Getshell

前言

本项目来源于有段时间看到了群友玩网络上的破解游戏，我虽然对此没有看法，但是突然想到了如果发布破解游戏的是一个malicious发布者，那么发布者可以在游戏中植入木马病毒。本项目实现了一个早期形态的木马，具体原理是将自解压程序、游戏启动器、恶意脚本的加密写入同一文件，通过自解压程序获得游戏文件和脚本文件，启动游戏后在后台解密脚本程序并运行。本项目主要是实现了这样的注入框架，根据需求可能再加入隐藏图标、要求用户付费才能启动等恶意功能。

文件结构

恶意程序（可自定义）

服务端程序（可自定义）

游戏启动器（可自定义）

一键式生成工具util5.py（5是因为这是第五版）

原理：

一键式工具util5.py首先生成自解压程序的代码，并编译成可执行文件。由于大小不定，一般要编译3次（自动）。随后加密指定的脚本程序（必须是可执行程序），最后合并三个文件。

需要自定义输入输出的话，可以更改util5.py的全局变量部分实现。

如果想要改变线程名称和产生独立进程，可以更改step2.data。