 的网络作业都是通过这个接口发出和接收数据包的。通过检查 SPI, 可以检查通过接口的协议。

如果 Winsock 两项未损坏, 则“协议”下包含 10 个节, 节标头中将包括以下名称:

- MSAFD Tcpip [TCP/IP]
- MSAFD Tcpip [UDP/IP]
- RSVP UDP Service Provider
- RSVP TCP Service Provider
- MSAFD NetBIOS [\Device\NetBT_Tcpip...]
- MSAFD NetBIOS [\Device\NetBT_Tcpip...]
- MSAFD NetBIOS [\Device\NetBT_Tcpip...]
- MSAFD NetBIOS [\Device\NetBT_Tcpip...]
- MSAFD NetBIOS [\Device\NetBT_Tcpip...]
- MSAFD NetBIOS [\Device\NetBT_Tcpip...]

如果发现“协议”名称与此列表中的名称不同, 则表明 Winsock2 项已

损坏或者已安装了第三方加载项，可能为木马软件。

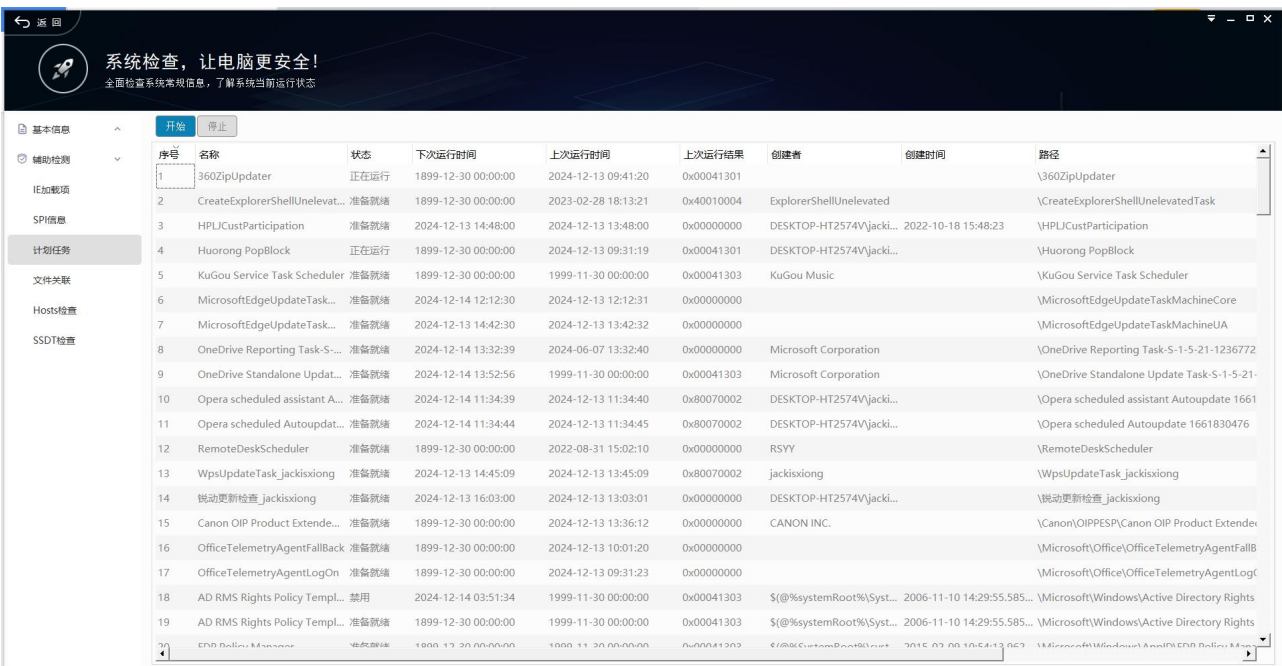
如果安装了第三方加载项，则加载项的名称将替换列表中的字母“MSAFD”。

如果列表中的节多于 10 个，则表明安装了第三方加载项。

用户可以通过检查 SPI 来查看是否安装第三方加载项，并确定是否为木马软件。

(3) 计划任务

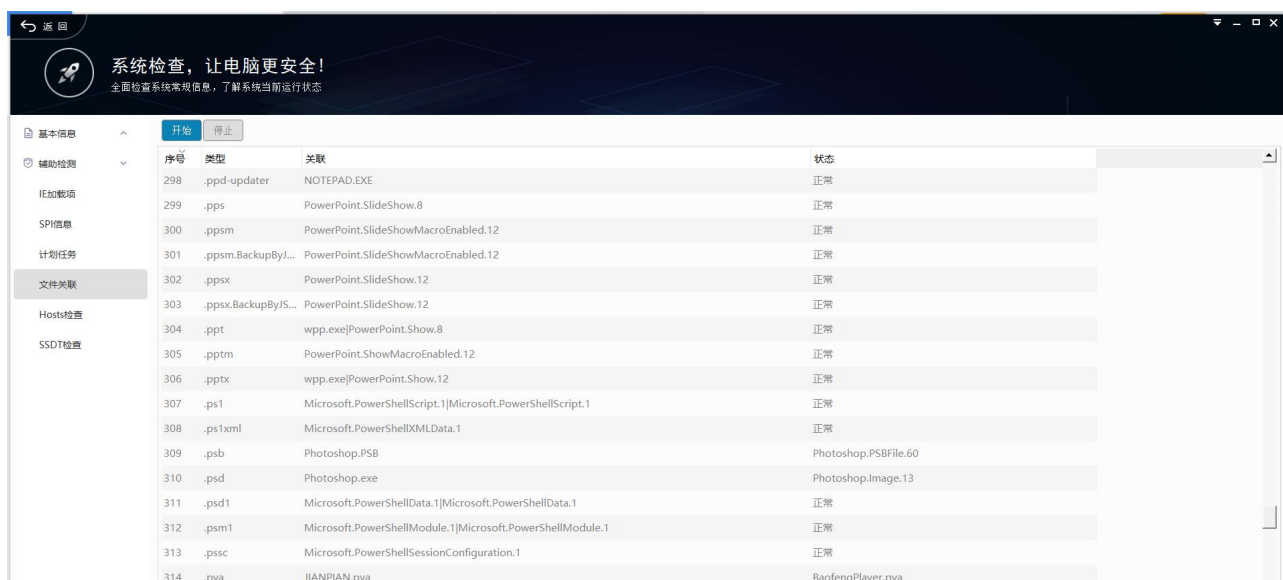
选中“计划任务”，点击“开始”可以列出电脑中所有的计划任务，包括名称、状态、下次运行时间、上次运行时间、上次运行结果、创建者、创建时间、路径。



