

说明

注意!!! 一定要按照“使用方法”章节配置和操作，不想看字的可以看图

注意!!! 由于钓鱼母体的变化较大，本工具不对钓鱼母体样本提供有效检测，所能检测的均为母体释放后的后门进程和文件

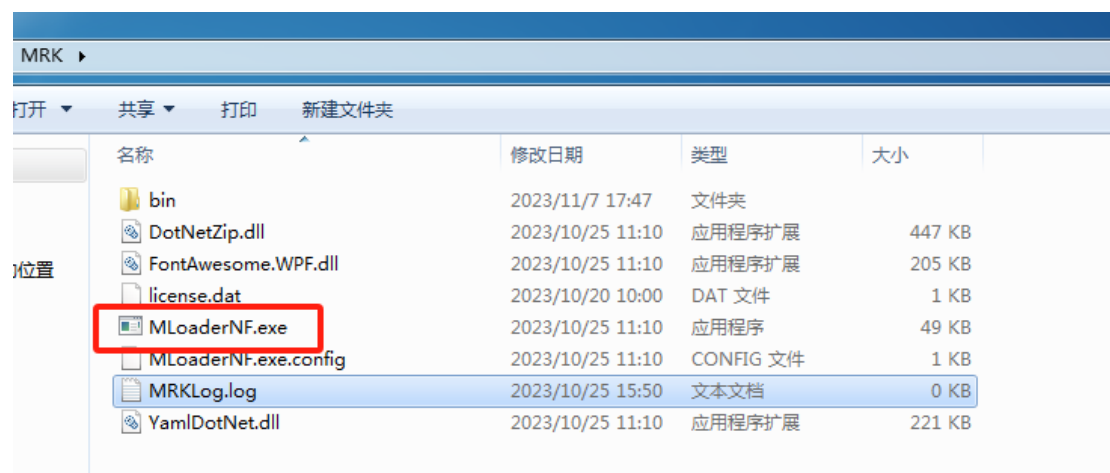
工具规则为最近频发的银狐木马收集制作而成，可能对未收集到的新版本银狐木马进程、文件无法识别，若无法对新版本银狐木马处置请将未扫描处置样本联系工号 17774 更新规则库。由于银狐木马的文件形态不断变化，无法保证将全部银狐文件处置掉，参考下例处置方法即可。

附：银狐组织目前在用第三只眼远控，安装目录默认在 C:\Users\用户名\AppData\Roaming\随机名字下。

第三只眼由于守护进程的原因，可能工具一次无法直接清除，建议根据下面“使用方法”操作扫描一遍后重启系统再到“C:\Users\用户名\AppData\Roaming\随机名称”下去删除文件夹即可

使用方法

运行 MLoaderNF.exe



在弹出的窗口中配置扫描选项勾选“文件扫描”和“进程扫描”和“注册表扫描”，并配置

- 1、勾选文件扫描，文件扫描路径可以不选择，可通过进程扫描的结果去找文件。如果要扫文件建议添加 C 盘全盘，根据系统资源设置线程数量，最小线程 1 最大 32，扫描速度可大幅提升。
- 2、进程扫描中“是否选择终止进程”选项选择“否”，或者选择“是”都行
- 3、注册表扫描中勾选“是否删除注册表键值对”选择“是”
- 4、在注册表扫描 HKEY_LOCAL_MACHINE 扫描中填入 SYSTEM
- 5、点击运行，在弹出的窗口中点击进去再按任意键即可开始扫描

MRK Loader

配置扫描选项

☐ 内核模式

线程数量: 32

☒ 文件扫描

- 是否删除文件 ☐ 是 ☒ 否
- 当文件大于 50 MB时, 跳过扫描
- 在下方选择或手动填写文件扫描路径, 点击+按钮添加新目录, 点击...按钮选择目录

+

c:\

...

