题目：小心点

文件：



解压密码：123456

题目描述：请不要在个人电脑上运行，分析可执行文件行为，构造相应flag，flag为zsctf2020{相应工具全称惯用大写缩写\_IP\_port}

Flag:zsctf2020{CS\_114.67.98.102\_30900}

Writeup:

IP和端口直接上火绒剑，看程序行为就完事了，相应工具名称可以上wireshark抓包可以找到流量，看特征可以知道是cobaltstrike，实在看不出来就放到网上的病毒分析引擎分析，会有智能识别