

# MWKT2.0使用手册

## 风险提示：

1.由于本工具权限非常高，使用时一定要注意json文件中的配置信息是否存在业务文件和系统文件，如果存在禁止清理，否则会导致系统崩溃。

2.低版本的操作系统使用时由于程序中关于hash检索目录的功能使用的是多线程，可能会导致系统卡顿、蓝屏，请谨慎使用。

## 一、工具介绍

MWKT（M78 Windows Killer Tool）是一款专门用于处理windows后门的专杀工具，该工具会从当前目录下读取json文件，点击自动加载会读取程序目录下的所有json加载，根据需求进行选择。

工具功能：

- 1.扫描/删除json文件中的指定文件和目录，如果是C:\users\用户\目录，会将主窗口显示的用户替换成“用户”（public除外）。
- 2.扫描/删除json中的启动项、计划任务、服务。
- 3.终止指定进程。
- 4.根据hash值检索进程、启动项、计划任务、服务对应的程序是否匹配，如果匹配则删除。
- 5.根据hash递归检索指定目录下的所有文件的hash值。

## 二、工具的使用

### 1、专杀配置文件的使用

1.先根据病毒特征生成json文件，在msangfor.com-专杀脚本-新建脚本中，如下以windows驱动人生病毒为例，先获取到病毒的维持项（WMI暂不支持扫描）：

文件：

c:\windows\syswow64\svchost.exe,c:\windows\syswow64\wmicx.exe,c:\windows\syswow64\drivers\svchost.exe,c:\windows\syswow64\drivers\taskmgr.exe,c:\windows\temp\svchost.exe,c:\windows\temp\m.ps1,c:\windows\temp\mkatz.ini

进程：svchost.exe,taskmgr.exe,wmicx.exe

启动项：Ddriver,WebServers

服务：Ddriver,WebServers

计划任务：

Ddrivers,DnsScan,WebServers,\\Microsoft\\Windows\\Bluetooths

hash：

59B18D6146A2AA066F661599C496090D,A4B7940B3D6B03269194F728610784D6,5AB6F8CA1F22D88B8EF9A4E39FCA0C03,BC26FD7A0B7FE005E116F5FF2227EA4D,4E4A2B3A8909AC1B4B79AC63C43D1DD8,C6521A04D01C0549A47A936E861DDC11

需要扫描的目录：

msangfor

申请工具

工具审批

用户审批

申请记录

在线沙箱

反馈建议

最新公告

专享脚本

新建脚本

公共脚本

我的脚本

工具管理

规则管理

首页 / 新建脚本

工具使用问题联系 张贺杰 (33142) 18878798855

基本信息

\* 脚本名称:

请输入脚本名称

脚本描述:

请输入脚本描述

\* 操作系统类型:

WindowsLinux

Windows配置

未特别说明的,均使用英文逗号(,) windows版本仅支持json配置输出

删除列表:

请输入文件或目录

输入文件或目录: c:\1.exe

进程列表:

请输入进程名

输入进程名: 360.exe

服务列表:

请输入服务名

输入服务名: xmrig.pwnrig

task任务:

请输入Windows计划任务名称

输入计划任务名称

启动项:

请输入启动项名称

输入启动项名称: start\_name

WMI项:

请输入WMI项名称

输入wmi项名称: wmi\_name

高级配置

Hash匹配:

md51,md52,md53

输入路径在后方的输入框中输入你要匹配的目录

HashDir:

c:\data , d:\wwwroot

在后方的输入框中输入你要匹配的目录

\* 可见范围:

私有公开

是否公开你生成的专享供其他用户使用

## 2.再获取生成的json文件，点击下载脚本。

msangfor.com/scripts/public

msangfor

申请工具

工具审批

用户审批

申请记录

在线沙箱

反馈建议

专享脚本

新建脚本

公共脚本

我的脚本

工具管理

规则管理

首页 / 公共脚本

工具使用问题联系 张贺杰 (33142) 18878798855

公共脚本

请输入关键字

重置搜索

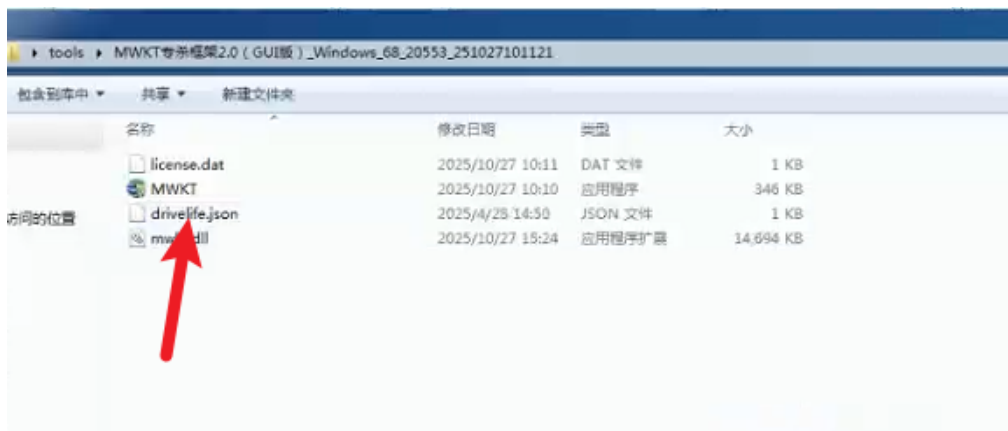
序号	作者	系统类型	文件名	描述	创建时间
30	王杰龙	Windows	drivelife	驱动人生病毒	2025-04-28T14:46:57.96
1	陈诺	Linux	Echeck_1	常见常规排查(含redis入侵检测)	2024-01-29T14:11:35.52
29	刘长松	Linux	外交字机挖矿clean	海嘤	2025-04-15T15:32:06.32
28	刘长松	Linux	Skidmap_Clear_20250306	更新了部分清理模块, 添加一些注释	2025-03-06T17:40:02.45
15	刘长松	Linux	Docker应用Commando Cat加密挖矿_0229_info	Docker API遭受 "Commando Cat" 加密挖矿,类似TeamTNT	2024-02-29T15:26:24.20
27	刘长松	Linux	Skidmap_Clear_20250306	更新了部分清理模块, 添加一些注释	2025-03-06T17:39:55.01
4	刘长松	Linux	Tsunami海啸病毒专享	该版本专享对应的是2023年FUDan超算的病毒版本, 一键查杀	2024-01-29T15:58:40.23
26	刘长松	Linux	yayaya专享——from_EDR	EDR出品的yayaya挖矿家族专享	2025-01-16T10:24:37.88
13	刘长松	Linux	2024挖矿处置0227_clean	挖矿处置, .ssh_miner.service	2024-02-27T09:37:12.95
20	刘长松	Linux	watchdog(据说)挖矿清理脚本	仅供学习参考	2024-05-09T16:17:30.75