☒ 进程扫描

- 是否终止进程 ☐ 是 ☒ 否
- 当进程大于 500 MB时, 跳过扫描
- 在下方指定要扫描的pid, 默认扫描全部进程

+

☒ 注册表扫描

- 是否删除注册表键值对 ☒ 是 ☐ 否
- 在下方填写注册表路径, 不包括根键

HKEY_LOCAL_MACHINE

+

system

HKEY_CURRENT_USER

+

生成配置文件预览

SpecialFiles: []

ScanPaths:

- c:\

SpecificPids: []

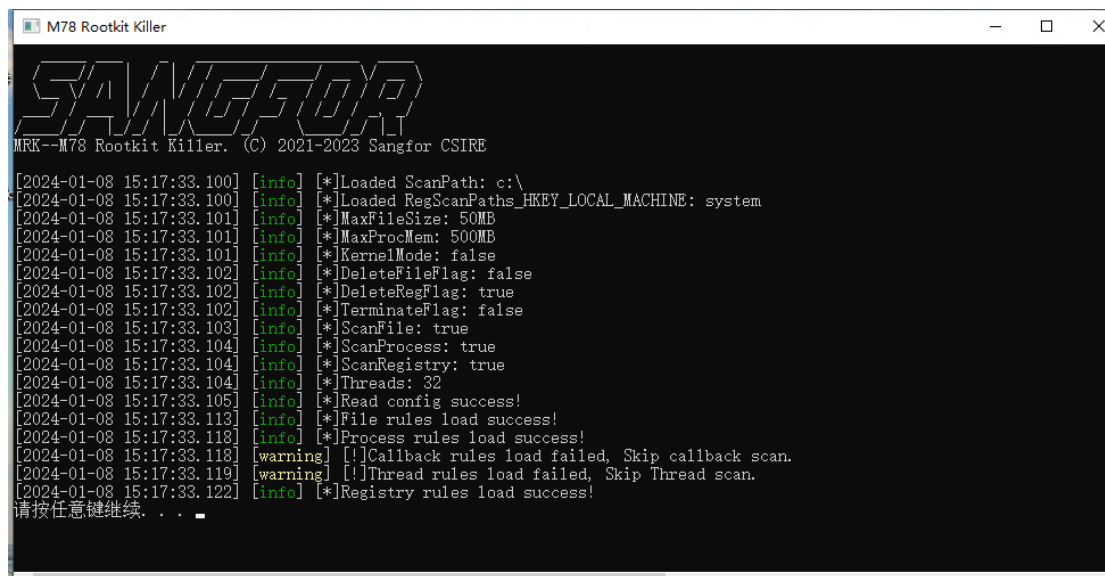
RegScanPaths_HKEY_LOCAL_MACHINE:

- system

RegScanPaths_HKEY_CURRENT_USER: []

生成Zip

直接运行



扫描效果

在根目录下的 MRKLog.log 保存着扫描结果

MRK 银狐专杀_37_17774_231221144744				
名称	修改日期	类型	大小	
bin	2023/12/26 14:46	文件夹		
DotNetZip.dll	2023/12/21 14:45	应用程序扩展	447 KB	
FontAwesome.WPF.dll	2023/12/21 14:45	应用程序扩展	205 KB	
license.dat	2023/12/21 14:47	DAT 文件	1 KB	
MLoaderNF.exe	2023/12/21 11:48	应用程序	50 KB	
MLoaderNF.exe.config	2023/12/21 14:45	CONFIG 文件	1 KB	
MRK 银狐专杀使用手册.pdf	2023/12/21 14:45	Microsoft Edge PDF ...	953 KB	
MRKLog.log	2023/12/26 14:47	文本文档	8 KB	
YamlDotNet.dll	2023/12/21 14:45	应用程序扩展	221 KB	