序号	名称	状态	下次运行时间	上次运行时间	上次运行结果	创建者	创建时间	路径
1	360ZipUpdater	正在运行	1899-12-30 00:00:00	2024-12-13 09:41:20	0x00041301			\360ZipUpdater
2	CreateExplorerShellUnelevatedTask	准备就绪	1899-12-30 00:00:00	2023-02-28 18:13:21	0x00010004	ExplorerShellUnelevated		\CreateExplorerShellUnelevatedTask
3	HPLJCustParticipation	准备就绪	2024-12-13 14:48:00	2024-12-13 13:48:00	0x00000000	DESKTOP-HT2574V\jacki...	2022-10-18 15:48:23	\HPLJCustParticipation
4	Huorong PopBlock	正在运行	1899-12-30 00:00:00	2024-12-13 09:31:19	0x00041301	DESKTOP-HT2574V\jacki...		\Huorong PopBlock
5	KuGou Service Task Scheduler	准备就绪	1899-12-30 00:00:00	1999-11-30 00:00:00	0x00041303	KuGou Music		\KuGou Service Task Scheduler
6	MicrosoftEdgeUpdateTaskMachineCore	准备就绪	2024-12-14 12:12:30	2024-12-13 12:12:31	0x00000000			\MicrosoftEdgeUpdateTaskMachineCore
7	MicrosoftEdgeUpdateTaskMachineUA	准备就绪	2024-12-13 14:42:30	2024-12-13 13:42:32	0x00000000			\MicrosoftEdgeUpdateTaskMachineUA
8	OneDrive Reporting Task-S-1-5-21-1236772	准备就绪	2024-12-14 13:32:39	2024-06-07 13:32:40	0x00000000	Microsoft Corporation		\OneDrive Reporting Task-S-1-5-21-1236772
9	OneDrive Standalone Update Task-S-1-5-21-1236772	准备就绪	2024-12-14 13:52:56	1999-11-30 00:00:00	0x00041303	Microsoft Corporation		\OneDrive Standalone Update Task-S-1-5-21-1236772
10	Opera scheduled assistant Autoupdate 1661	准备就绪	2024-12-14 11:34:39	2024-12-13 11:34:40	0x80070002	DESKTOP-HT2574V\jacki...		\Opera scheduled assistant Autoupdate 1661
11	Opera scheduled Autoupdate 1661830476	准备就绪	2024-12-14 11:34:44	2024-12-13 11:34:45	0x80070002	DESKTOP-HT2574V\jacki...		\Opera scheduled Autoupdate 1661830476
12	RemoteDeskScheduler	准备就绪	1899-12-30 00:00:00	2022-08-31 15:02:10	0x00000000	RSYY		\RemoteDeskScheduler
13	WpsUpdateTask_jackisxiong	准备就绪	2024-12-13 14:45:09	2024-12-13 13:45:09	0x80070002	jackisxiong		\WpsUpdateTask_jackisxiong
14	锐动更新检查_jackisxiong	准备就绪	2024-12-13 16:03:00	2024-12-13 13:03:01	0x00000000	DESKTOP-HT2574V\jacki...		\锐动更新检查_jackisxiong
15	Canon OIP Product Extended Support	准备就绪	1899-12-30 00:00:00	2024-12-13 13:36:12	0x00000000	CANON INC.		\Canon\OIPPE\Canon OIP Product Extended Support
16	OfficeTelemetryAgentFallBack	准备就绪	1899-12-30 00:00:00	2024-12-13 10:01:20	0x00000000			\Microsoft\Office\OfficeTelemetryAgentFallBack
17	OfficeTelemetryAgentLogOn	准备就绪	1899-12-30 00:00:00	2024-12-13 09:31:23	0x00000000			\Microsoft\Office\OfficeTelemetryAgentLogOn
18	AD RMS Rights Policy Template	禁用	2024-12-14 03:51:34	1999-11-30 00:00:00	0x00041303	\$(@%systemRoot%\Syst...	2006-11-10 14:29:55.585...	\Microsoft\Windows\Active Directory Rights Management Services\AD RMS Rights Policy Template
19	AD RMS Rights Policy Template	准备就绪	1899-12-30 00:00:00	1999-11-30 00:00:00	0x00041303	\$(@%systemRoot%\Syst...	2006-11-10 14:29:55.585...	\Microsoft\Windows\Active Directory Rights Management Services\AD RMS Rights Policy Template

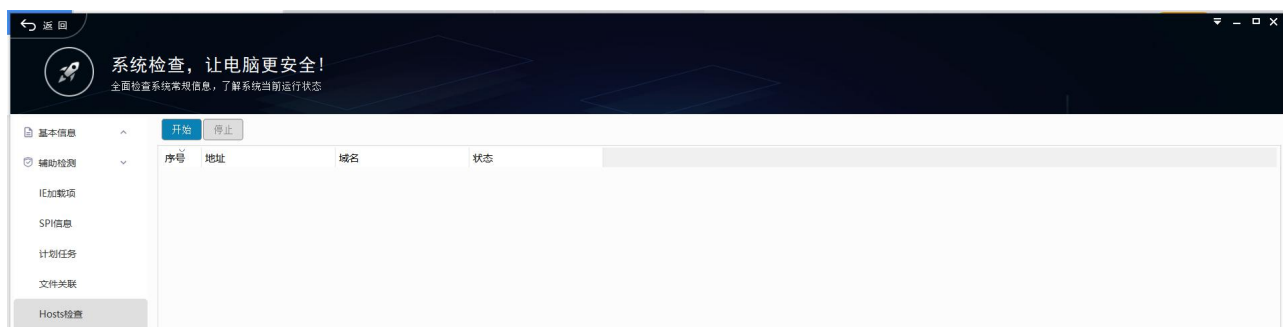
(4) 文件关联

选中“文件关联”，点击“开始”可以列出文件关联的分析情况，包括类型、关联和状态。



(5) Hosts 检查

选中“Hosts 检查”，点击“开始”可以列出主机 Host 的地址、域名和状态。



(6) SSDT 检查

选中“SSDT 检查”，点击“开始”可以列出 SSDT 检查的函数、文件地址、内存地址和文件路径。SSDT (System Services Descriptor Table) 检查是指对系统服务描述符表进行检查和维护的过程。