共 30 条数据

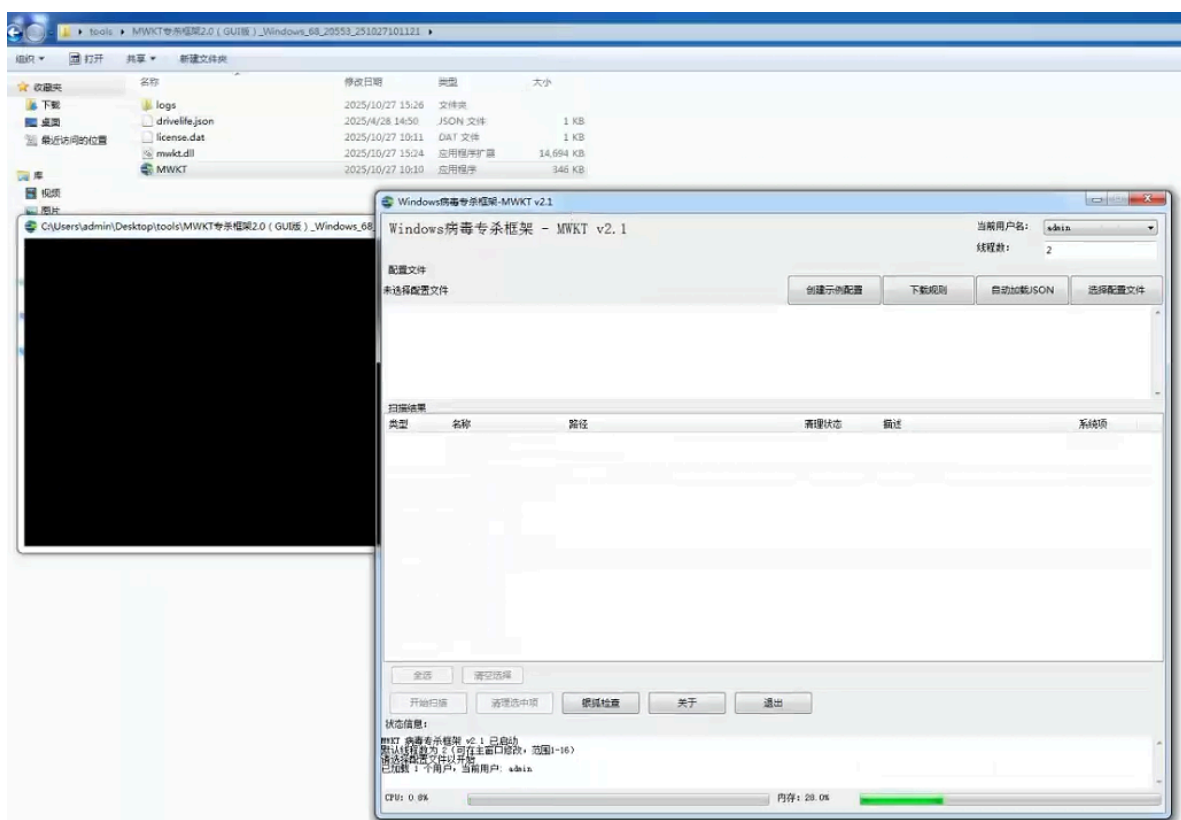
10 条/页 < 1 2 3

## 3.将json文件跟MWKT主程序放在同一目录下。

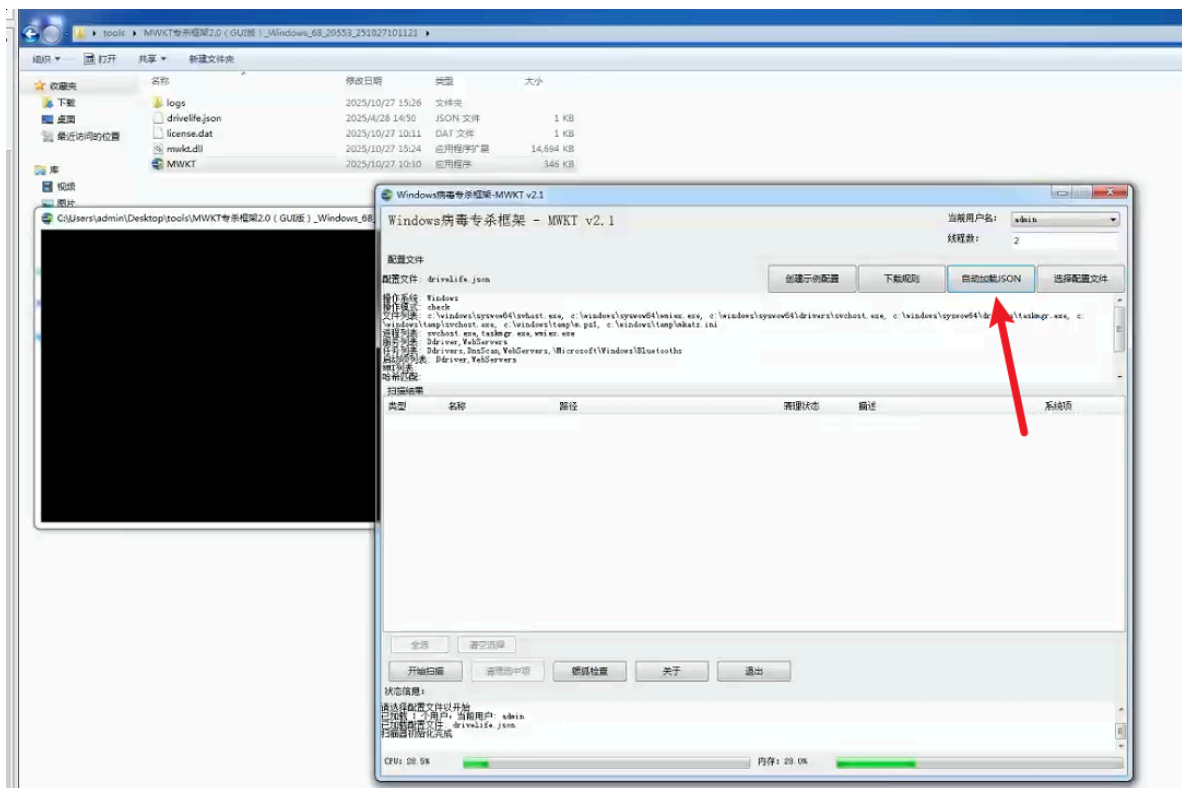
3 / 18



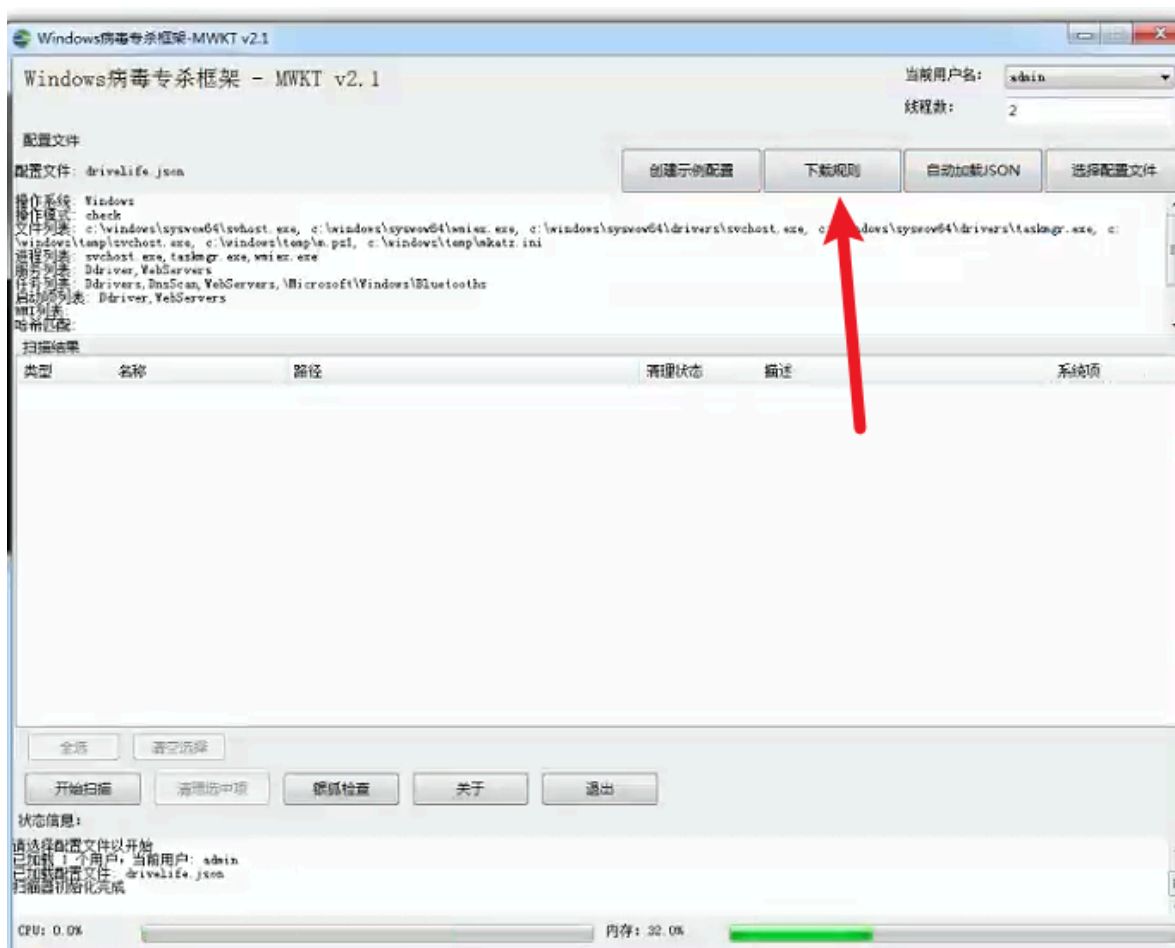
4.双击MWKT.exe，打开后会显示GUI界面。

