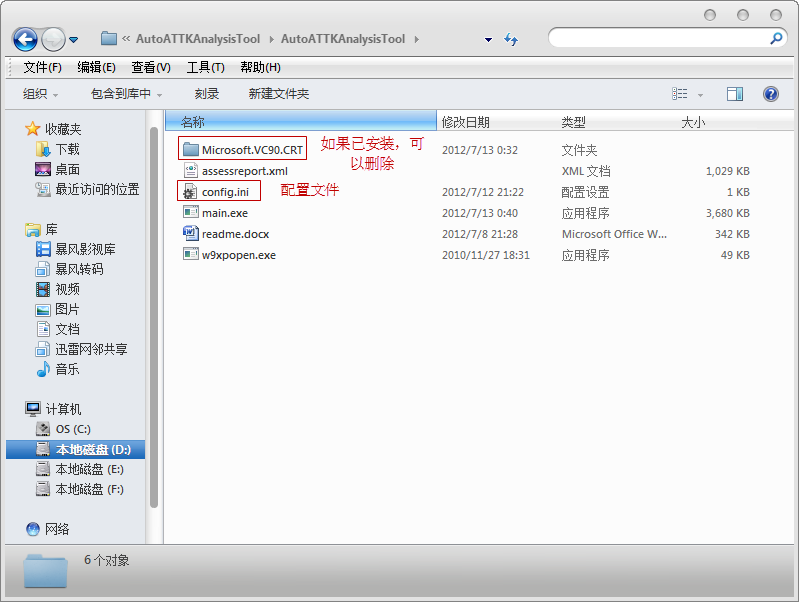
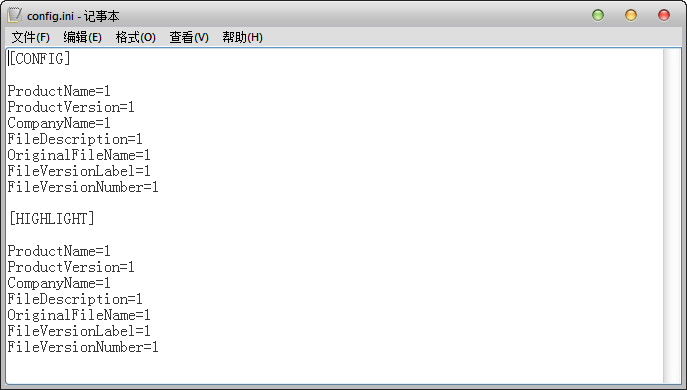
**Auto ATTK Analysis Tool**

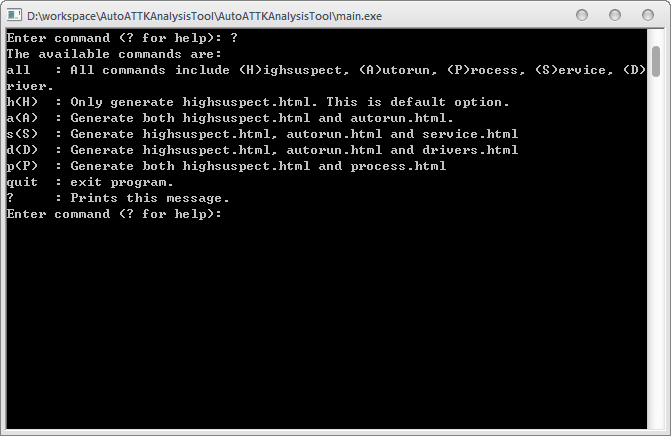
1. 以下是目录结构，如果你机器中已经安装了python解释器（最好是Python2.7）或者是VS2008，那么你的机器默认已经安装了Microsoft.VC90.CRT中的msvcr90.dll。如果如此，你可以将目录中的Microsoft.VC90.CRT文件夹删除以节省大小。