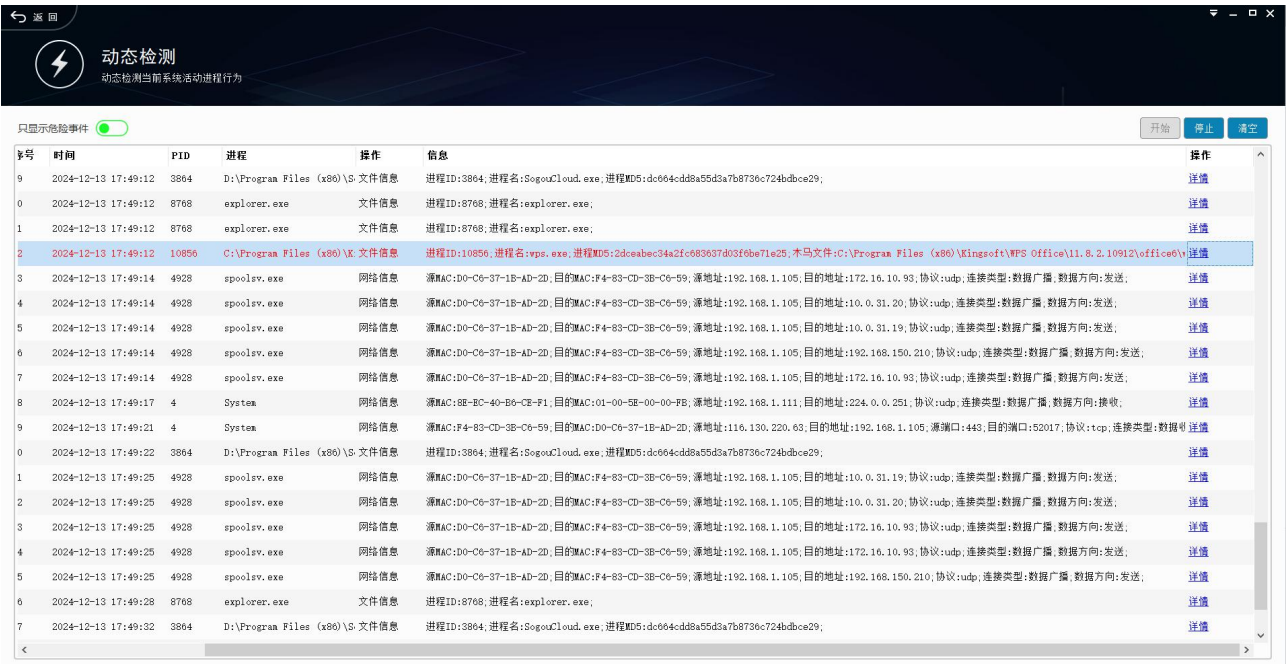


7.4 动态检测

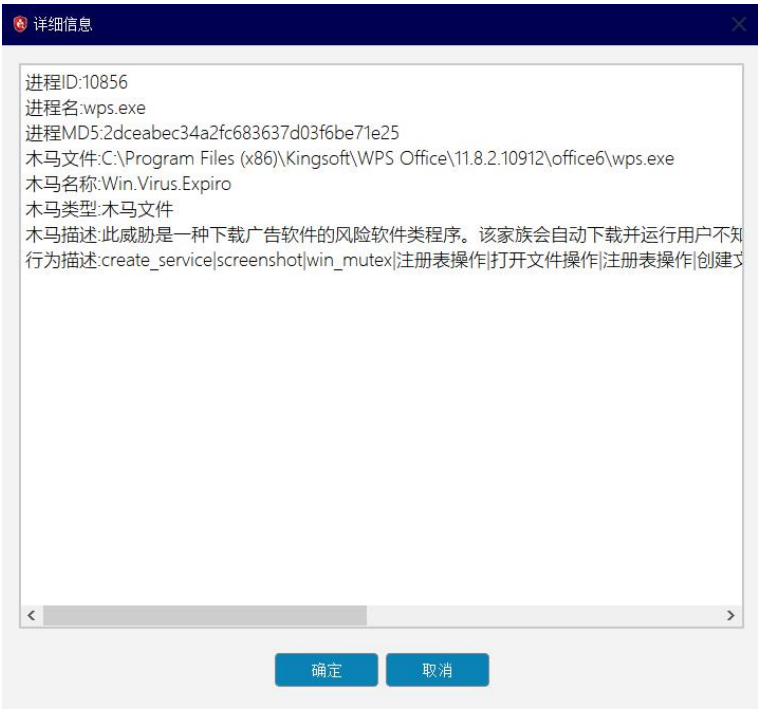
点击主界面中的“动态检测”，可以对主机的注册表、进程行为、网络行为和文件行为进行检测。



点击“开始检测”后跳转到动态检测页面，点击“开始”按钮进行检测，并将恶意信息显示出来。



点击“详情”，可以文件信息或网络信息等详细信息，标红的表示可能中了木马。



7.5 进程信息

点击主界面中的“进程信息”，可以查看当前活动进程内存映像的父进程 ID、进程 ID、进程名、路径、大小、修改时间、内核句柄数、用户句柄数、图形句柄数、线程数、所有者、数字签名、文件说明、文件版本、产品名称、公司名称、授权信息、操作（可点击查看模块、内存、关系和提取）。

返回

进程信息

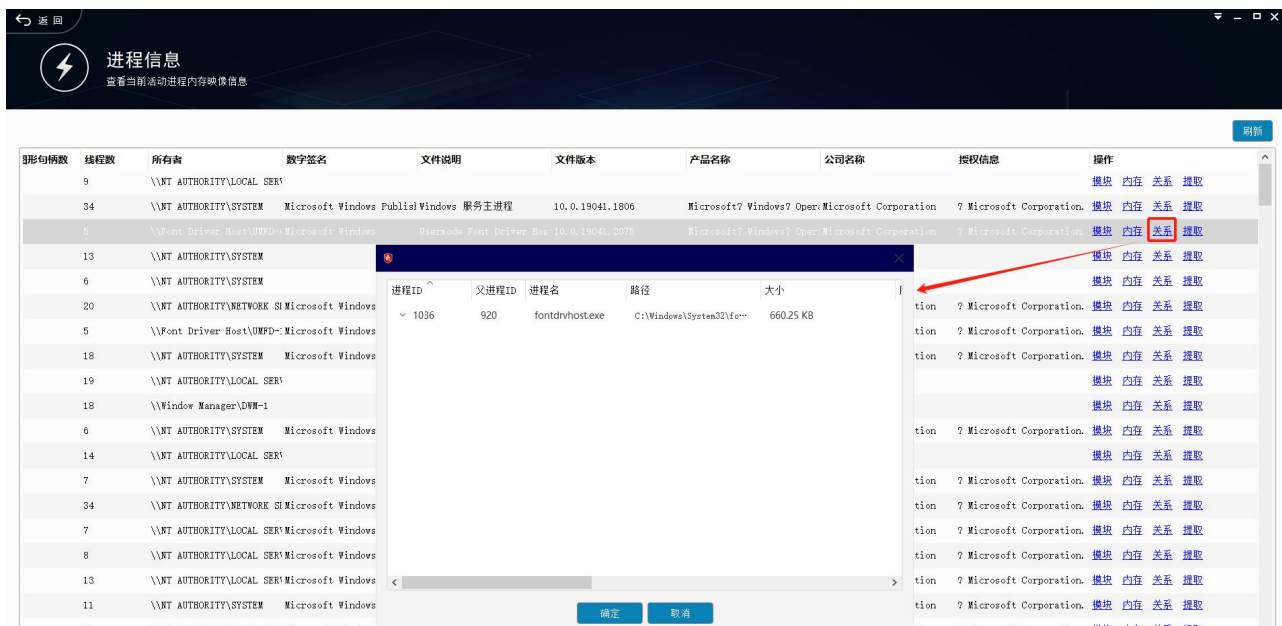
查看当前活动进程内存映像信息

图形句柄数	线程数	所有者	数字签名	文件说明	文件版本	产品名称	公司名称	授权信息	操作
9		\\NT AUTHORITY\LOCAL SER							模块 内存 关系 提取
34		\\NT AUTHORITY\SYSTEM	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
5		\\Font Driver Host\UNFD-	Microsoft Windows	Usermode Font Driver Hos	10.0.19041.2075	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
13		\\NT AUTHORITY\SYSTEM							模块 内存 关系 提取
6		\\NT AUTHORITY\SYSTEM							模块 内存 关系 提取
20		\\NT AUTHORITY\NETWORK SI	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
5		\\Font Driver Host\UNFD-	Microsoft Windows	Usermode Font Driver Hos	10.0.19041.2075	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
18		\\NT AUTHORITY\SYSTEM	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
19		\\NT AUTHORITY\LOCAL SER							模块 内存 关系 提取
18		\\Window Manager\DW-1							模块 内存 关系 提取
6		\\NT AUTHORITY\SYSTEM	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
14		\\NT AUTHORITY\LOCAL SER							模块 内存 关系 提取
7		\\NT AUTHORITY\SYSTEM	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
34		\\NT AUTHORITY\NETWORK SI	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
7		\\NT AUTHORITY\LOCAL SER	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
8		\\NT AUTHORITY\LOCAL SER	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
13		\\NT AUTHORITY\LOCAL SER	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
11		\\NT AUTHORITY\SYSTEM	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取
6		\\NT AUTHORITY\LOCAL SER	Microsoft Windows Publish	Windows 服务主进程	10.0.19041.1806	Microsoft? Windows? Oper	Microsoft Corporation	? Microsoft Corporation.	模块 内存 关系 提取