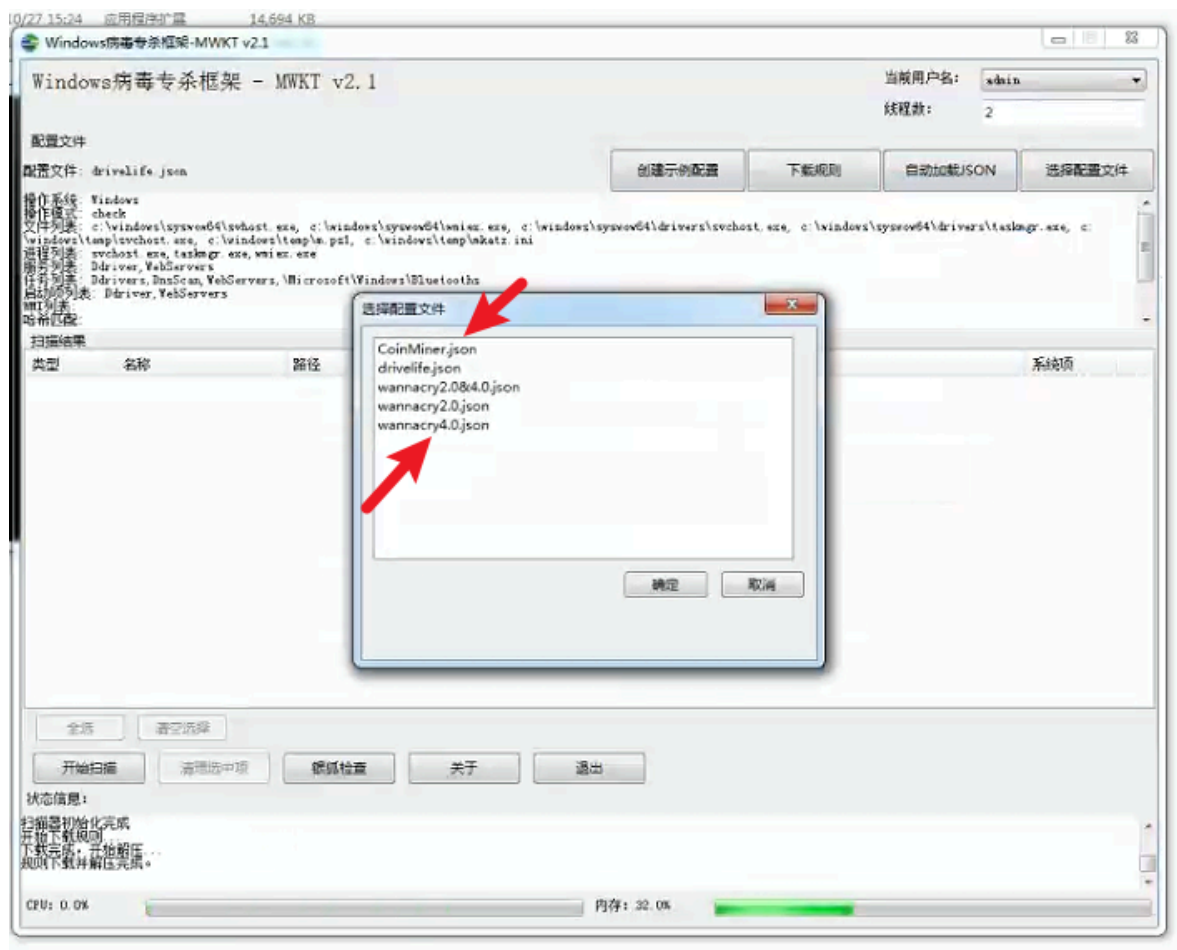


5.点击自动加载会加载当前目录下的json文件到扫描器。

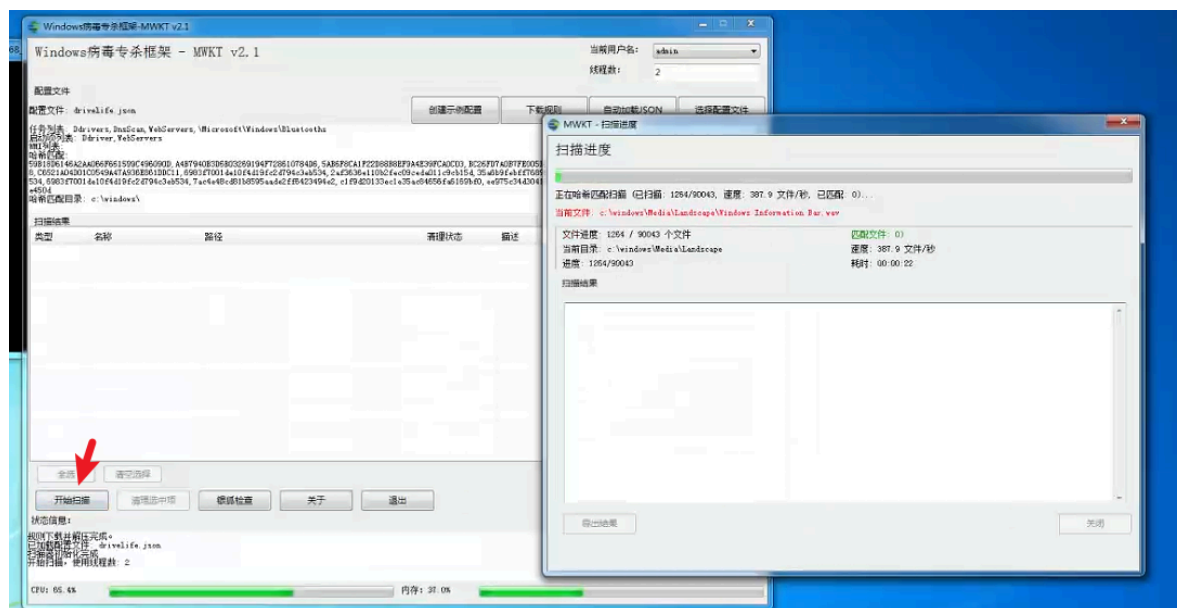


6. 点击下载规则按钮，会远程下载5个默认的配置文件，这个时候选择自动加载，会提示需要选择哪个配置文件加载。

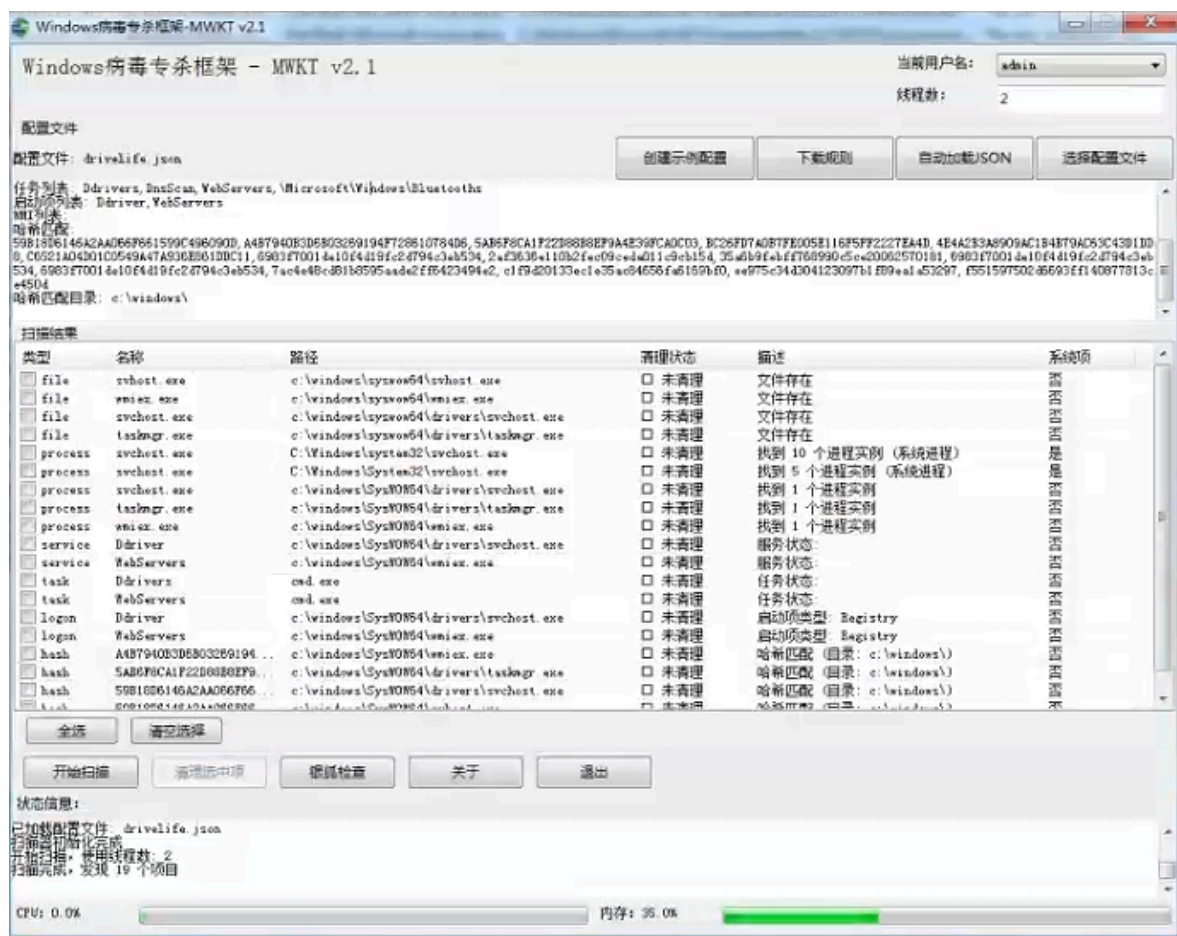