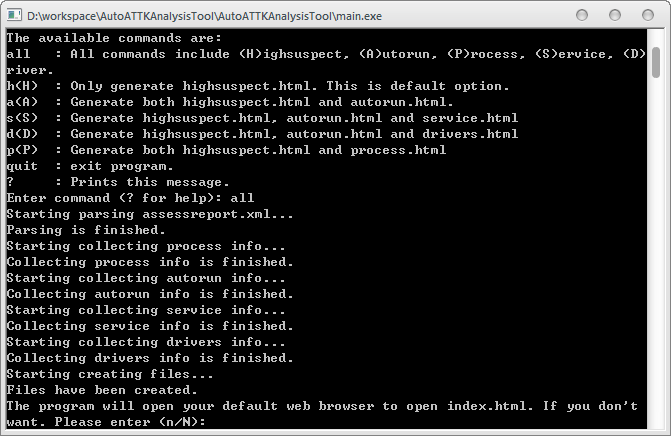
注：config.ini不再是白名单配置，有[CONFIG]和[HIGHLIGHT]两个section，其中分别有文件的所有版本信息，如果设为1则其是否为空会当作判断可疑或者高亮显示的依据。设为0则不会对其敏感。建议[CONFIG]中全部设为1，[HIGHLIGHT]可以自定义，自己觉得哪些信息为空不会可疑，就设为0.



1. 使用时需要将case中提交上来的ATTK日志中的assessreport.xml文档放入当前目录中，然后执行main.exe，界面如图，输入?即可看使用命令（目前最好使用all，这样能收集所有信息）：



1. 使用命令all并回车，会解析assessreport.xml并生成html，生成完毕后会提示程序会用默认的浏览器打开index.html，如果不需要则输入n/N，其他输入会自动打开index.html：



1. 目前工具只对xml解析，将问题分类为HighSuspect(高可疑)、Autorun(run，Winlogon等自启动)、Process(进程)、Service(服务)、Drivers(驱动程序)5项：

|  |
| --- |
|  |

可以看到现在可疑列表中分为4个级别，分别用不同颜色表示，红>橙>蓝>灰

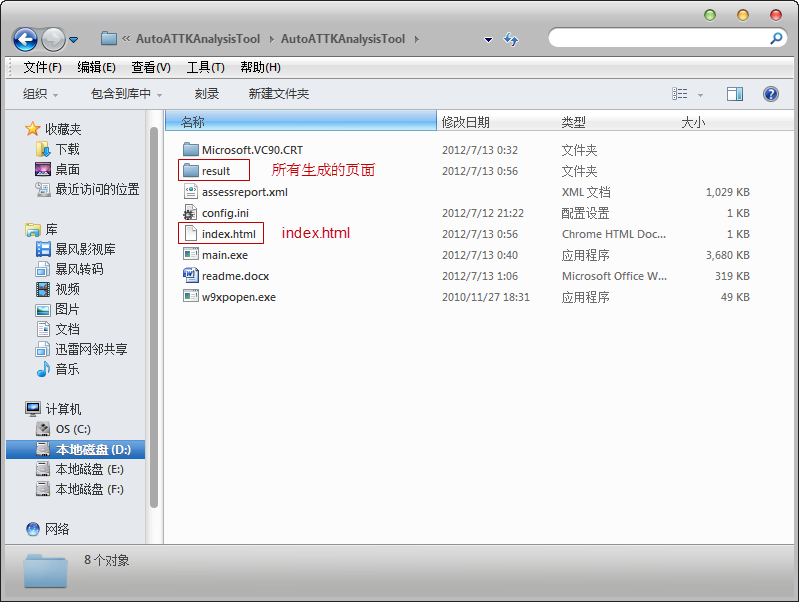
红：无全部config.ini中[HIGHLIGHT]设置为1的版本信息，且存在启动项、服务或进程。

橙：无全部config.ini中[HIGHLIGHT]设置为1的版本信息，但不存在启动项、服务或进程。

蓝：无任何config.ini中[CONFIG]设置为1的版本信息，存在启动项、服务或进程。

灰：无任何config.ini中[CONFIG]设置为1的版本信息，但不存在启动项、服务或进程。

1. 最后是程序运行完的目录结构，打开index.html即可看到所有结果：



***较上一版本的改进：***

1. 进程列表名截取以exe截取，修改为以.exe截取。感谢Zero
2. 进程列表树根节点换行问题。
3. 更改逻辑把文件版本信息缺少，但是只出现了一次（没有在启动项或进程中的）的文件也列出来了，高度可疑为橙色，非高度可疑为灰色。同时改进了进程树。感谢Jack
4. 因为MD5问题去除白名单设置，Config.ini改为设置可疑列表依据版本信息项自定义和高亮（红、橙）显示自定义。感谢Jacky
5. 设置超链接点击过后不变色，文件信息字体缩小，一目了然。感谢Jacky