银狐远控后门扫描效果

存在形如 match 规则则是匹配成功,但是要注意可能存在一小部分进程误报,如杀软进程,像下面的火绒进程就是误报。匹配后下方出现 match process PID: pid,processname 即是匹配成功并结束进程如下图 pid: 5560、5604 都被扫描出但并未处置,这时候可以配合 evrything 工具找一找扫描到的进程,并删除所找到的文件,因为所使用的是白+黑技术,同目录下文件数量可能是几个

```

[2023-12-14 14:49:01.536] [warning] [!]Callback rules load failed, Skip callback scan.
[2023-12-14 14:49:01.536] [warning] [!]Thread rules load failed, Skip Thread scan.
[2023-12-14 14:49:01.539] [info] [*]Registry rules load success!
[2023-12-14 14:49:46.336] [info] [Process Scan]
[2023-12-14 14:49:46.339] [info] [Process Scan]
[2023-12-14 14:49:46.339] [info] [*]Scan Specific pid
[2023-12-14 14:49:58.781] [critical] Match Rule: gh0st_common
[2023-12-14 14:49:58.782] [critical] author: yinhu
[2023-12-14 14:49:58.783] [critical] description: yinhu common rule
[2023-12-14 14:49:58.785] [critical] group: Sangfor M78 Team
[2023-12-14 14:49:58.786] [critical] date: 2023-12-4
[2023-12-14 14:49:58.788] [critical] [+]Match process PID: 2036, HipsDaemon.exe
[2023-12-14 14:50:15.958] [critical] Match Rule: yinhu_C_sharp_backdoor_2023
[2023-12-14 14:50:15.959] [critical] author: yinhu
[2023-12-14 14:50:15.960] [critical] description: yinhu C sharp backdoor
[2023-12-14 14:50:15.962] [critical] group: Sangfor M78 Team
[2023-12-14 14:50:15.963] [critical] date: 2023-11-6
[2023-12-14 14:50:15.965] [critical] Match Rule: AsyncRAT
[2023-12-14 14:50:15.966] [critical] author: AsyncRAT C Sharp
[2023-12-14 14:50:15.967] [critical] description: AsyncRAT backdoor
[2023-12-14 14:50:15.969] [critical] group: Sangfor M78 Team
[2023-12-14 14:50:15.970] [critical] date: 2023-12-13
[2023-12-14 14:50:15.972] [critical] [+]Match process PID: 5560, 胡翰林12.11号三号机早班苹果雷蛇汇率表.exe
[2023-12-14 14:50:16.443] [critical] Match Rule: gh0st_common
[2023-12-14 14:50:16.444] [critical] author: yinhu
[2023-12-14 14:50:16.445] [critical] description: yinhu common rule
[2023-12-14 14:50:16.446] [critical] group: Sangfor M78 Team
[2023-12-14 14:50:16.447] [critical] date: 2023-12-4
[2023-12-14 14:50:16.449] [critical] [+]Match process PID: 5604, erp.exe

```

火绒杀毒软件进程

银狐后门进程

这时候转到任务管理器找到 pid 为 5604 和 5560，右键打开文件夹位置

任务管理器

文件(F) 选项(O) 查看(V)

进程 性能 应用历史记录 启动 用户 详细信息 服务

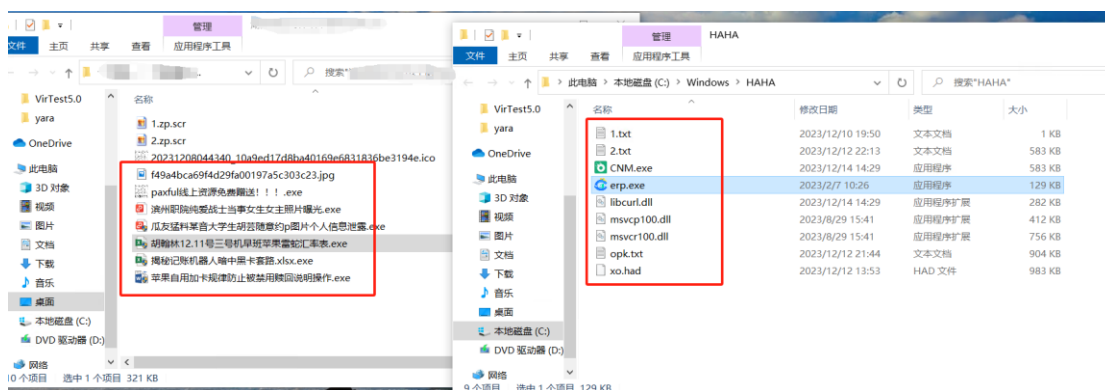
名称	PID	状态	用户名	CPU	内存(活动...	UAC 虚拟化
audiodg.exe	5064	正在运行	LOCAL SE...	00	4,656 K	不允许
ChsIME.exe	6036	正在运行	admin	00	1,080 K	已禁用
ChsIME.exe	3884	正在运行	SYSTEM	00	6,060 K	不允许
cmd.exe	4384	正在运行	SYSTEM	00	616 K	不允许
conhost.exe	5780	正在运行	SYSTEM	00	4,912 K	不允许
csrss.exe	516	正在运行	SYSTEM	00	764 K	不允许
csrss.exe	612	正在运行	SYSTEM	00	716 K	不允许
csrss.exe	1112	正在运行	SYSTEM	00	1,016 K	不允许
ctfmon.exe	5764	正在运行	admin	00	9,144 K	已禁用
dllhost.exe	6360	正在运行	admin	00	2,776 K	已禁用
dwm.exe	696	正在运行	DWM-1	00	14,744 K	已禁用
dwm.exe	4800	正在运行	DWM-2	00	37,780 K	已禁用
erp.exe	5604	正在运行	admin	00	6,736 K	不允许
explorer.exe	5916	正在运行			5,224 K	已禁用
fontdrvhost.exe	916	正在运行			972 K	已禁用
fontdrvhost.exe	912	正在运行			1,192 K	已禁用
HipsDaemon.exe	2036	正在运行			6,108 K	不允许
HRSword.exe	3012	正在运行			7,888 K	不允许
LogonUI.exe	816	正在运行			1,184 K	不允许
lsass.exe	752	正在运行			5,548 K	不允许
MLoaderNF.exe	1884	正在运行			8,164 K	已禁用
MRK64.exe	5704	正在运行			9,656 K	不允许
msedge.exe	3652	正在运行			3,468 K	已禁用
msedge.exe	3928	正在运行			1,408 K	已禁用
msedge.exe	8296	正在运行			6,672 K	已禁用
msedge.exe	8332	正在运行			5,132 K	已禁用
msedge.exe	8368	正在运行	admin	00	3,604 K	已禁用
msedge.exe	9100	正在运行	admin	00	16,500 K	已禁用
msedge.exe	1572	正在运行	admin	00	40,656 K	已禁用
OneDrive.exe	9124	正在运行	admin	00	21,144 K	已禁用
rdpclip.exe	5248	正在运行	admin	00	2,124 K	已禁用
Registry	108	正在运行	SYSTEM	00	4,504 K	不允许
RuntimeBroker.exe	6992	正在运行	admin	00	4,960 K	已禁用
RuntimeBroker.exe	7276	正在运行	admin	00	5,548 K	已禁用