7.加载完配置文件后，点击开始扫描，会显示扫描进度。

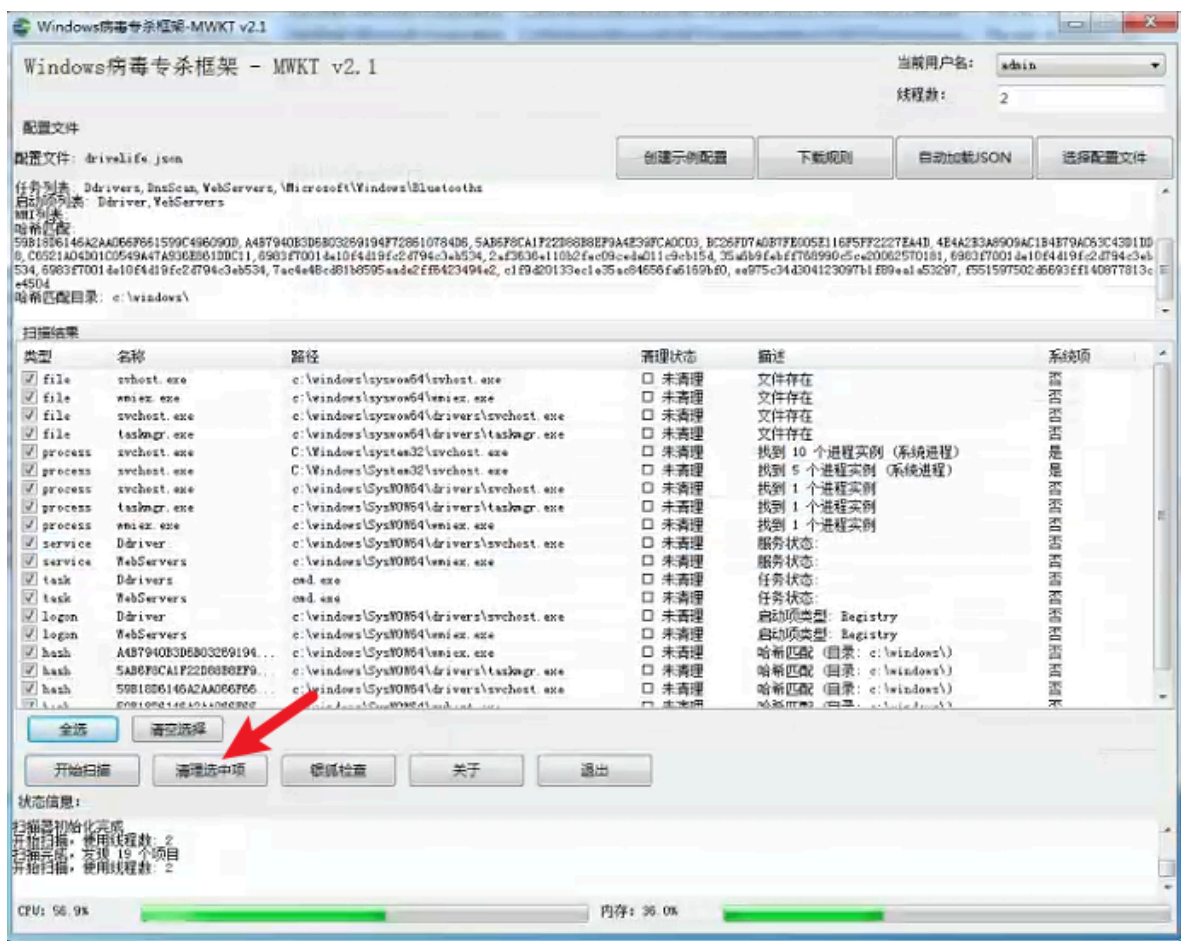


8.扫描完成后，扫描结果会显示在主窗口扫描结果中。

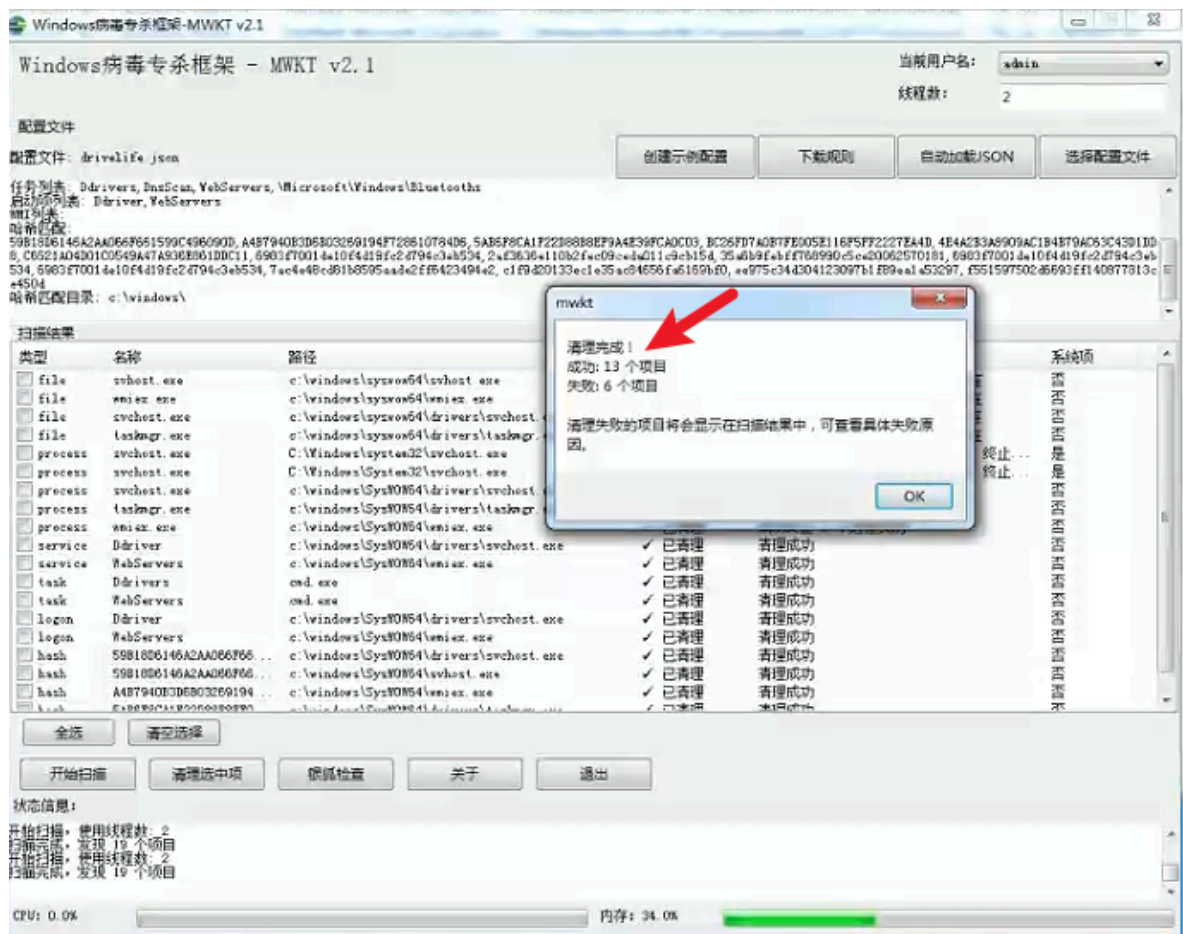


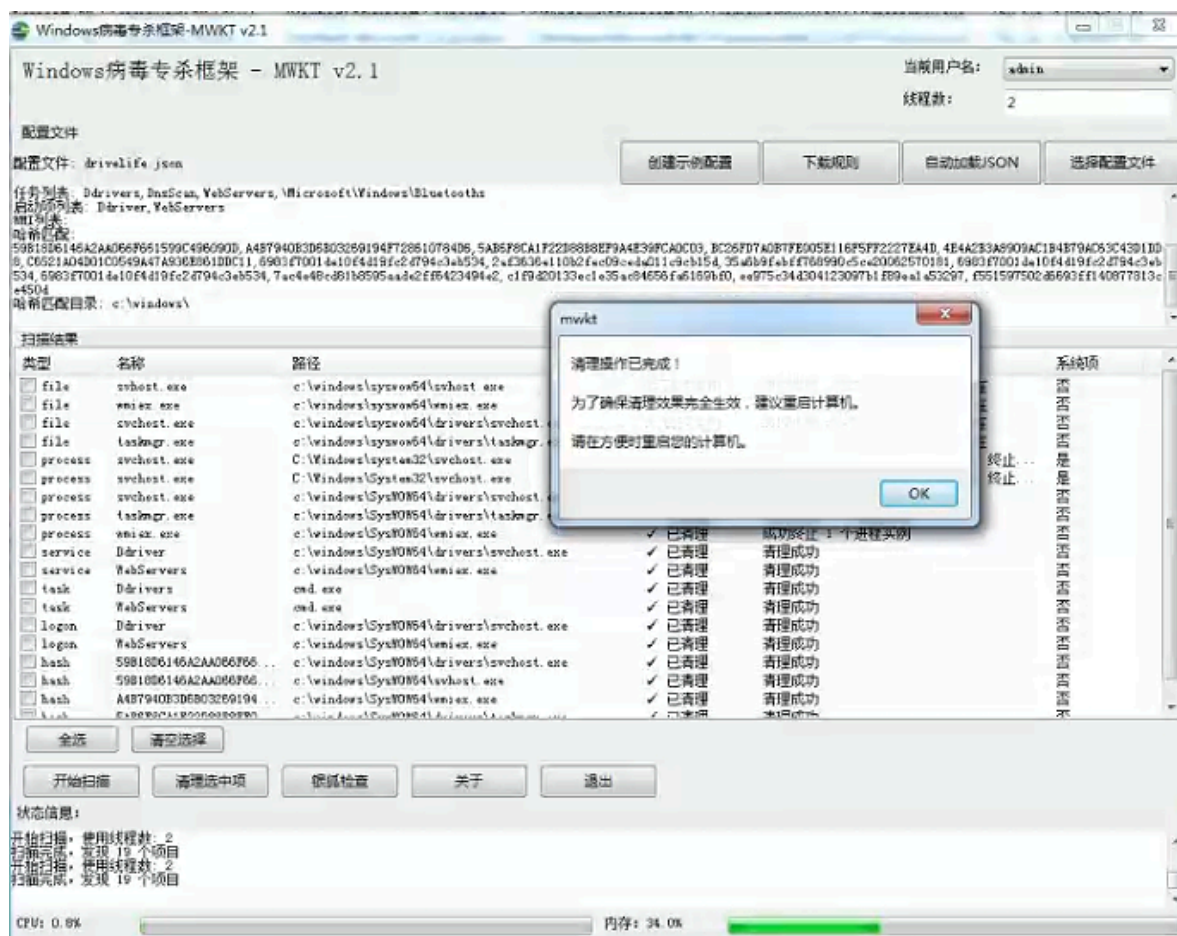
9. 确认扫描出的结果非误报，选中需要清理的扫描结果，点击清理选中项，即可开始清理。