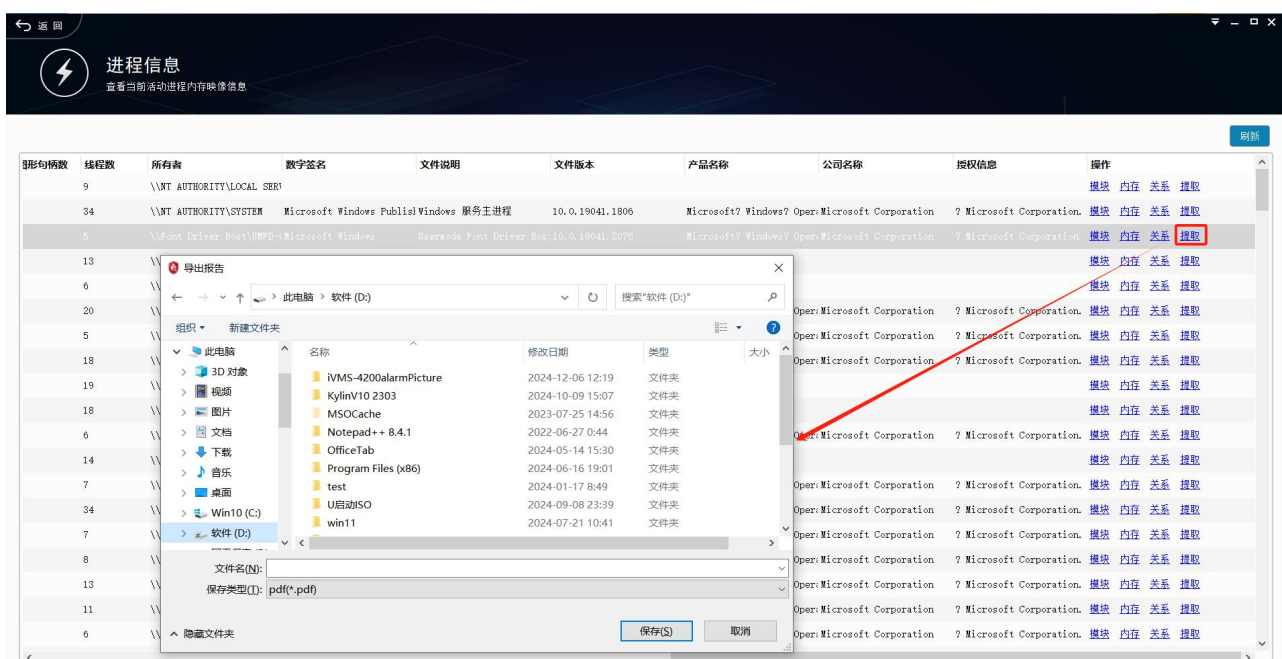
点击“内存”，可查看进程的地址、大小、标志、状态、类型和操作。



点击“关系”，可以查看进程 ID、父进程 ID、路径和大小。



点击“提取”，输入文件名和保存路径，可导出该进程的所有信息。



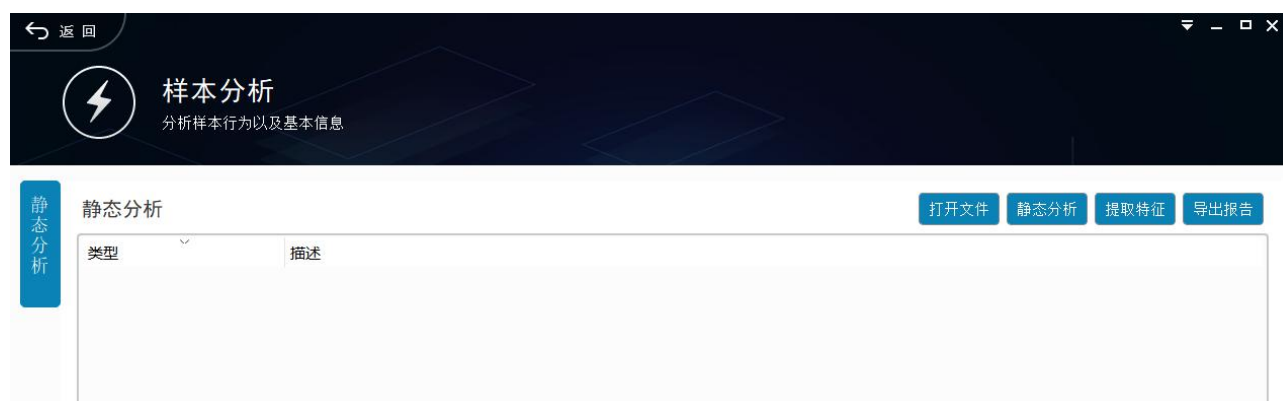
基本信息

基本信息

名称	描述
父进程ID	920
进程ID	1036
进程名	fontdrvhost.exe
路径	C:\Windows\System32\fontdrvhost.exe
大小	660.25 KB
修改时间	2022-12-28 00:20:13
内核句柄数	36
用户句柄数	0
图形句柄数	0
线程数	5
所有者	\\Font Driver Host\UMFD-0
数字签名	Microsoft Windows
文件说明	Usermode Font Driver Host
文件版本	10.0.19041.2075
产品名称	Microsoft? Windows? Operating System
公司名称	Microsoft Corporation
授权信息	? Microsoft Corporation. All rights reserved.

7.6 样本分析

点击主界面右侧的“样本分析”，可对选择的可执行 exe 程序样本进行静态分析。



点击“打开文件”，选择 exe 文件。

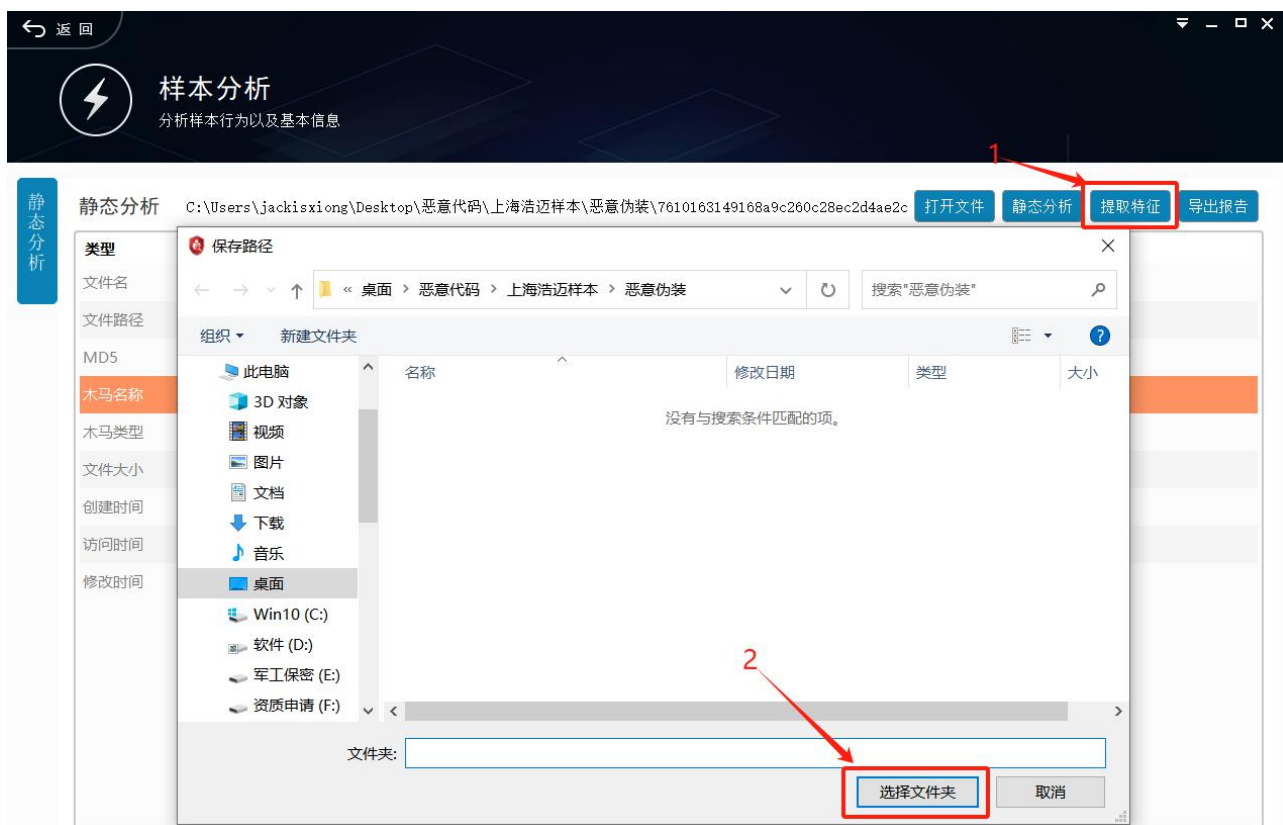


点击“静态分析”，可显示文件名、文件路径、MD5、木马名称、木马类型、文件大小、创建时间、访问时间和修改时间。



点击“提取特征”，选择需要保存的文件夹路径，即可保存后缀为 hts 的特征库。

20241213154854.HTS	2024-12-13 15:48	HTS 文件	4 KB
--------------------	------------------	--------	------



点击“导出报告”，输入文件名和保存路径，可导出格式为 xlsx 表格的报告。

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	类型	描述											
2	文件名	7610163149168a9c260c28ec2d4ae2cf.exe											
3	文件路径	C:\Users\jacksixiong\Desktop\恶意代码\上海浩迈样本\恶意伪装											
4	MD5	7610163149168a9c260c28ec2d4ae2cf											
5	木马名称	Html.Exploit.IFrame											
6	木马类型	恶意伪装											
7	文件大小	3.38 KB											
8	创建时间	2024-12-13 12:24:49											
9	访问时间	2024-12-13 15:46:13											
10	修改时间	2018-03-16 23:05:58											

