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)

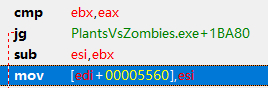
1. 实现原理
2. 进程内存读取的基础知识

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。

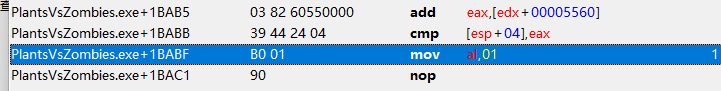
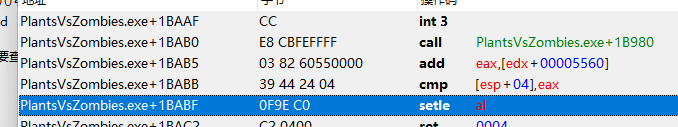
由此，要改写游戏代码，只要找到反汇编代码的分配基址+偏移量。

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，由此找到使用阳光时的代码位置，根据原理将减法代码删掉，就可以不消耗阳光种植。

**难点**：仅完成以上操作后如果当前阳光不足，植物处于灰色无法种植。为此先寻找访问阳光变量的地址，发现有两个一直在访问的指令，经检测发现，一个是显示阳光数量的指令，另一个是检测植物阳光是否够用的代码。在检测阳光是否够用处，把比较设定的setle改成直接赋值mov即可。同时要把消耗阳光处的二次确认删掉。

**最终效果：**使用指令后，冷却结束的植物全部亮起，终止时不消耗阳光。再次使用取消该效果。

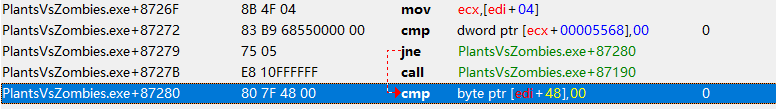


1. stealMoney
2. stealSun
3. alwaysOn

首先尝试找到一个植物冷却标志变量，参考阳光影响的亮起，认为应该有个bool值确定植物是否冷却中，尝试后发现，植物冷却结束后有一个值设为1，冷却时设为0。接下来寻找改变该值的地址。找到了放置时清空和冷却结束置1两处代码，把放置后清空改掉即可。

**难点**：以上操作出现问题，当游戏刚开始或刚放下某些植物后，处于冷却中的植物没有办法立刻停止冷却。为此研究置1部分代码，在这部分程序确认植物是否被选中，然后判断是否在冷却中，如果在冷却中就开始计数的更新。我们直接截断这一步骤。

**最终效果：**使用该指令后，所有植物立即取消冷却。



1. other
2. 创新点
3. 小组分工