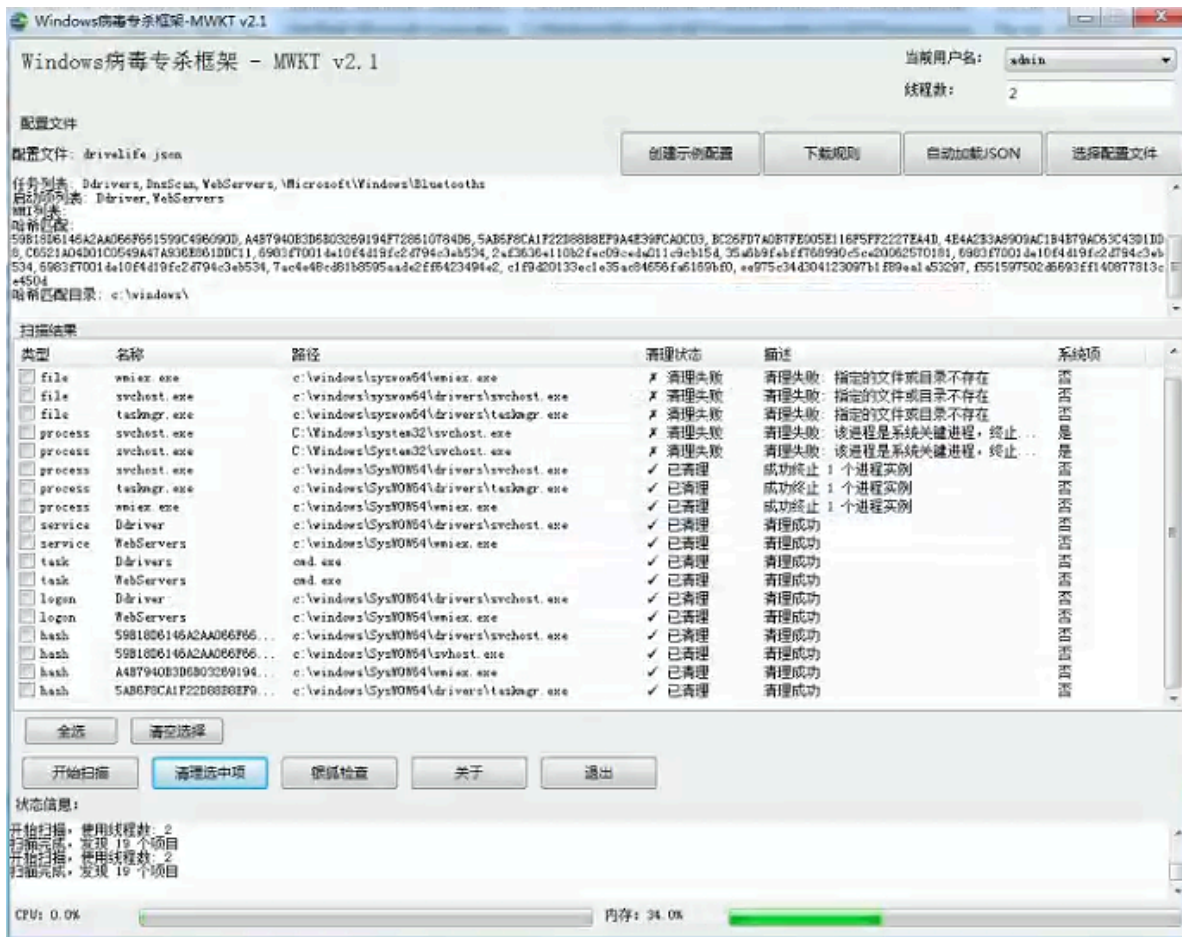




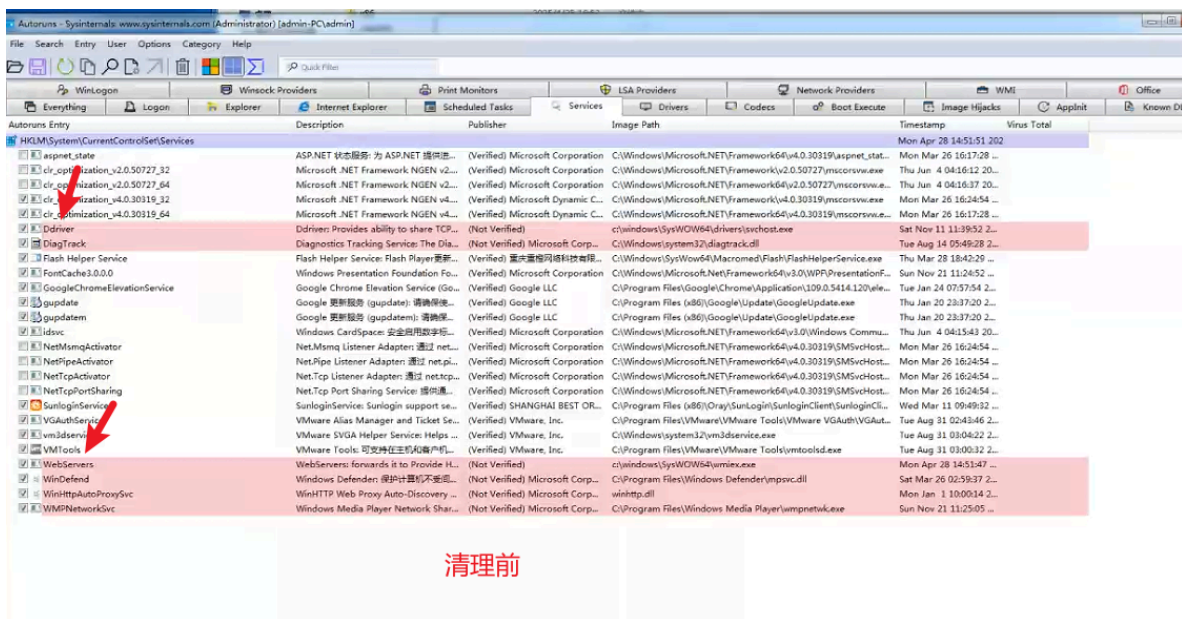
10.清理结束会出现清理成功,



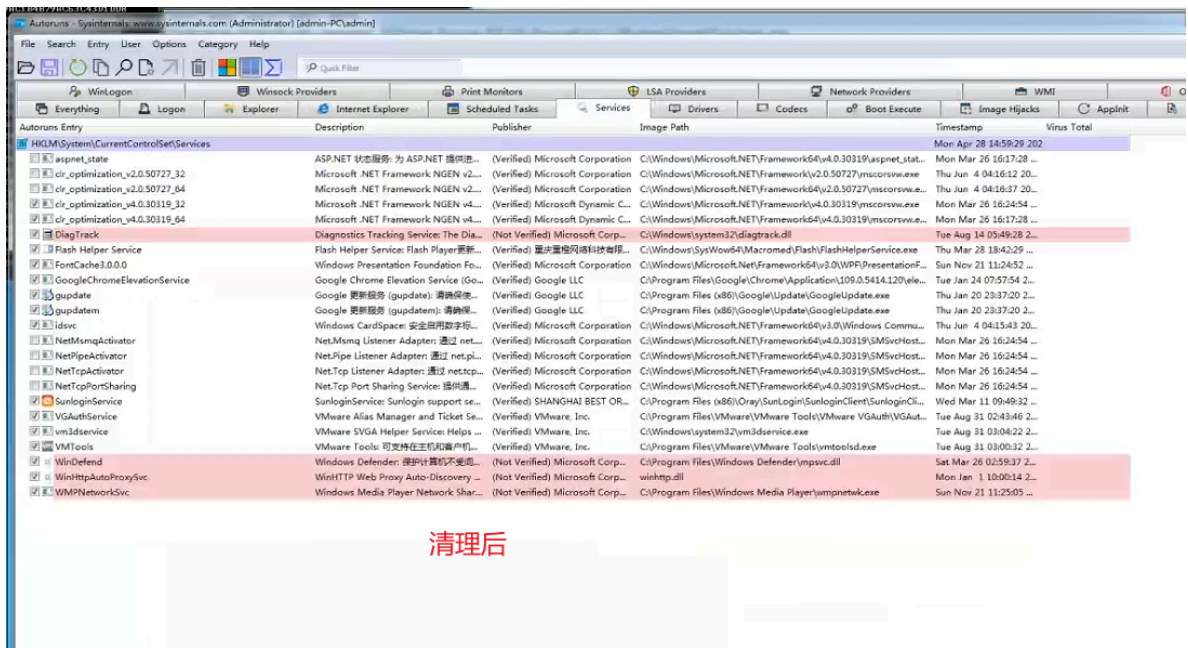




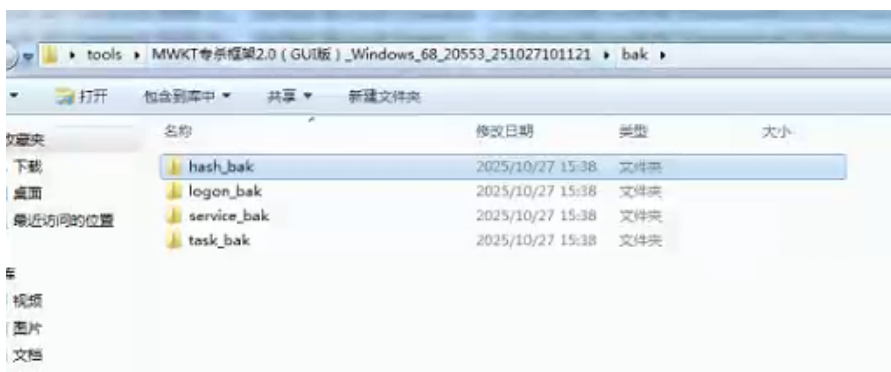
11.如下图, 清理后维持项已消失, 删除的文件将备份。



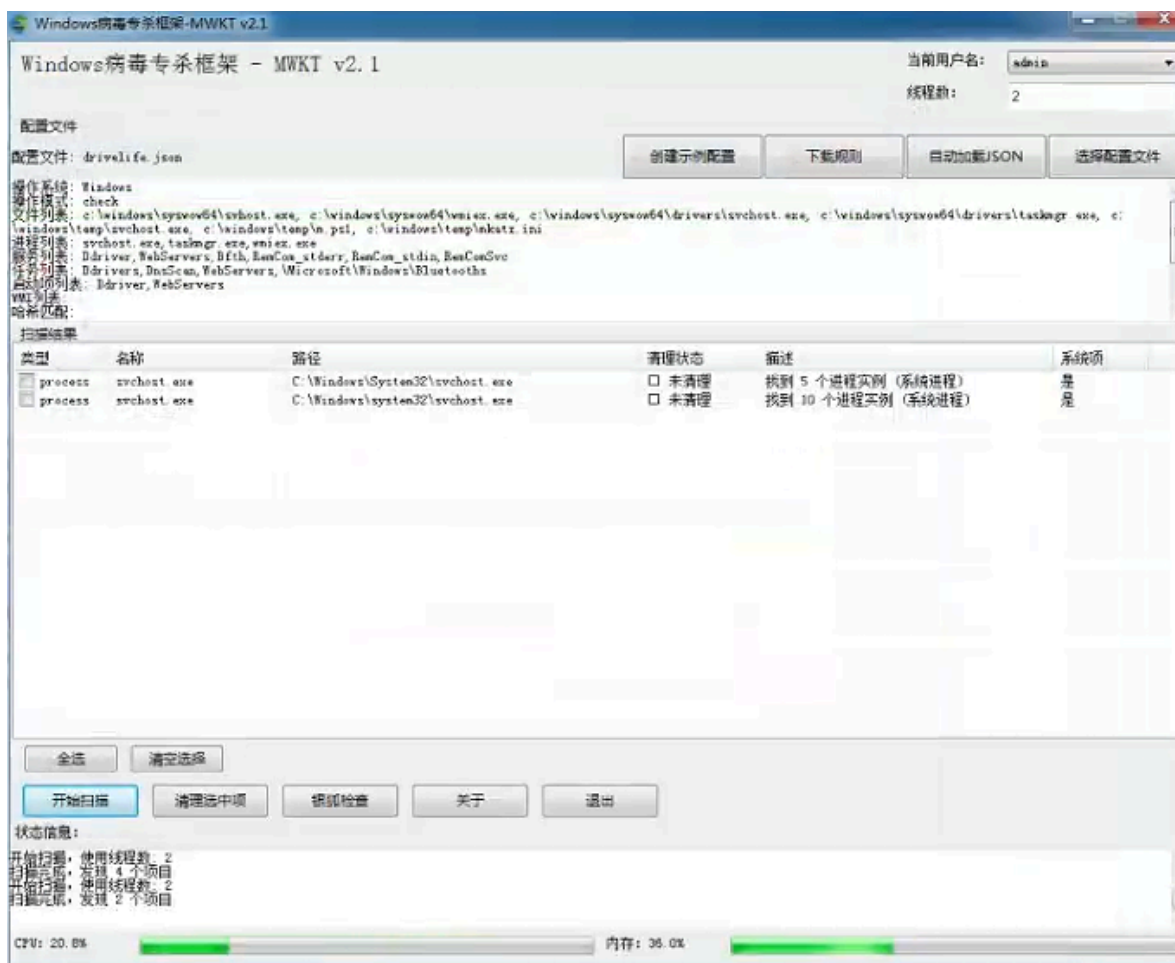




9.清理的文件备份在程序的bak目录下。

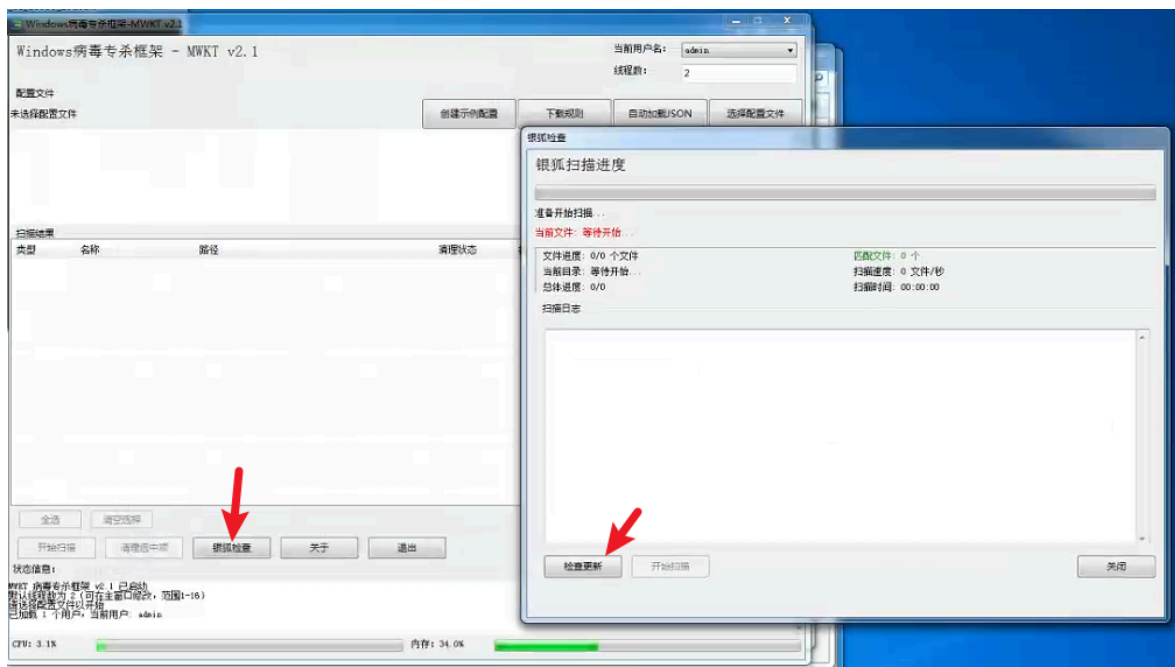


10.最后重启主机，然后重启后再次扫描，看是否存在残留。（svchost对应的路径为系统文件，所以不会进行清理）

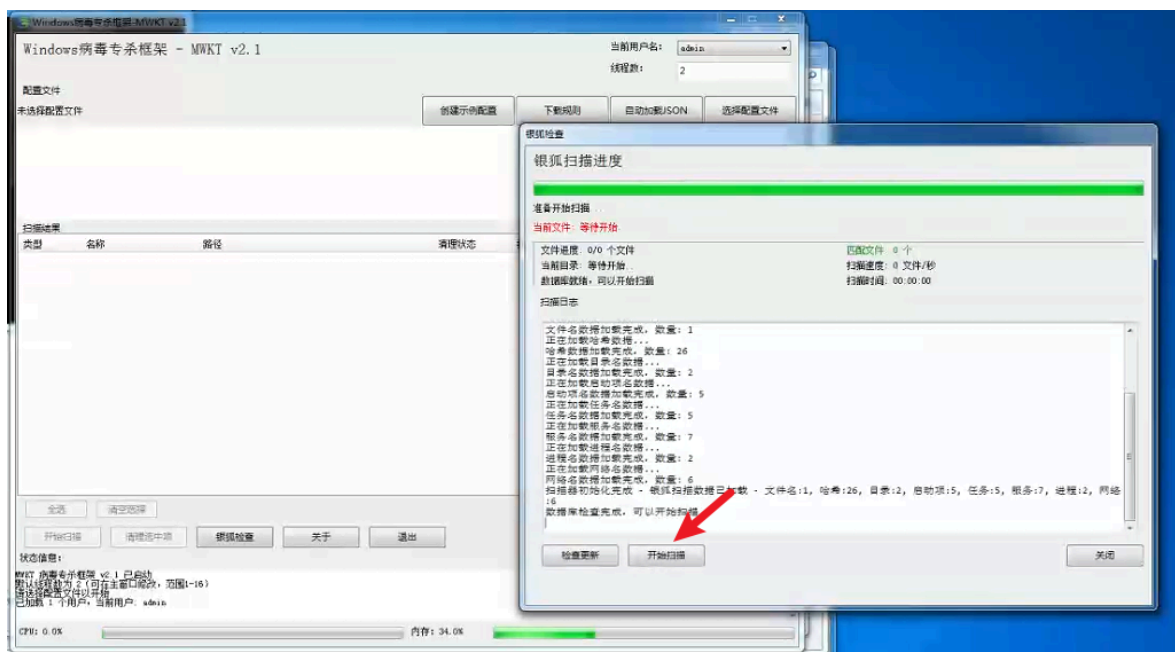


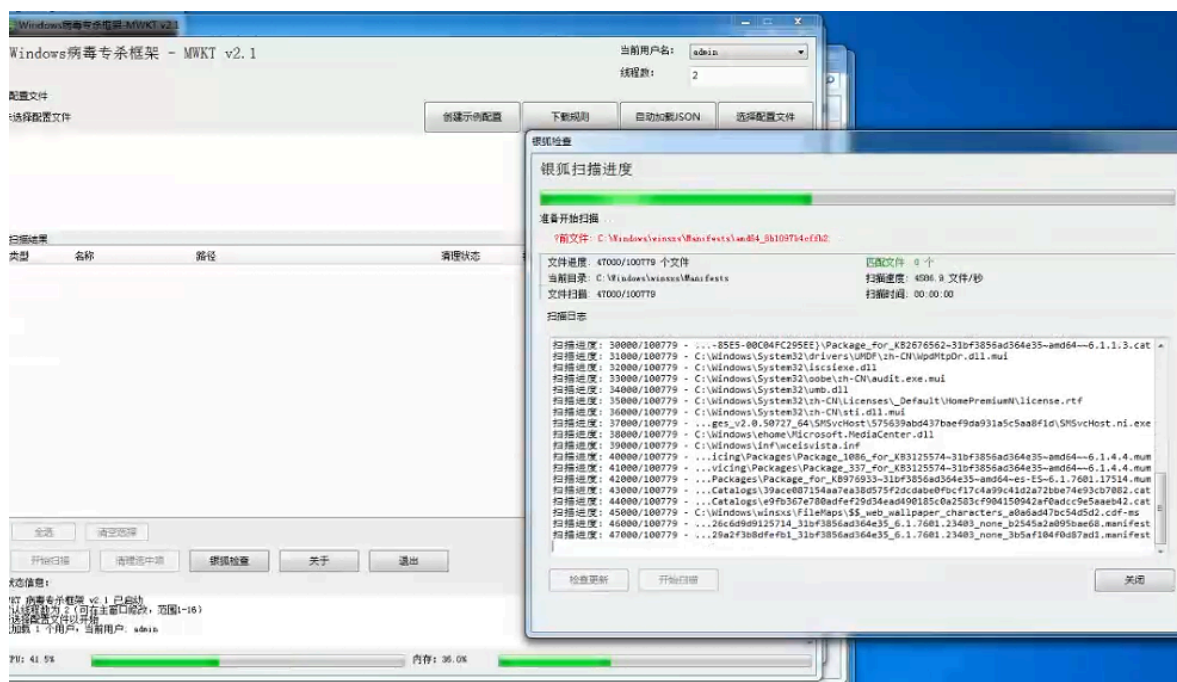
## 2、银狐检查

1. 点击: “银狐检查”, “检查更新”, 即可检查当前是否存在银狐规则库, 如果不存在则会下载。



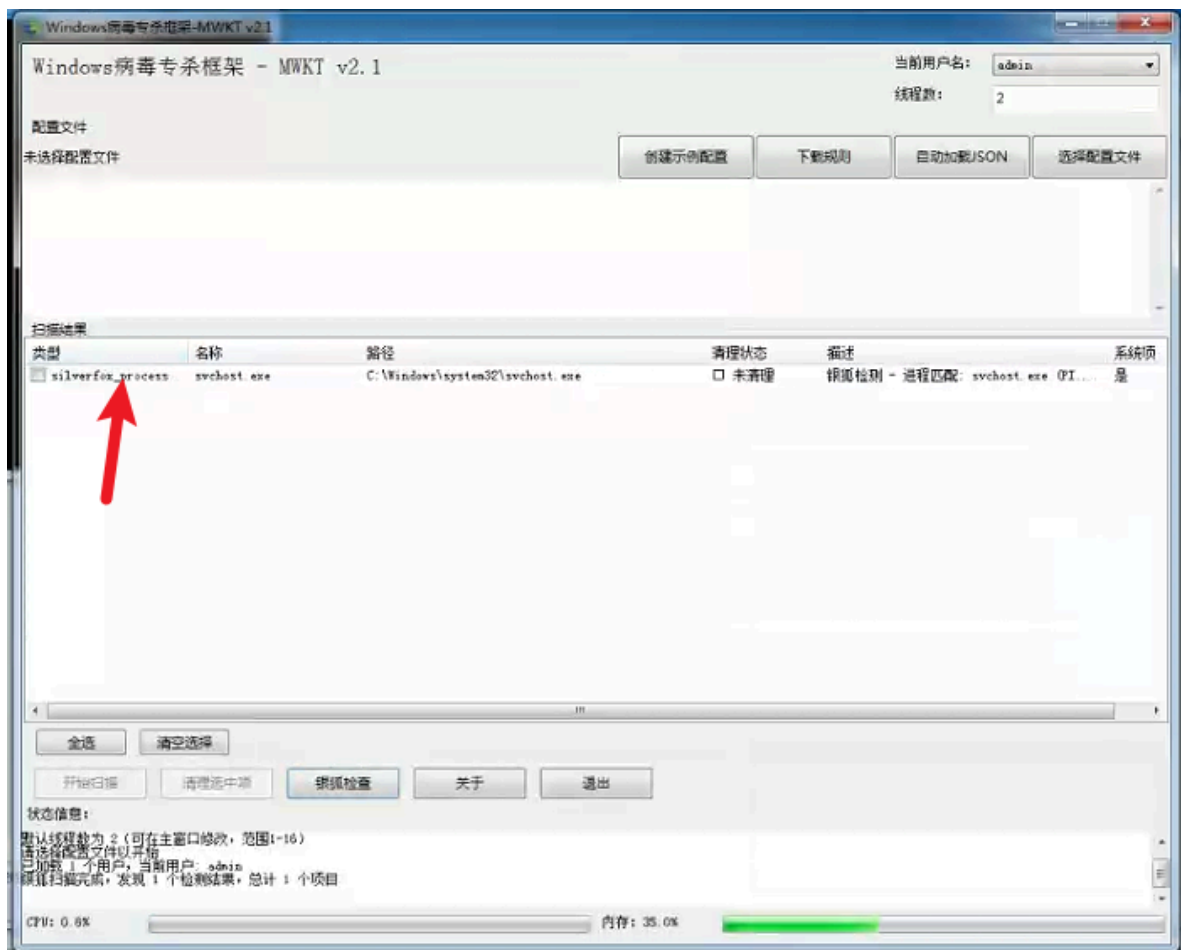
2. 下载完成后才能开始扫描。





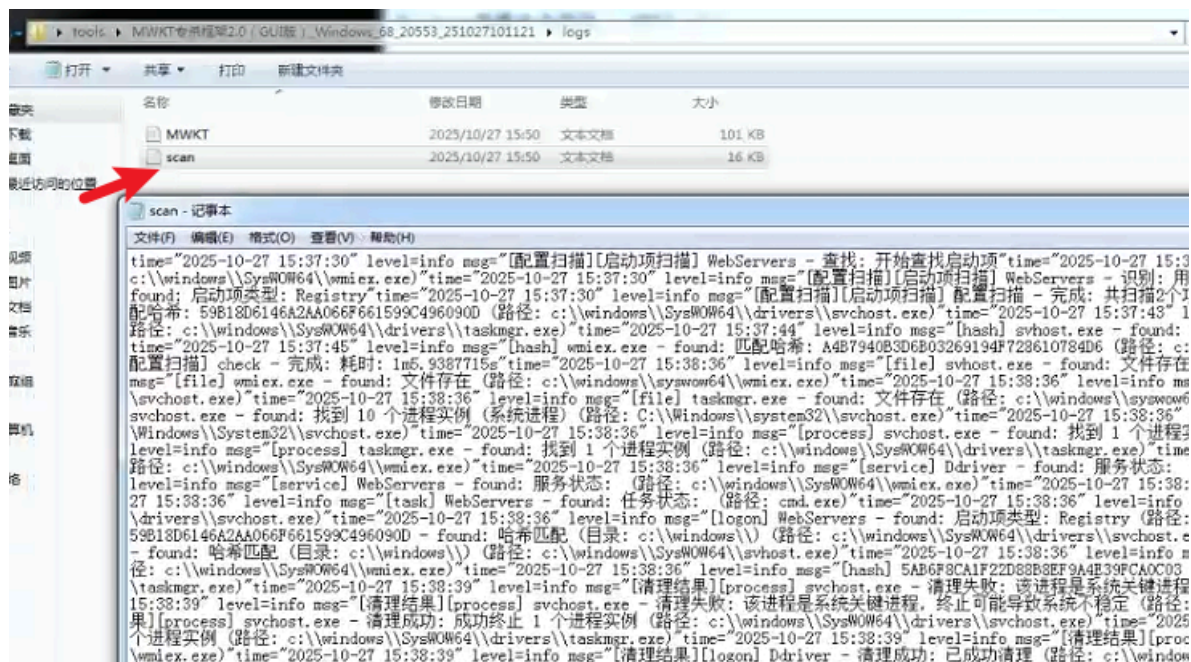
3.扫描结果会显示到扫描结果，用silverfox前置作为标记，注意：银狐只做检查，无法进行清理。





### 3、日志

1. 日志分为MWKT和scan。MWKT是程序的运行日志，scan为程序扫描日志和清理日志，需要关注的是scan.log。



## 2.如下图，为银狐检查扫描出的可疑文件：

```
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 mshwriwp.dll - 发现: 用户项 (创建: 2025-07-18 15:49:18, 修改: 2025-05-20 19:12:30) (路径: C:\Windows\WinSxS\wow64_microsoft-windows-core\mrecognition_31bf3856ad364e35_10.0.26100.1_none_da246f3668921fmsmhwriwp.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 libcefwrapper.dll - 发现: 用户项 (创建: 2025-07-18 15:49:18, 修改: 2025-05-20 19:12:30) (路径: C:\Program Files (x86)\Lenovo\PCManager\5.1.120.7041\Runtime\libcefwrapper.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 widevinecdm.dll - 发现: 用户项 (创建: 2025-07-29 08:52:59, 修改: 2025-07-29 08:52:59) (路径: C:\Users\lenovo\AppData\Local\Roaming\ Tencent\wechat\plugins\Plugins\WMPFDrm\1002\extracted\WidevineCdm.platform_specific\win_x64\widevinecdm.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 gnsdk.fp.dll - 发现: 用户项 (创建: 2025-09-11 12:10:10, 修改: 2025-09-11 12:10:10) (路径: C:\Windows\WinSxS\wow64_microsoft-windows-media\player-core_31bf3856ad364e35_10.0.26100.5074_none_b1b23ae0535ad5f0gnsdk.fp.