7.7 日志管理

点击主界面右侧的“日志管理”，可查询、删除或导出内存扫描日志、快速扫描日志、全盘扫描日志、自定义扫描日志、选择扫描日志、动态检测日志、实时保护日志。

点击“查询”即可查询日志时间、目标、摘要和操作（查看和删除）；

点击“删除”按钮会删除所有当前查询到的日志记录；点击“导出”会导出所有当前查询到的日志记录。

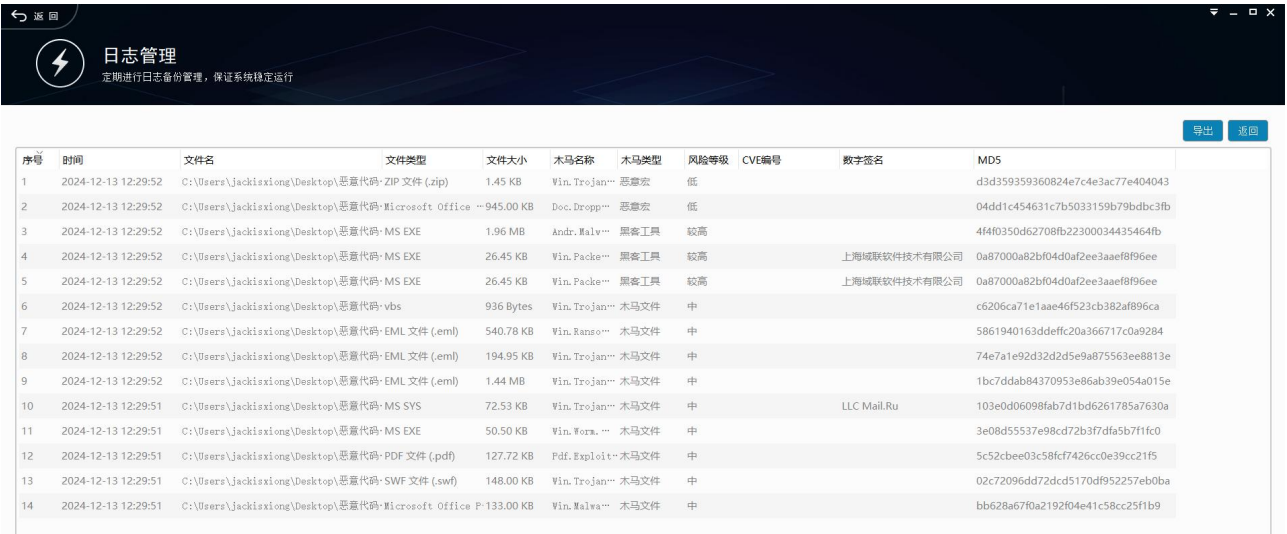


点击“查询”按钮，可以查看对应的日志。





点击“查看”，可以查看对应的扫描信息；点击“删除”，删除当前选中的日志记录。



7.8 系统设置

点击主界面右侧的“系统设置”，可进行“安全设置”、“存储设置”、

“扫描设置”、“进程设置”、“域名设置”、“IP 设置”、“端口设置”。

7.8.1 安全设置

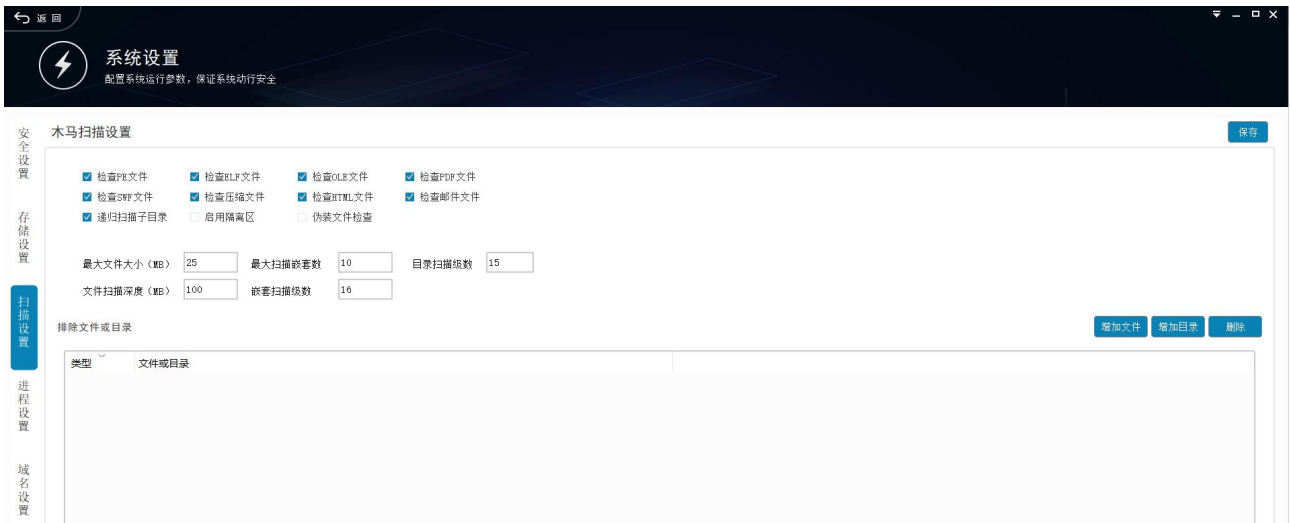
可以设置用户登录超时时间（分钟），用户密码更改周期（天），密码重试次数，账户锁定时间（分钟），点击右上角“保存”。

