

深思数盾加壳工具使用手册（Windows 版）

使用说明与支持范围

适用于 C、C++、Delphi、VB、VC++、PB、BCB 等语言开发的 exe、dll 等程序保护。

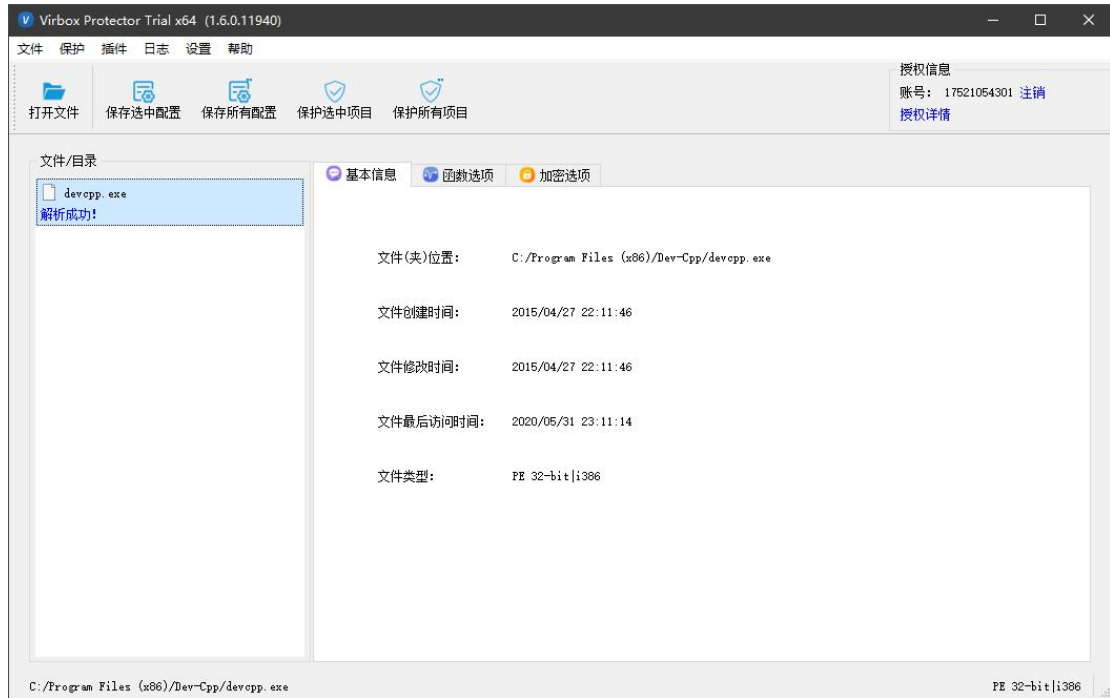
操作流程

- 将需要保护的 exe 或 dll 文件导入 *Virbox Protector* 中
- 配置函数选项，设计个性化的保护方案
- 配置加密选项
- 执行保护
- 备份原始文件，将受保护的文件更名后替换原文件，保存好配置文件

范例

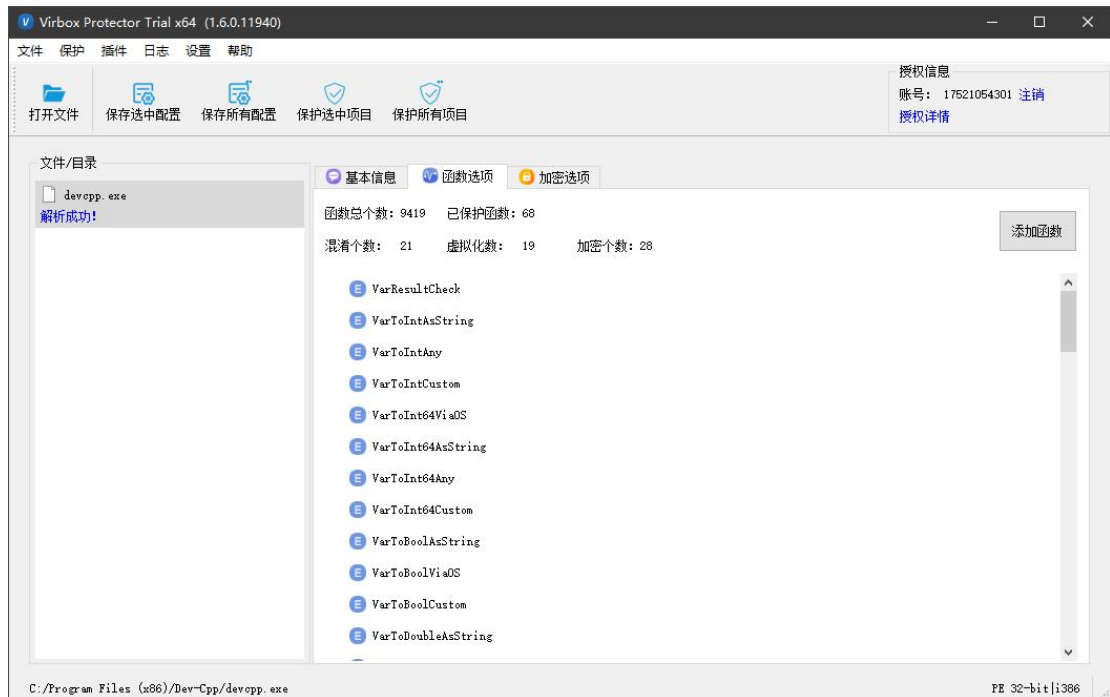
项目	版本
操作系统	Windows 10 家庭中文版
演示程序	Dev C++ V5.11
开发语言	Delphi

