PVZ Cheater汇编小组作业报告

覃诗睿 朱旭 张泽卿

1. 开发环境

操作系统：Windows 10/11

IDE: Visual Studio 2022

内存信息获取工具：Cheat Engine 7.5

目标程序：PlantsVsZombies.exe(95版)

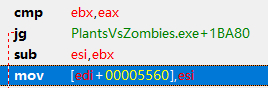
1. 实现原理
2. 进程内存读取的基础知识

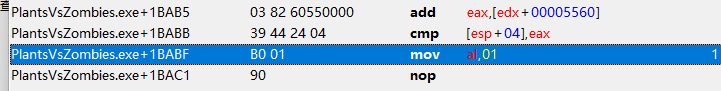
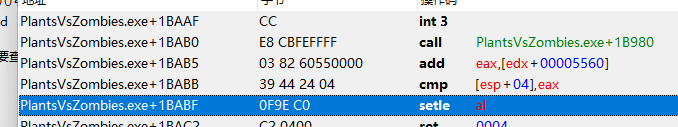
首先区分以下概念：PID·分配基址·句柄

* PID是进程标识符，在进程开启时被分配
* 分配基址是进程对应的汇编代码块在进程的内存空间中的起始地址，即代码模块（本项目中为PlantsVsZombies.exe）在操作系统为进程分配的虚拟内存中的偏移量。
* 句柄是操作系统提供给程序引用和操作进程的机制，可以获取进程数据、访问进程内存等等。

由此，要改写游戏代码，只要找到反汇编代码的分配基址+偏移量。

1. 其它
2. 实现的功能及难点
3. freeSun

首先找到阳光变量存储的地址，然后检查是什么改变了该变量，由此找到了使用阳光时的代码位置，根据原理将减法代码删掉，再将比较的对象变成0，就可以不消耗且无视当前阳光量。



1. stealMoney
2. stealSun
3. 创新点
4. 小组分工