自定义规则教程手册

序言

本教程适用于火绒安全个人版第五代，主要为想学习自定义规则的人群所编写，希望读者能通过本教程获得很大的帮助。本人文笔有些浅薄，部分词语表达可能有所不当，但我会以最通俗易懂的方式尝试让读者理解这篇教程的内容。

本篇教程共五大章节，简短的说明通配符、文件规则、注册表规则、执行规则和合理运用自定义规则功能，每章节都有举例并在部分章节加入实训题，让读者能够通过实践来增强自己的规则编写能力。

本人鼓励这篇教程的转载、修改和再次创作，本教程基于火绒安全软件个人版编写，内容会包含部分软件截图等内容。如有侵权等问题，请联系本人邮箱 Me@mylake.club 删除处理。

云梦泽 编写

目录

第一章-理解通配符

火绒规则包编写需要对软件支持的三个通配符有基本的了解，便于后期更灵活的编写规则包。

符号	符号名称	符号含义
*	星号符	表示任意长度字符
?	问号符	表示一个长度字符
>	大于号	表示一个目录(不包括该目录的下层目录)

例子：

C:\Windows* 作用域:window 目录下所有文件和目录
C:\Users*\Desktop\ 作用域:Users 目录下“任意目录下”的 Desktop 目录下
C:\Program Files\Bonjour*.exe 作用域: Bonjour 目录下所有的 exe 文件(可执行文件)
C:\Program Files\Dolby\dax3api* 作用域: Dolby 目录下以 dax3api 开头的任意格式文件或者目录

C:\Windows\? 作用域:window 目录下只有 1 个字符的文件或文件夹
C:\Users\? \Desktop\ 作用域:Users 目录下只有一个字符的目录的 Desktop 目录下
C:\Program Files\Bonjour\? .exe 作用域: Bonjour 目录下只有一个字符的 exe 文件(可执行文件)
C:\Program Files\Dolby\dax3api? 作用域: Dolby 目录下以 dax3api?命名文件或者目录