右键菜单选项:

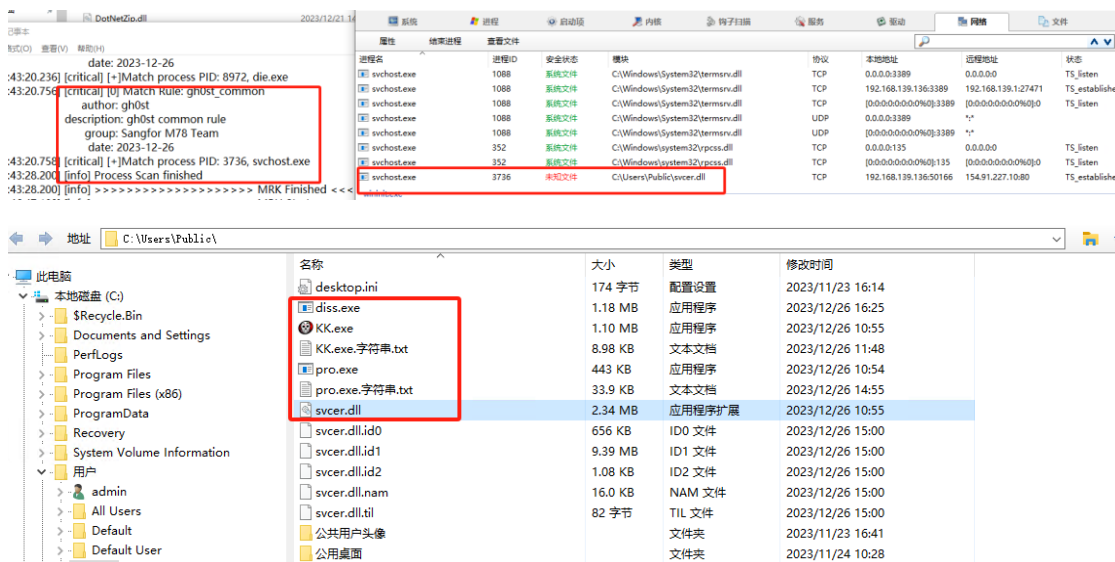
- 结束任务(E)
- 结束进程树(T)
- 提供反馈(B)
- 设置优先级(P)
- 设置相关性(F)
- 分析等待链(A)
- UAC 虚拟化(V)
- 创建转储文件(C)
- 打开文件所在的位置(O)
- 在线搜索(N)
- 属性(R)
- 转到服务(S)