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 DolbyDDPDecMft.dll - 发现: 用户项 (创建: 2025-09-25 11:18:05, 修改: 2025-09-25 11:18:06) (路径: C:\Program Files\WindowsApps\DolbyLaboratories.DolbyDigitalPlusDecoderOEM_1.2.581.0_x64_r1z1tebtyb220MFT\Win32\DolbyDDPDecMft.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 DolbyDDPDecMft.dll - 发现: 用户项 (创建: 2025-09-25 11:18:05, 修改: 2025-09-25 11:18:07) (路径: C:\Program Files\WindowsApps\DolbyLaboratories.DolbyDigitalPlusDecoderOEM_1.2.581.0_x64_r1z1tebtyb220MFT\Win32\DolbyDDPDecMft.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 libcefwrapper.dll - 发现: 用户项 (创建: 2025-10-14 10:07:49, 修改: 2025-05-20 19:12:30) (路径: C:\Program Files (x86)\Lenovo\PCManager\5.1.120.9262\Runtime\libcefwrapper.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 44juOxG.Kg - 发现: 用户项 (创建: 2025-10-22 10:58:50, 修改: 2016-09-19 09:55:54) (路径: C:\Program Files (x86)\demoapi\MoGs4z\44juOxG.Kg)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 Dsz.dll - 发现: 用户项 (创建: 2025-10-22 10:58:51, 修改: 2018-03-23 23:01:38) (路径: C:\Program Files (x86)\demoapi\MoGs4z\Dsz.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 PP6VCO21ZMsU.exe - 发现: 用户项 (创建: 2025-10-22 10:58:51, 修改: 2017-02-25 02:32:08) (路径: C:\Program Files (x86)\demoapi\MoGs4z\PP6VCO21ZMsU.exe)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 bolva2.dll - 发现: 用户项 (创建: 2025-10-22 11:00:22, 修改: 2024-10-21 17:59:42) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\bolva2.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 innocallback.dll - 发现: 用户项 (创建: 2025-10-22 11:00:22, 修改: 2024-10-21 17:59:42) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\innocallback.