C:\Windows\> 作用域:window 目录下的文件

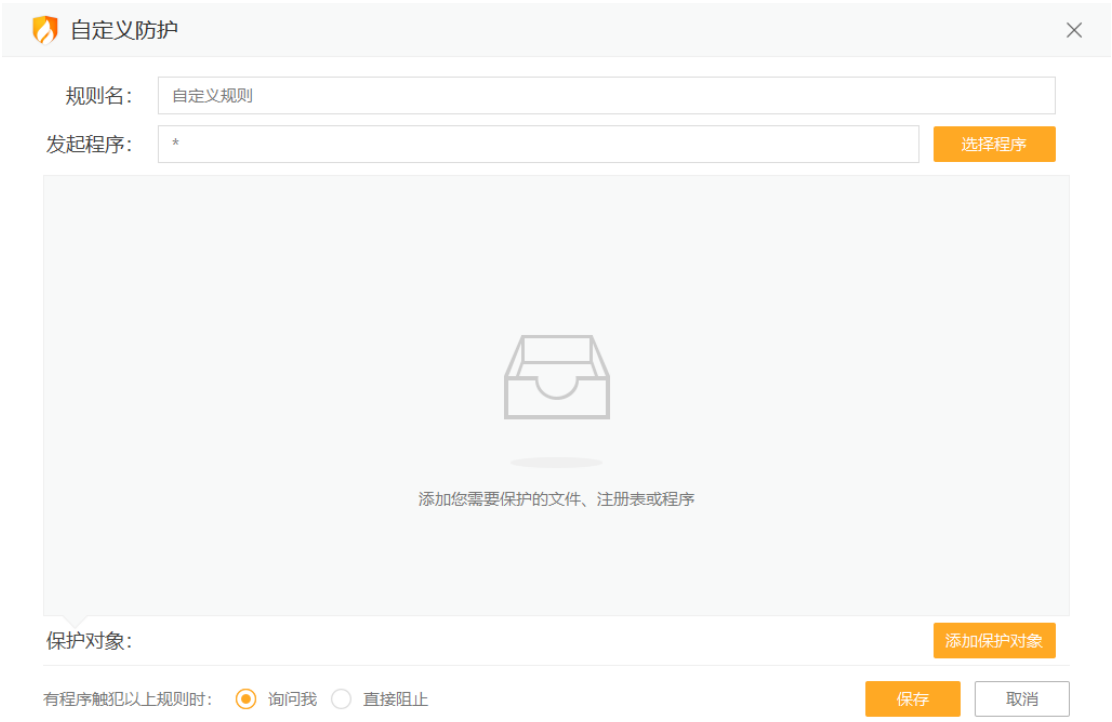
以上是三种通配符的举例,并分别说明了作用,读者只需要理解即可。

第二章-文件规则

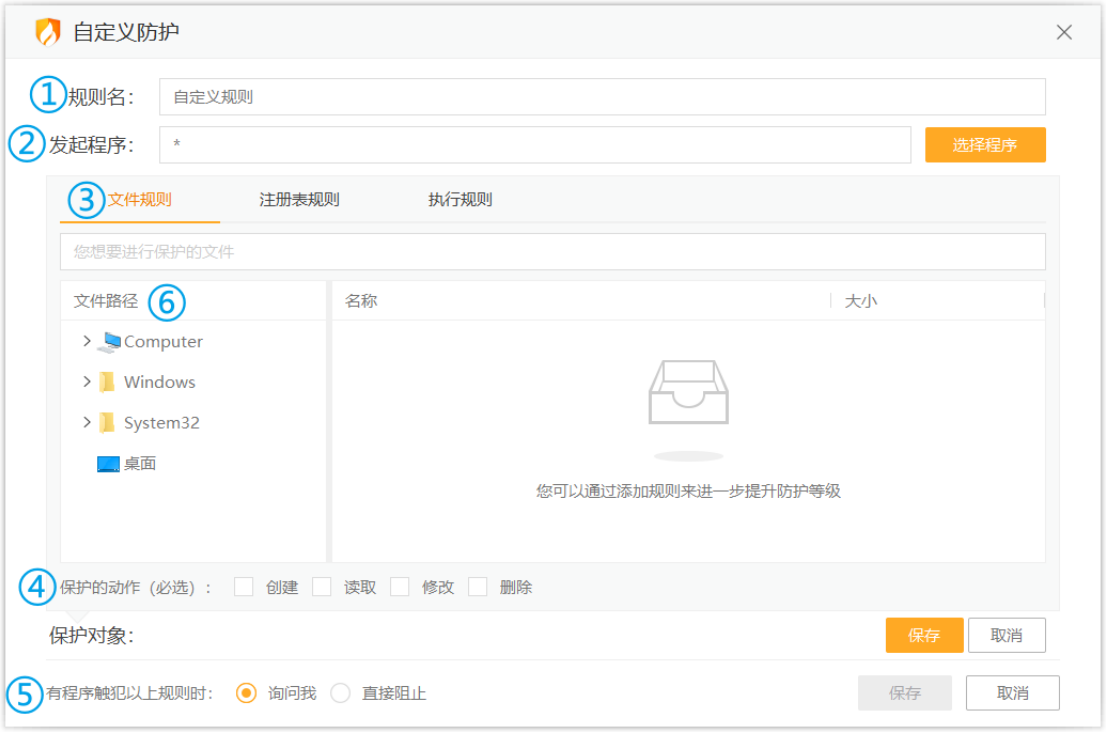
本章节学习自定义规则的文件规则，适用于对文件的**创、读、修、删**四个操作。

通过打开安全设置，找到高级防护->自定义防护，然后点击右下角添加规则

在点击添加规则后，如下图：



随后再次点击右下角的添加保护对象



上图就是规则包的标准编写界面

①：编写规则的命名

②： 发起程序则表示某个程序对文件规则的四项操作，一般默认*

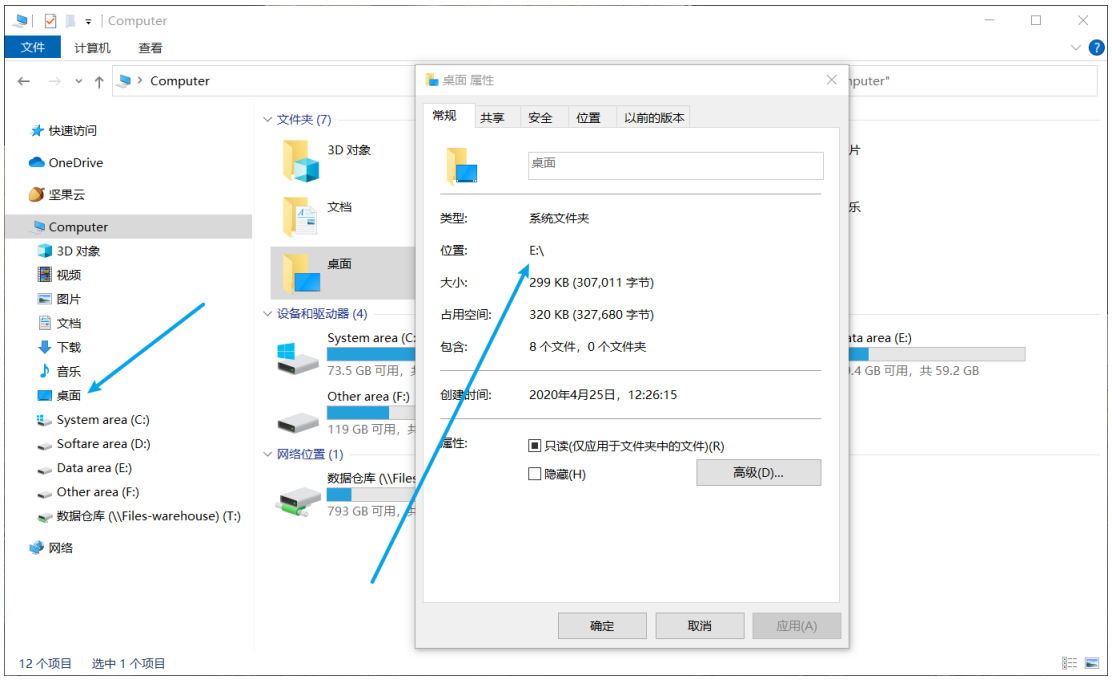
③：表示当前编写的是文件规则

④：对四项操作的的控制

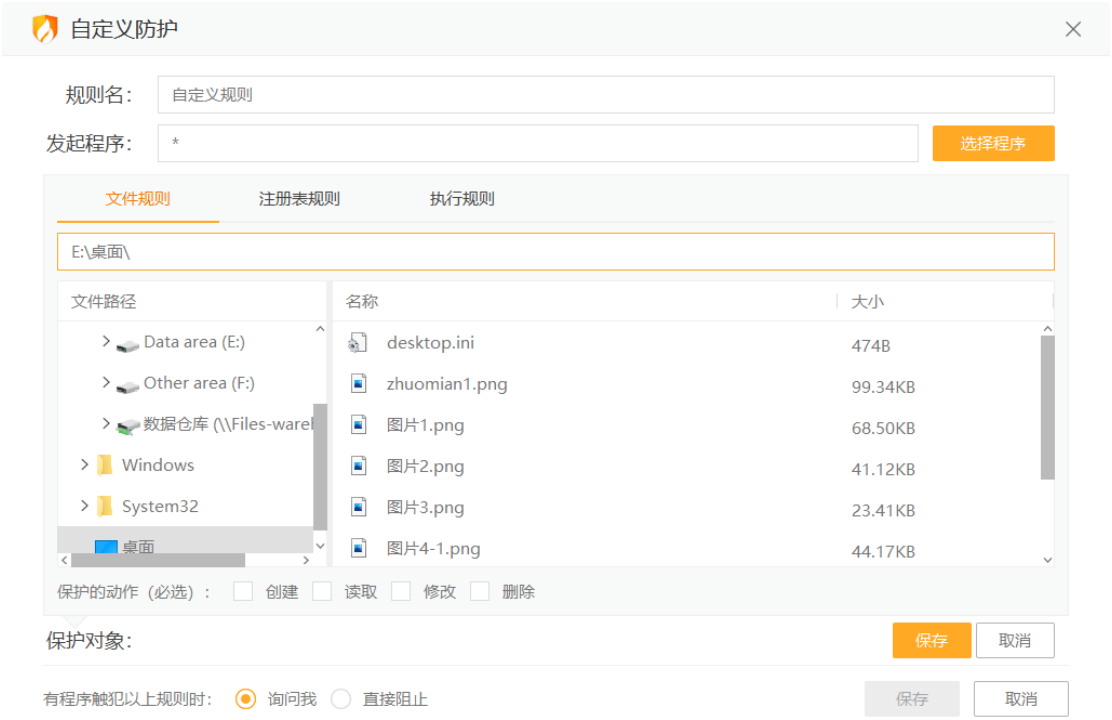
⑤：触犯规则后是否右下角弹出询问框

⑥：整个电脑的文件路径，可以通过点击来选择(通常路径是通过复制粘贴到上面的栏里)

随后尝试编写一个规则，比如禁止桌面创建文件和文件夹，首先要找到桌面的绝对路径，可以通过在“我的电脑”里面右侧的快速访问栏中点击桌面查看属性即可找到桌面的绝对路径。



接着复制位置路径到编写界面



可以看到如上图所示，还需要在目录后加上*星号，随后勾选创建即可。

若是不想让桌面内容被删除，也可以勾选删除，具体思路还需读者自己灵活配置。

假如桌面有名为 juemi.docx 的文档，为了避免被家人误删或者点开查看，可以尝试编写规则：E:\桌面\juemi.docx，把保护动作的读取和删除勾选上，保存规则即可。

章节实训

有需求，请在 C 盘根目录下创建一个名为 Test 的文件夹，在里面放入名为 test.txt 的文件，然后这个目录不能够被查看，请编写规则实现这个功能。(实现功能后需要删除规则，然后再删除目录)