就可找到后门文件路径，这时把进程和相关后门文件删除即可



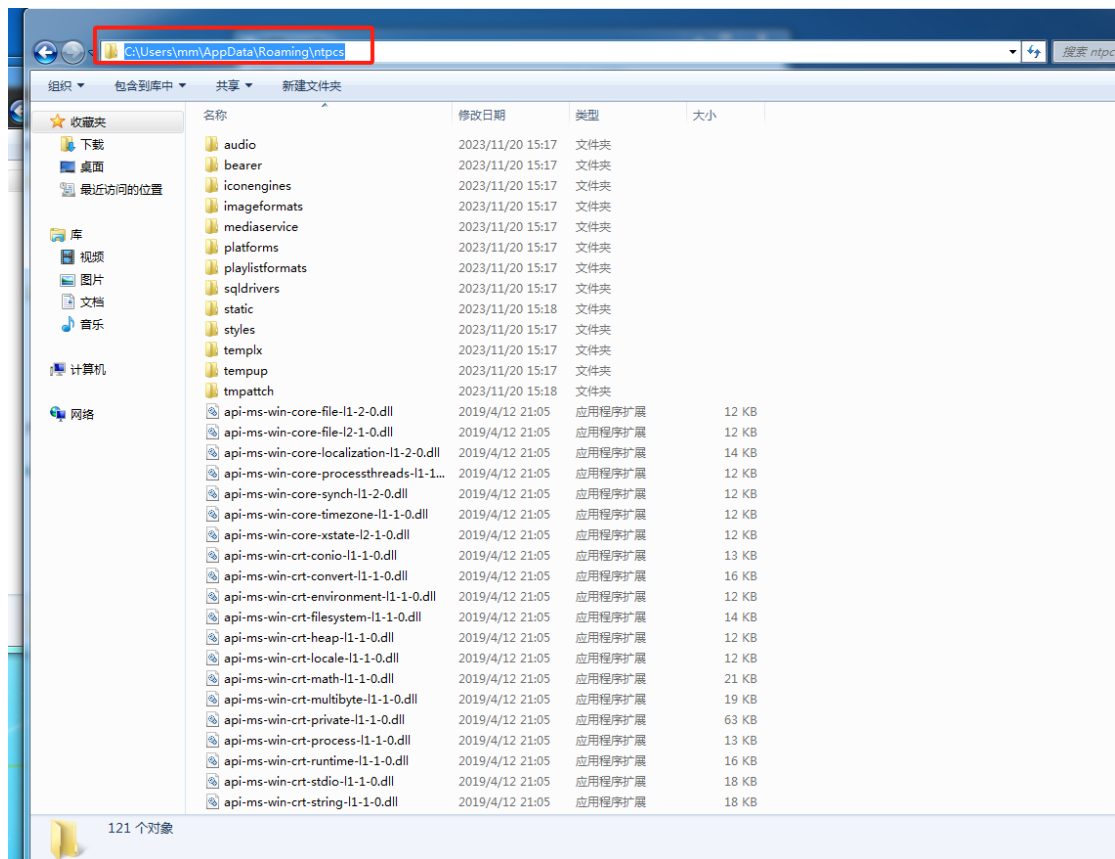
特殊情况下还存在另一个持久化项，一个恶意 dll 被加载到了 svchost.exe 进程里，这时候把进程结束再删除 dll 即可



