

ASPack 2.x脱壳小记

作者：Delort

备注：此题脱壳简单，无需手工

1.x64dbg

x64dbg运行找到

004012A7	call <JMP.&RegisterClassA>	<user3
004012B8	call <JMP.&DialogBoxParamA>	<user3
004013AF	call <JMP.&GetDlgItemTextA>	<user3
00401495	call <JMP.&wsprintfA>	<user3
004014C6	call <JMP.&wsprintfA>	<user3
00401539	call <JMP.&GetDlgItemTextA>	<user3
0040163C	call <JMP.&MessageBoxA>	<user3
0040165E	call <JMP.&MessageBoxA>	<user3
0040166A	call <JMP.&EndDialog>	<user3
00401676	call <JMP.&EndDialog>	<user3
00401691	call <JMP.&GetCommandLineA>	<kerne
004016A3	call <JMP.&strchr>	<crtdl
004016DD	call <JMP.&GetModuleHandleA>	<kerne
10011C8A	call dword ptr ds:[<&GetModuleFileNameA>]	<kerne
10011CAA	call dword ptr ds:[<&LoadLibraryA>]	<kerne
10011D02	call dword ptr ds:[<&GetCommandLineA>]	<kerne
10011D0D	call dword ptr ds:[<&GetEnvironmentStrings>]	<kerne
10011D18	call dword ptr ds:[<&GetVersion>]	<kerne
10011EFA	call dword ptr ds:[<&UnhandledExceptionFilter>]	<kerne
10012022	call dword ptr ds:[<&ExitProcess>]	<kerne

2.纠正指令

纠正前：

0401683	. 5E	pop esi	
0401684	. 5B	pop ebx	
0401685	. C9	leave	
0401686	. C2 10 00	ret 10	
0401689	<. 00 00	add byte ptr ds:[eax],al	sub_401689
040168B	. 00 55 89	add byte ptr ss:[ebp-77],dl	
040168E	. E5 51	in eax,51	
0401690	. 57	push edi	
0401691	. E8 5A 00 00 00	call <JMP.&GetCommandLineA>	
0401696	. 89 C7	mov edi,eax	
0401698	. 80 3F 22	cmp byte ptr ds:[edi],22	22:'\"'
040169B	. 75 23	jne crackme6.4016C0	
040169D	. 6A 22	push 22	
040169F	. 89 F8	mov eax,edi	
04016A1	. 40	inc eax	
04016A2	. 50	push eax	
04016A3	. E8 08 01 00 00	call <JMP.&strchr>	
04016A8	. 83 C4 08	add esp,8	
04016AB	. 89 45 FC	mov dword ptr ss:[ebp-4],eax	
04016AE	. 09 C0	or eax,eax	
04016B0	. 74 29	je crackme6.4016DB	

纠正后：

00401689	<	. 00 00	add byte ptr ds:[eax],al
0040168B	.	. 90	nop
0040168C	\$. 55	push ebp
0040168D	.	. 89 E5	mov ebp,esp
0040168F	.	. 51	push ecx
00401690	.	. 57	push edi
00401691	.	. E8 5A 00 00 00	call <JMP.&GetCommandLineA>
00401696	.	. 89 C7	mov edi,eax
00401698	.	. 80 3F 22	cmp byte ptr ds:[edi],22
0040169B	..	. 75 23	jne crackme6.4016C0
0040169D	.	. 6A 22	push 22
0040169F	.	. 89 F8	mov eax,edi
004016A1	.	. 40	inc eax
004016A2	.	. 50	push eax
004016A3	.	. E8 08 01 00 00	call <JMP.&strchr>
004016A8	.	. 83 C4 08	add esp,8

此处即为OEP。

3.使用Scylla

dump:

新开一个CrackMe进程。

然后使用独立版进行dump:

01676 . E8 A5 00 00 00 call <JMP.&EndDialog>
0167B . 31 C0 xor eax ,eax
0167D . 40 inc eax
0167E . EB 02 jmp crackme6.401682
01680 > 31 C0 xor eax ,eax
01682 > 5F pop edi
01683 . 5E pop esi
01684 . 5B pop ebx
01685 . C9 leave
01686 . C2 10 00 ret 10
01689 < 00 00 add byte ptr ds:[eax],al sub_401689
0168B . 90 nop
0168C \$ 55 push ebp
0168D . 89 E5 mov ebp ,esp
0168F . 51 push ecx
01690 . 57 push edi
01691 . E8 5A 00 00 00 call <JMP.&GetCommandLineA>
01696 . 89 C7 mov edi ,eax
01698 . 80 3F 22 cmp byte ptr ds:[edi],22 22:'\"'
0169B < 75 23 jne crackme6.4016C0
0169D . 6A 22 push 22
0169F . 89 F8 mov edi ,eax
016A1 . 40 inc eax
016A2 . 50 pop esi
016A3 . E8 08 01 00 00 call <JMP.&GetCommandLineA>
016A8 . 83 C4 08 mov ecx ,ecx
016AB . 89 45 FC mov edi ,edi
016AE . 09 C0 cmp byte ptr [edi],0
016B0 . 74 29 jz crackme6.4016C0
016B2 . 89 C7 mov ecx ,ecx

0040168C crackme6.exe:\$168C
内存 1 内存 2
十六进制
61000 36 00 38 00
61010 28 00 2A 00
61020 1E 00 20 00
61030 18 00 1A 00
61040 30 00 32 00
61050 20 00 22 00
61060 10 00 12 00
61070 18 00 00 00
61080 00 00 00 00
61090 7C 17 E6 76
610A0 18 00 00 00
610B0 00 00 00 00
610C0 14 00 16 00

Commands are comma sep

Scylla x86 v0.9.8
File Imports Trace Misc Help
Attach to an active process
16188 - crackme6.exe - C:\Users\delor\Documents\MyReverse\看雪刷题\1\crackme6.exe Pick DLL
Imports
kernel32.dll (3) FThunk: 00003100
user32.dll (8) FThunk: 00003114
crt.dll (6) FThunk: 0000313C
Show Invalid Show Suspect Clear
IAT Info
OEP 0040168C IAT Autosearch
VA 00403100 Get Imports
Size 00000054
Actions
Autotrace
Dump
Dump PE Rebuild
Fix Dump
Log
IAT Search Adv: Found 17 (0x11) possible IAT entries.
IAT Search Adv: Possible IAT first 00403100 last 00403150 entry.
IAT Search Adv: IAT VA 00403100 RVA 00003100 Size 0x0054 (84)
IAT Search Adv: IAT VA 00403150 RVA 00003150 Size 0x0054 (84)

然后fix dump.