第三章-注册表规则

注册表规则和文件规则在编写过程方面类似，只是把文件路径转变成注册表路径。

学习注册表规则需要对注册表有一定程度的了解，如果不了解请跳过本章节进入第四章。

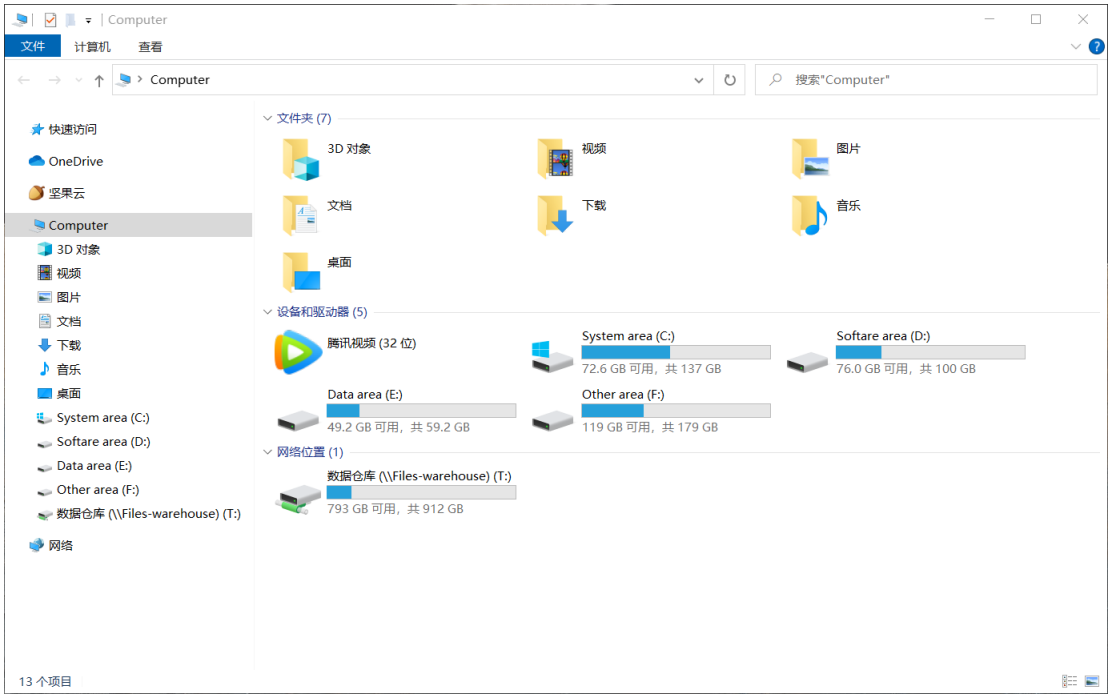
尝试用注册表规则禁止新安装的程序注册开机自启。

开自启的注册表路径如下:
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run

通过复制粘贴到编写规则的栏上面，再 Run 目录跟上*星号符，勾选修改并保存即可。

章节实训

“我的电脑”里面会出现腾讯视频，虽然能删除，但是过段时间又出现了，请编写规则阻止其重新出现(合理运用搜索引擎)。


Computer
文件
计算机
查看
Computer
搜索"Computer"
快速访问
OneDrive
坚果云
Computer
3D 对象
视频
图片
文档
下载
音乐
桌面
System area (C:)
Softare area (D:)
Data area (E:)
Other area (F:)
数据仓库 (\\Files-warehouse) (T:)
网络
文件夹 (7)
3D 对象
视频
图片
文档
下载
音乐
桌面
设备和驱动器 (5)
腾讯视频 (32 位)
System area (C:)
72.6 GB 可用，共 137 GB
Softare area (D:)
76.0 GB 可用，共 100 GB
Data area (E:)
49.2 GB 可用，共 59.2 GB
Other area (F:)
119 GB 可用，共 179 GB
网络位置 (1)
数据仓库 (\\Files-warehouse) (T:)
793 GB 可用，共 912 GB
13 个项目

第四章-执行规则

执行规则可以对 exe 文件的执行进行控制，操作选项只有执行并且默认勾选。

这个功能主要阻止家里小孩玩游戏挺有用，把游戏目录内的主程序填入，然后左下角选择直接阻止。

章节实训

试一试把 QQ 给阻止掉！

第五章-合理使用

规则编写注意事项：

1. 火绒本身的目录以及火绒本身的程序对规则是免疫的，也就是说尝试阻止火绒目录内容做任何修改是无效的。
2. 学习过程中规则编写后，养成良好的学习习惯请删除无用的规则。
3. 切记不能够尝试 C:*这种类型的编写，一不小心发生谁也不知道。
4. 想折腾规则的话，比较建议装个虚拟机在里面随便玩。
5. 灵活使用搜索引擎。

结束

教程编写日期:2021 年 8 月 2 日星期一

感谢读者能够耐心的看完本篇教程，相信你能够编写出日常使用的基本规则包，想要更进一步，还望能够学习了解更多的知识提升自己的能力。