7.8.2 存储设置

可以设置日志保存周期（天），剩余空间报警（GB），是否勾选覆盖 3 个月前数据，数据已满报警（MB）。

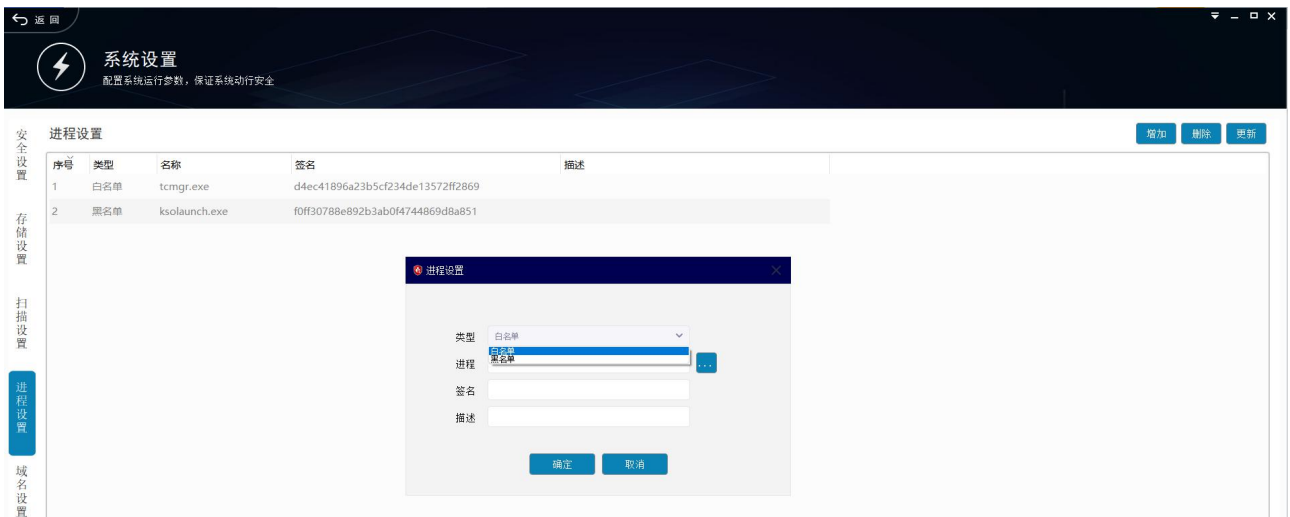
7.8.3 扫描设置

可以按照下图所示进行设置，同时还可以增加排除文件或排除文件目录。



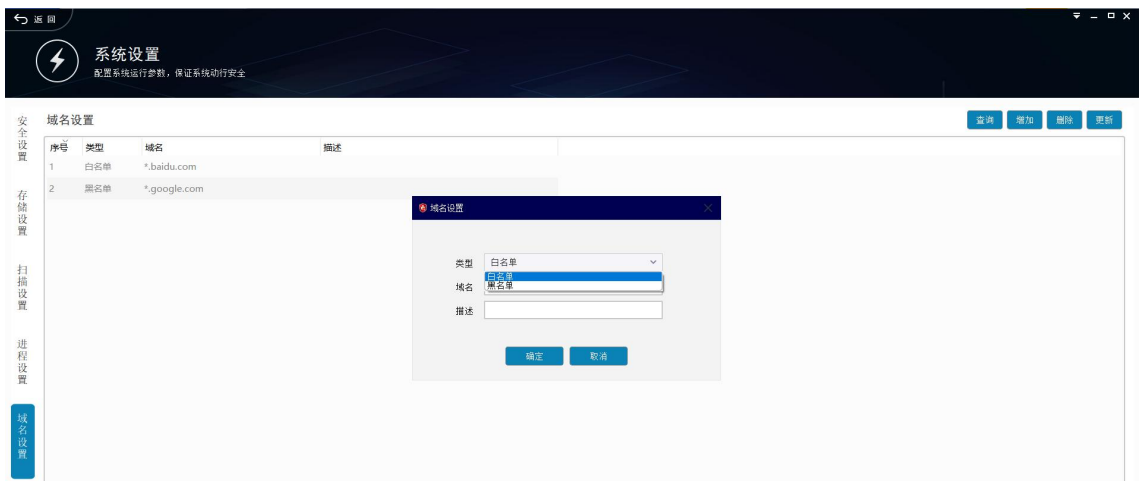
7.8.4 进程设置

可以增加或删除进程白名单或黑名单，点击“更新”完成设置更新。



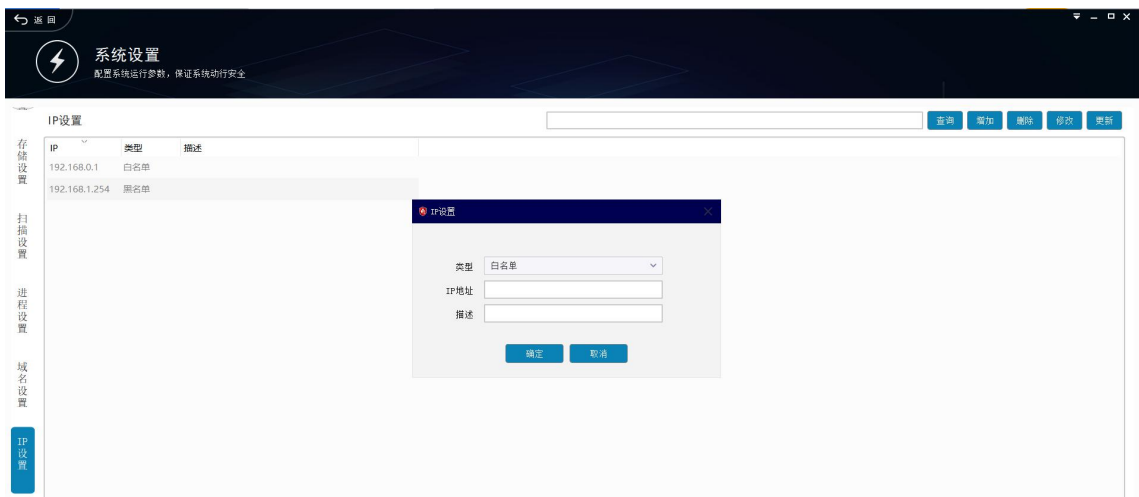
7.8.5 域名设置

可以添加域名白名单或域名黑名单，点击“更新”完成设置更新。



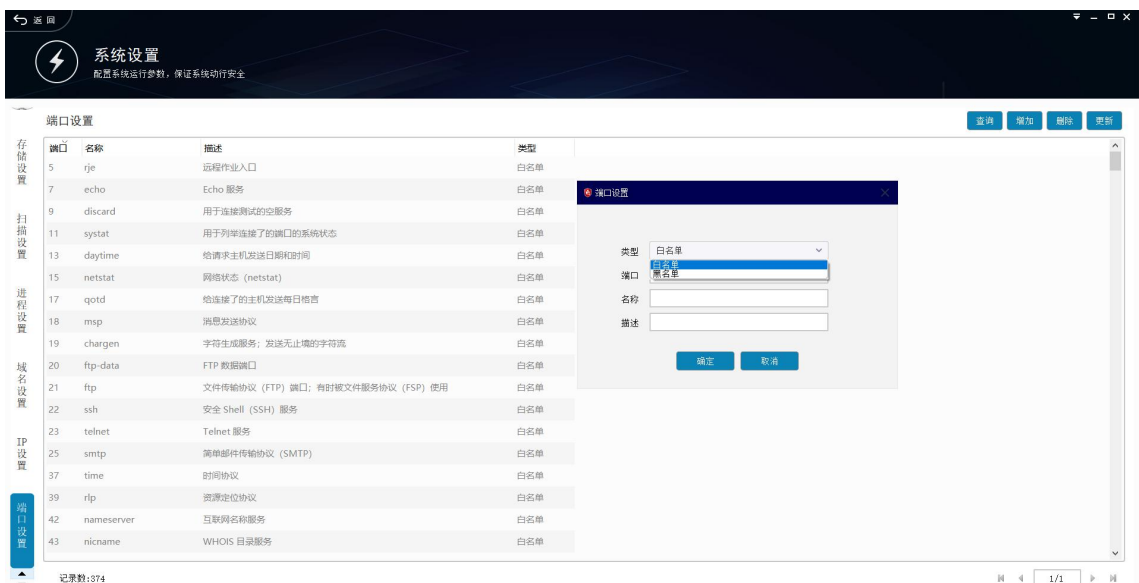
7.8.6 IP 设置

可以添加、删除或修改 IP 白名单或黑名单，点击“更新”完成设置更新。



7.8.7 端口设置

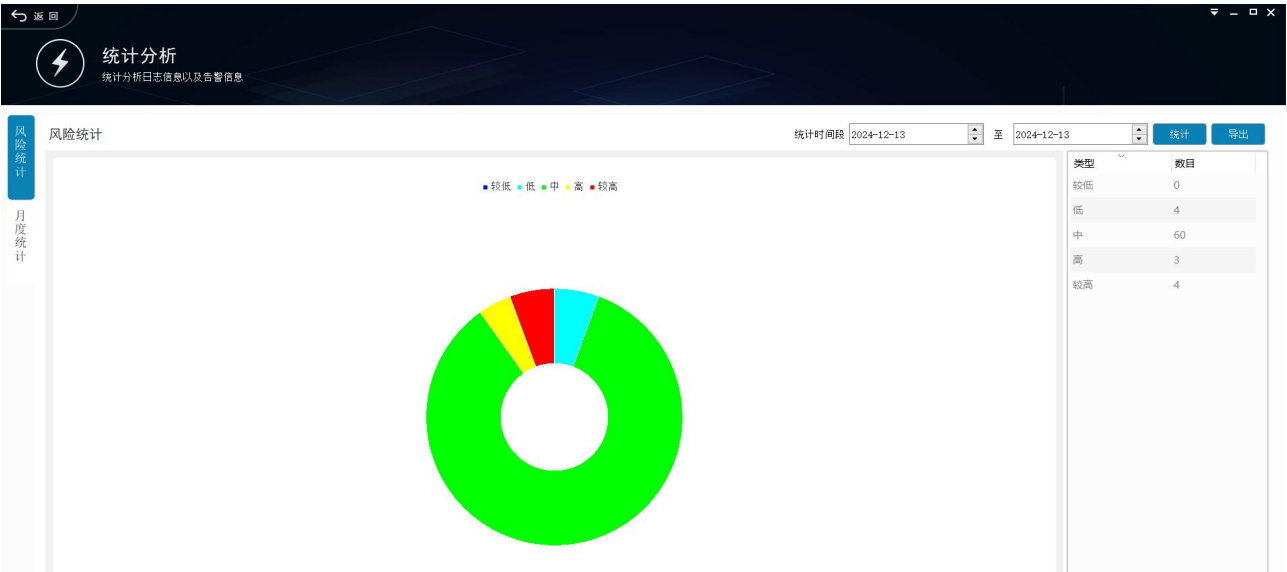
可以添加或删除端口白名单或黑名单，点击“更新”完成设置更新。



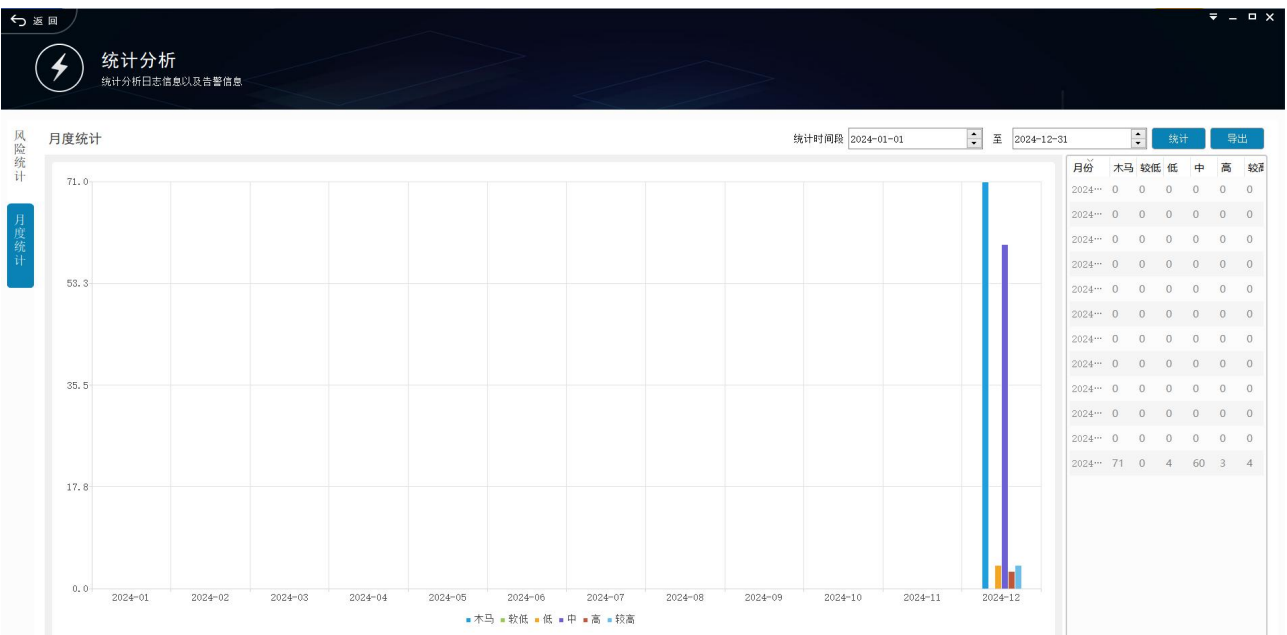
7.9 统计分析

点击主界面右侧的“统计分析”，可查看“风险统计”和“月度统计”图。

(1) 选择“风险统计”选项卡，点击右上角“统计”按钮，形成圆形图。点击“导出”选择导出路径和输入文件名，可导出 xls 表格格式文件。



(2) 选择“月度统计”选项卡，点击右上角“统计”按钮，形成柱状图。点击“导出”选择导出路径和输入文件名，可导出 xls 表格格式文件。



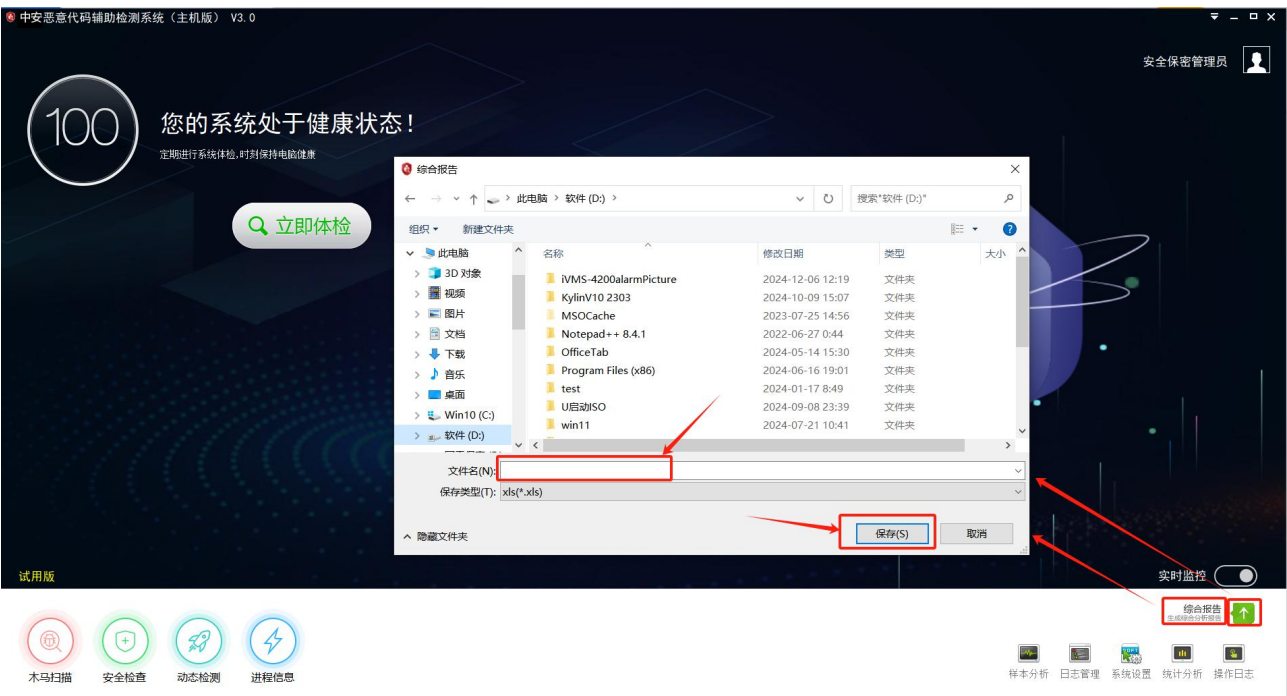
7.10 操作日志

点击主界面右侧的“操作日志”，在弹出的页面右侧点击“查询”按钮，可查看安全审计员 audadmin 的操作日志，也可以删除该日志信息，点击“导出”选择导出路径和输入文件名，可导出 xls 表格格式文件。



7.11 综合报告导出

点击主界面右侧的“综合报告”或点击向上箭头，输入文件名和选择保存路径后，点击“保存”按钮可以导出 xls 表格格式文件。