1. 导入文件



将需要保护的 executable 文件或库文件导入 *Virbox Protector Trial* 中

2. 配置函数选项



配置函数选项，设计个性化的保护方案

温馨提示：保护方式的安全性：代码虚拟化 > 代码混淆 > 代码加密。

3.配置加密选项



配置加密选项

①自定义输出目录

可以修改程序保护后生成文件的路径和名称，默认为与被保护程序同一路径

②导入表保护

去除原程序的导入表，将导入地址表(IAT) 替换为修复函数，由壳代码接管导入函数的跳转。可以达到保护程序的函数外部调用，干扰逆向分析、防脱壳的作用。

温馨提示：基于安全的考虑，我们建议您使用这个选项。

③压缩

将原始的代码段与数据包打包并压缩，将原始程序入口（OEP）替换为壳代码，运行时由壳代码将代码 段与数据段还原，并进行一些重定位等操作，使程序能正常运行。减小程序体积的同时可以防止静态反编译和程序补丁。

温馨提示：压缩模块需要一个固定大小的空间，如果被保护的 application 体积较小，压缩的效果并不明显，甚至还有可能出现体积增加的情况，但对于体积较大的程序效果比较明显。

④资源保护

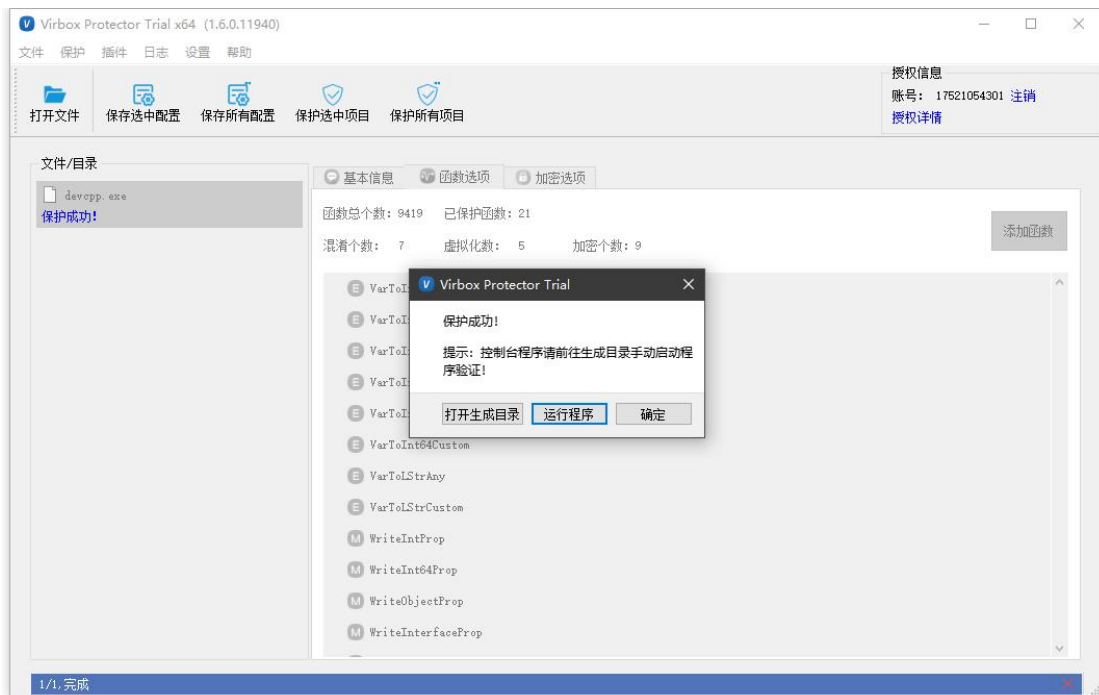
加密资源段，对被保护程序的资源区段进行加密，运行的时候需要用户使用相应许可进行解密方可使用程序。

⑤插件

- **检测硬件断点：**检测程序中是否设置硬件断点，若检测到则程序直接终止运行；
- **检测内存断点：**检测程序中是否设置内存断点，若检测到则程序直接终止运行；
- **内存检查：**检测程序中内存是否被修改，若检测到则程序直接终止运行；

温馨提示：代码加密和内存检测有冲突，不可同时使用。

4.执行保护



保护成功

5.替换文件

温馨提示：加壳后的程序会在输出目录下生成两个新文件：*devcpp.exe.ssp* 和

devcpp.ssp.exe

devcpp.ssp.exe 为保护后的程序，请备份好未经保护的 *devcpp.exe*，并将 *devcpp.ssp.exe* 名称修改为 *devcpp.exe*。

devcpp.exe.ssp 为配置文件，保存了加密过程中的所有配置项目。