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 net4.5.2.exe - 发现: 用户项 (创建: 2025-10-22 11:00:26, 修改: 2024-10-21 17:59:44) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\net4.5.2.exe)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 DownNet.png - 发现: 用户项 (创建: 2025-10-22 11:00:28, 修改: 2024-10-21 17:59:42) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\DownNet.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 welcome_bg.png - 发现: 用户项 (创建: 2025-10-22 11:00:28, 修改: 2025-04-09 14:37:00) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\welcome_bg.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 background_welcome_more.png - 发现: 用户项 (创建: 2025-10-22 11:00:28, 修改: 2025-04-09 14:37:00) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\background_welcome_more.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 finish_bg.png - 发现: 用户项 (创建: 2025-10-22 11:00:28, 修改: 2025-04-09 14:37:00) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\finish_bg.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 button_customize_setup.png - 发现: 用户项 (创建: 2025-10-22 11:00:28, 修改: 2025-04-09 14:37:00) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\button_customize_setup.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 button_uncustomize_setup.png - 发现: 用户项 (创建: 2025-10-22 11:00:28, 修改: 2025-04-09 14:37:00) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\button_uncustomize_setup.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 slides_picture_1.png - 发现: 用户项 (创建: 2025-10-22 11:00:29, 修改: 2025-04-09 14:37:00) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\slides_picture_1.