时间	文件名	文件类型	文件大小	木马名称	木马类型	风险等级	CVE编号	数字签名
2024-12-13 19:19:41	C:\Users\jackson\Desktop\恶意代码\上海信迈样本\dlf\01b17424 MS DLL		6.75 KB	Win.Adware.Downware	木马文件	中		
2024-12-13 19:19:51	C:\Users\jackson\Desktop\恶意代码\上海信迈样本\bat\c223d63i bat		1.14 KB	Win.Trojan.CAZF_Agent	木马文件	中		
2024-12-13 19:19:51	C:\Users\jackson\Desktop\恶意代码\上海信迈样本\bat\download bat		286 Bytes	Win.Trojan.CAZF_Agent	木马文件	中		
2024-12-13 19:19:51	C:\Users\jackson\Desktop\恶意代码\上海信迈样本\doc\0622D6 Microsoft Office Word (.docx)		16.80 KB	Doc.Downloader.Bartalex	木马文件	中		
2024-12-13 19:19:51	C:\Users\jackson\Desktop\恶意代码\上海信迈样本\bat\fc0992ba bat		56.16 KB	Win.Trojan.CAZF_Agent	木马文件	中		
2024-12-13 19:19:51	C:\Users\jackson\Desktop\恶意代码\上海信迈样本\签名样本\3 MS EXE		112.67 KB	Win.Trojan.Puke	木马文件	中		Sail Machine
2024-12-13 19:19:51	C:\Users\jackson\Desktop\恶意代码\上海信迈样本\邮件样本\1 EML 文件 (.eml)		95.77 KB	Win.Adware.Nimnul	木马文件	中		
2024-12-13 19:19:55	C:\Users\jackson\Desktop\恶意代码\上海信迈样本\eml\11 (2).en EML		7.27 KB	Win.Adware.Downware	木马文件	中		

