1. 设置项变更说明
   1. 原设置项如下图



不要了

* 1. 变更如下
     1. 将“文件类型”变更为“扫描类型”
     2. 设置项目变更为“扫描PUA”（checkbox），“递归扫描目录”（checkbox），“扫描大于20M的文件”（checkbox）
     3. “宏病毒查杀”全不要了
     4. 其他不变
  2. 相关设置可写入配置文件中

1. 引擎说明：
   1. 病毒库已经更新
   2. 执行查毒的命令（**需要在子线程中执行**）：

clamscan.exe D:\antivirus\test\

查询路径D:\antivirus\test\下的文件（不含子目录）

备注：查询的路径可以是多个

* 1. 根据配置选项添加扫描参数
     1. 勾选“扫描PUA”后扫描时添加参数“--detect-pua”
     2. 勾选“递归扫描目录”后扫描时添加参数“-r”
     3. 不勾选“扫描大于20M的文件”后扫描时添加参数“--max-filesize=20M”
     4. 勾选“扫描压缩包”后扫描时添加参数“--scan-archive=no”
     5. 每有一项白名单添加一个参数“--exclude=REGEX”
        1. 由于选项支持正则表达式windows下的全路径的分隔符“\”应变更为“\\”
        2. 由于该选项只能接一个项目，所以当白名单为多条时，每条对应一个参数项
        3. 如果白名单项为“全路径”时，建议后面添加“$”，表示该行结束，避免多匹配文件
     6. 处理方式
        1. 处理方式为“手动处理”时，在扫描后查看威胁列表时点击后面的按钮，由python的api处理；
        2. 处理方式为“自动处理”时，
           1. 勾选“备份到恢复区”时，添加参数“--move=Path”Path为隔离区路径
           2. 未勾选“备份到恢复区”时，添加参数“--remove=yes”
     7. 每个选项以空格分隔

示例：

clamscan.exe -r --exclude=D:\\antivirus\\test\\clam.exe$ D:\antivirus\test\

* 1. 输出内容处理
     1. 正常情况输出内容
        1. 文件正常

D:\antivirus\test\Makefile: OK

界面仅回显扫描文件的全路径名，即“： ”（第二个冒号后有个空格）之前的内容，该信息不计入数据库扫描明细表

* + - 1. 文件有威胁（未添加“--detect-pua”参数时）

D:\antivirus\test\clam.exe: Clamav.Test.File-6 FOUND

“： ”后，“FOUND”前是威胁名称即“Clamav.Test.File-6”，该信息应计入数据库扫描明细表，其中“FOUND”字应该抛弃；“： ”前的全路径应在界面回显

* + - 1. 文件有威胁（已添加“--detect-pua”参数时）

D:\antivirus\test\clam.exe: PUA.Win.Packer.AcprotectUltraprotect-1 FOUND

在示例病毒中仅仅是病毒名称有变化，处理与上面一项完全相同

* + - 1. 自动移动文件到安全区

添加“--move=”参数是发现威胁后立即将有威胁的文件移动到安全区，在“FOUND”行后会有另一行信息：

D:\antivirus\test\clam.exe: moved to 'D:\antivirus\isol\\clam.exe'

该信息不需要显示，需要记入数据库隔离区表，变更明细表对应数据“处理类型”为“修复”

* + - 1. 自动删除文件

添加参数“--remove”，发现威胁后立即将有威胁的文件删除，在“FOUND”行后会有另一行信息：

D:\antivirus\test\clam.exe: Removed.

该信息不需要显示，不需要记入数据库，变更明细表对应数据“处理类型”为“修复”

* + - 1. 文件是白名单中的

扫描时如果文件是白名单中的一项会显示如下信息：

D:\antivirus\test\clam.exe: Excluded

该信息仅回显文件的全路径名，不记入数据库

* + - 1. 汇总信息

文件扫描完成后会输出汇总信息

其中有用数据为：

* + - * 1. Infected files: 已发现威胁数量
        2. Time: 扫描消耗时间
        3. Scanned files: 扫描文件总数
    1. 其他情况输出内容：

其他情况输出的消息为错误或警告等，暂不处理。

* 1. 其他处理
     1. 查询病毒库信息

执行命令 clamconf.exe -n

返回内容中“daily.cld:”或“daily.cvd:”开头的行是病毒库信息