第三只眼后门扫描效果

清除注册表内容再重启删除文件即可

第三只眼远程控置文件路径默认为 C:\Users\用户名\AppData\Roaming\随机名称，如果存在可在扫描结束后把文件夹删除即可



第三只眼进程扫描效果，扫到进程后再通过进程去找文件即可

```
[2023-11-20 15:50:26.728] [critical] Match Rule: process_3eye
[2023-11-20 15:50:26.732] [critical]   author: 3eye
[2023-11-20 15:50:26.734] [critical]   description: 3eye-backdoor
[2023-11-20 15:50:26.736] [critical]   group: Sangfor M78 Team
[2023-11-20 15:50:26.737] [critical]   date: 2023-11-20
[2023-11-20 15:50:26.739] [critical] [!]Match process PID: 2436, sdcsvr.exe
[2023-11-20 15:50:26.743] [critical] [!]terminate success.
[2023-11-20 15:50:26.744] [info] Scan process PID: 2452, VGAuthService.exe
[2023-11-20 15:50:27.195] [info] Scan process PID: 2460, ntpqs.exe

[2023-11-20 15:50:27.816] [critical] Match Rule: process_3eye
[2023-11-20 15:50:27.820] [critical]   author: 3eye
[2023-11-20 15:50:27.821] [critical]   description: 3eye-backdoor
[2023-11-20 15:50:27.823] [critical]   group: Sangfor M78 Team
[2023-11-20 15:50:27.824] [critical]   date: 2023-11-20
[2023-11-20 15:50:27.825] [critical] [!]Match process PID: 2460, ntpqs.exe
[2023-11-20 15:50:27.826] [critical] [!]terminate success.
[2023-11-20 15:50:27.840] [info] Scan process PID: 2492, vmttoolsd.exe
[2023-11-20 15:50:28.402] [info] Scan process PID: 2500, vm3dservice.exe
[2023-11-20 15:50:28.699] [info] Scan process PID: 2524, svchost.exe
[2023-11-20 15:50:28.701] [error] [!]OpenProcess failed! Skip this process PID: 2524, svchost.exe
[2023-11-20 15:50:28.702] [info] Scan process PID: 2532, MsMpEng.exe
[2023-11-20 15:50:28.703] [error] [!]OpenProcess failed! Skip this process PID: 2532, MsMpEng.exe
[2023-11-20 15:50:28.704] [info] Scan process PID: 2664, vm3dservice.exe
[2023-11-20 15:50:29.024] [info] Scan process PID: 8, svhsrv.exe

[2023-11-20 15:50:30.297] [critical] Match Rule: process_3eye
[2023-11-20 15:50:30.302] [critical]   author: 3eye
[2023-11-20 15:50:30.303] [critical]   description: 3eye-backdoor
[2023-11-20 15:50:30.304] [critical]   group: Sangfor M78 Team
[2023-11-20 15:50:30.305] [critical]   date: 2023-11-20
[2023-11-20 15:50:30.308] [critical] [!]Match process PID: 8, svhsrv.exe
[2023-11-20 15:50:30.311] [critical] [!]terminate success.
[2023-11-20 15:50:30.312] [info] Scan process PID: 916, dilhost.exe
[2023-11-20 15:50:30.668] [info] Scan process PID: 792, WmiPrvSE.exe
[2023-11-20 15:50:31.073] [info] Scan process PID: 3288, msdtc.exe
[2023-11-20 15:50:31.323] [info] Scan process PID: 3864, WmiPrvSE.exe
[2023-11-20 15:50:31.958] [info] Scan process PID: 4024, svchost.exe
[2023-11-20 15:50:32.140] [info] Scan process PID: 4024, svchost.exe
```

第三只眼注册表持久项删除效果

```
-----
[2024-01-08 11:29:50.652] [info] [Registry Scan]
[2024-01-08 11:31:06.030] [critical] [0] Match Rule: reg_3eye
      author: 3eye
      description: 3eye-backdoor
      group: Sangfor M78 Team
      date: 2024-1-6
[2024-01-08 11:31:06.031] [critical] [*] Matched Value Data, system\ControlSet001\Services\sdypnt, ImagePath -> C:\Users\admin\AppData\Roaming\ntpcs\ntpq.exe -s sdypnt
[2024-01-08 11:31:06.032] [info] [+] Delete system\ControlSet001\Services\sdypnt -> ImagePath success
[2024-01-08 11:31:06.034] [info] [+] Delete system\ControlSet001\Services\sdypnt -> DisplayName success
[2024-01-08 11:31:06.036] [info] [+] Delete system\ControlSet001\Services\sdypnt -> ObjectName success
[2024-01-08 11:31:06.038] [info] [+] Delete system\ControlSet001\Services\sdypnt -> Description success
[2024-01-08 11:31:08.548] [critical] [0] Match Rule: reg_3eye
      author: 3eye
      description: 3eye-backdoor
      group: Sangfor M78 Team
      date: 2024-1-6
[2024-01-08 11:31:08.550] [critical] [*] Matched Value Data, system\ControlSet001\Services\sucata, ImagePath -> C:\Users\admin\AppData\Roaming\ntpcs\sdcsr.exe -s sucata
[2024-01-08 11:31:08.552] [info] [+] Delete system\ControlSet001\Services\sucata -> ImagePath success
[2024-01-08 11:31:08.554] [info] [+] Delete system\ControlSet001\Services\sucata -> DisplayName success
[2024-01-08 11:31:08.556] [info] [+] Delete system\ControlSet001\Services\sucata -> ObjectName success
[2024-01-08 11:31:08.558] [info] [+] Delete system\ControlSet001\Services\sucata -> Description success
[2024-01-08 11:32:51.884] [info] Registry Scan Finished
-----
```