八、安全审计员登录操作

8.1 密码修改

使用安全审计员 audadmin 账户登录系统后，在主界面右上角点击“安全审计员”或旁边的图标，可以修改账户登录密码。



8.2 操作日志

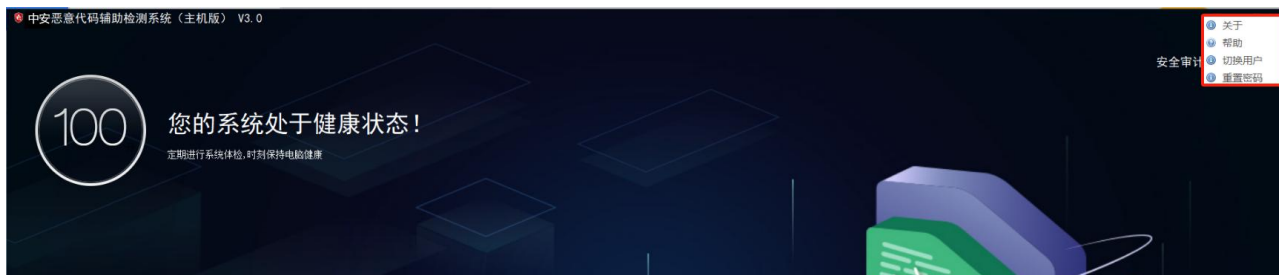
点击主界面右侧的“操作日志”，在弹出的页面右侧点击“查询”按钮，可查看安全审计员 audadmin 的操作日志，也可以删除该日志信息，点击“导出”选择导出路径和输入文件名，可导出 xls 表格格式文件。

The screenshot shows the '操作日志管理' (Operation Log Management) interface. It features a search bar at the top with a '查询' (Query) button. Below is a table with columns for '序号' (Serial Number), '时间' (Time), '用户' (User), and '内容' (Content). The table lists various system events, including user logins, logouts, and security checks performed by 'sysadmin' and 'secadmin' users. At the bottom right, there are buttons for '删除' (Delete) and '导出' (Export).

序号	时间	用户	内容
1	2024-12-13 17:45:41	sysadmin	用户登录失败
2	2024-12-13 17:45:47	sysadmin	用户登录成功
3	2024-12-13 17:47:31	sysadmin	用户退出: sysadmin
4	2024-12-13 17:47:46	secadmin	用户登录成功
5	2024-12-13 17:48:42	secadmin	动态检测: 启动
6	2024-12-13 17:58:23	secadmin	动态检测: 停止
7	2024-12-13 17:58:38	secadmin	辅助检测: 文件关联
8	2024-12-13 17:58:38	secadmin	辅助检测: 文件关联
9	2024-12-13 17:58:41	secadmin	辅助检测: Hosts检查
10	2024-12-13 17:58:43	secadmin	辅助检测: Hosts检查
11	2024-12-13 17:58:44	secadmin	辅助检测: SSDT检查
12	2024-12-13 17:58:49	secadmin	辅助检测: SSDT检查
13	2024-12-13 17:58:51	secadmin	辅助检测: SSDT检查
14	2024-12-13 17:58:55	secadmin	辅助检测: Hosts检查
15	2024-12-13 17:58:55	secadmin	辅助检测: Hosts检查
16	2024-12-13 17:58:55	secadmin	辅助检测: Hosts检查

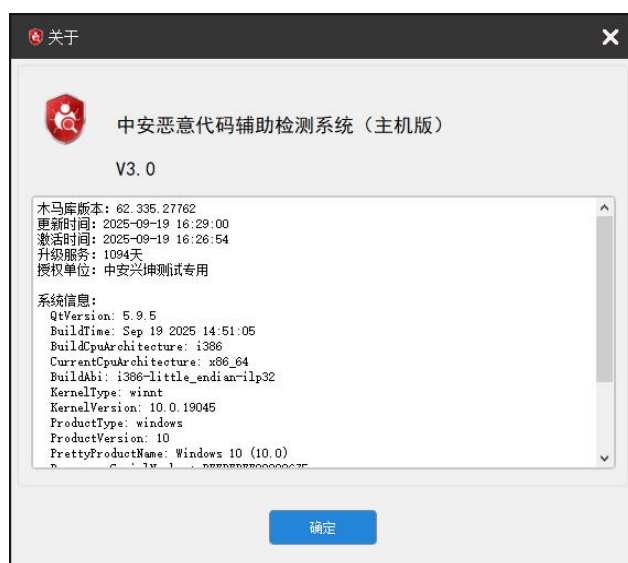
九、三员通用操作

使用安三员登录系统后，点击主界面右上角的倒三角按钮，均有“关于”、“帮助”、“切换用户”和“重置密码”的功能。



9.1 关于

点击“关于”，可查看木马库版本、木马库更新时间、升级服务（默认三年）、授权单位和系统信息。



9.2 帮助

点击“帮助”，可以查看该系统的用户手册。

9.3 切换用户

点击“切换用户”，可以切换登录其他账户。



9.4 重置密码

系统管理员登录点击“重置密码”，可以重置安全保密管理员和安全审计员的密码。若重置安全保密管理员的密码，当前管理员密码即输入系统管理员密码，协助管理员密码即输入安全审计员的密码；若重置安全审计员的密码，当前管理员密码即输入系统管理员密码，协助管理员密码即输入安全保密管理员的密码；



安全保密管理员登录点击“重置密码”，可以重置系统管理员和安全审计员的密码。若重置系统管理员的密码，当前管理员密码即输入安全保密管

理员密码，协助管理员密码即输入安全审计员的密码；若重置安全审计员的密码，当前管理员密码即输入安全保密管理员密码，协助管理员密码即输入系统管理员的密码；



The screenshot shows a '重置密码' (Reset Password) dialog box. It contains three input fields: '重置管理员' (Reset Administrator), '当前管理员密码' (Current Administrator Password), and '协助管理员密码' (Assistance Administrator Password). The '重置管理员' dropdown menu is open, showing '系统管理员' (System Administrator) as the selected option. The '当前管理员密码' dropdown menu is also open, showing '系统管理员' (System Administrator) and '安全审计员' (Security Auditor) as options. The '协助管理员密码' field is empty. At the bottom, there are two buttons: '确定' (Confirm) and '取消' (Cancel).

安全审计员登录点击“重置密码”，可以重置系统管理员和安全保密管理员的密码。若重置系统管理员的密码，当前管理员密码即输入安全审计员密码，协助管理员密码即输入安全保密管理员的密码；若重置安全保密管理员的密码，当前管理员密码即输入安全审计员密码，协助管理员密码即输入系统管理员的密码。



The screenshot shows a '重置密码' (Reset Password) dialog box. It contains three input fields: '重置管理员' (Reset Administrator), '当前管理员密码' (Current Administrator Password), and '协助管理员密码' (Assistance Administrator Password). The '重置管理员' dropdown menu is open, showing '系统管理员' (System Administrator) as the selected option. The '当前管理员密码' dropdown menu is also open, showing '系统管理员' (System Administrator) and '安全保密管理员' (Security Confidential Administrator) as options. The '协助管理员密码' field is empty. At the bottom, there are two buttons: '确定' (Confirm) and '取消' (Cancel).

十、技术支持

公司网址：<https://www.bjzaxk.com>

软件使用中有任何问题，请致电：400-812-8882