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 slides_picture_2.png - 发现: 用户项 (创建: 2025-10-22 11:00:29, 修改: 2025-04-09 14:37:00) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\slides_picture_2.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]隐藏文件 slides_picture_3.png - 发现: 用户项 (创建: 2025-10-22 11:00:29, 修改: 2025-04-09 14:37:00) (路径: C:\Users\lenovo\AppData\Local\Temp\is-RGG29.tmp\slides_picture_3.png)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 oneocr.dll - 发现: 用户项 (创建: 2025-10-28 10:24:35, 修改: 2025-10-28 10:24:44) (路径: C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2025.11100.9001.0_x64_8wekyb3d8bbwe\oneocr.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]签名无效 onnxruntime.dll - 发现: 用户项 (创建: 2025-10-28 10:24:35, 修改: 2025-10-28 10:24:51) (路径: C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2025.11100.9001.0_x64_8wekyb3d8bbwe\onnxruntime.dll)
time="2025-11-03 17:11:54" level=info msg="[银狐扫描]扫描完成 - 完成: 共发现 60 个结果
time="2025-11-04 10:37:53" level=info msg="[银狐扫描]扫描完成 - 完成: 共发现 0 个结果
time="2025-11-04 10:37:53" level=info msg="[银狐扫描]签名无效 vulkan-1.dll - 发现: 用户项 (创建: 2024-04-01 15:22:17, 修改: 2024-04-02 01:13:20) (路径: C:\Windows\WinSxS\amd64_microsoft-windows-vulkan-loader_31bf3856ad364e35_10.0.26100.1_none_0c34f0225775d0vulkan-1.dll)
time="2025-11-04 10:37:53" level=info msg="[银狐扫描]签名无效 vulkan-1.dll - 发现: 用户项 (创建: 2024-04-01 15:22:17, 修改: 2024-04-02 01:13:24) (路径: C:\Windows\WinSxS\x86_microsoft-windows-vulkan-loader_31bf3856ad364e35_10.0.26100.1_none_b0165e7e6d4a049avulkan-1.dll)
time="2025-11-04 10:37:53" level=info msg="[银狐扫描]签名无效 mshwriwp.dll - 发现: 用户项 (创建: 2025-02-06 13:43:27, 修改: 2025-02-06 13:43:27) (路径: C:\Windows\WinSxS\amd64_microsoft-windows-core\mrecognition_31bf3856ad364e35_10.0.26100.1591_none_c9bf29d328e4d08mshwriwp.dll)
```