

REPORT:

코드엔진 Basic

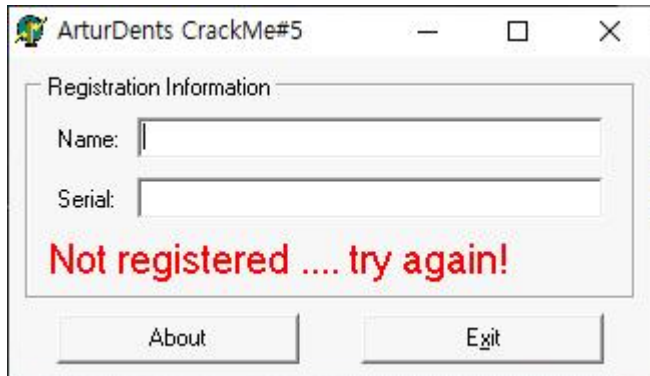
RCE 10 Writeup

COLONY
1824275 정상지

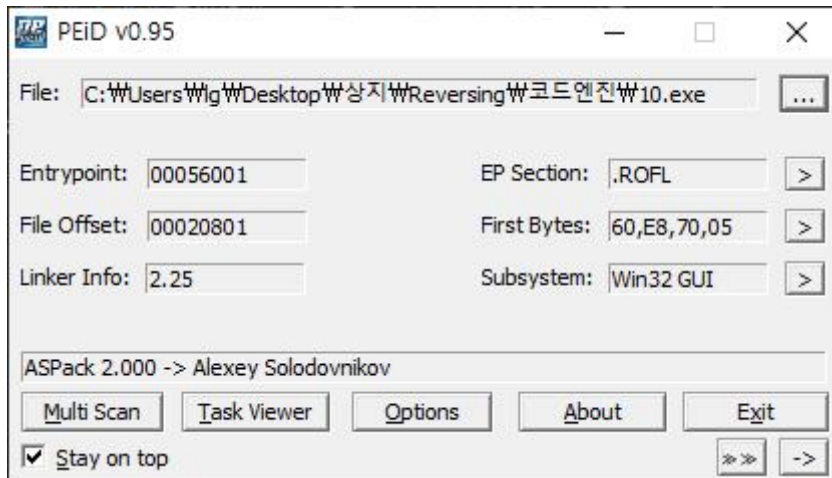
2021.05.30

OEP를 구한 후 '등록성공' 으로 가는 분기점의 OPCODE를 구하시오.

프로그램 실행



해당 프로그램은 ASpack으로 패킹되어있는 것을 확인할 수 있다



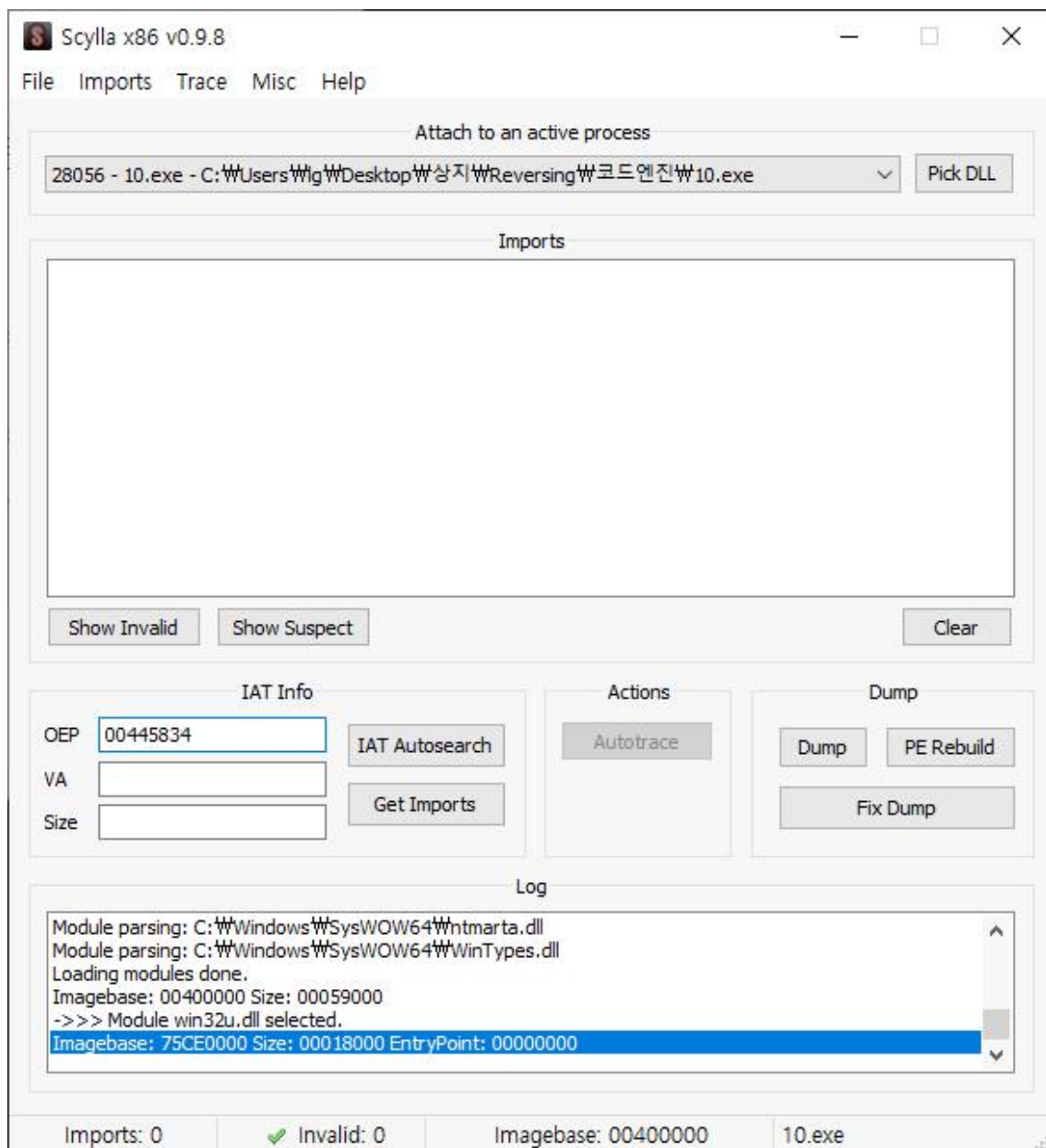
pushad에서부터 popad까지 패킹과정이므로



popad에서 breakpoint를 걸고 디버깅

ret 호출 불러진 곳이 oep ->00445834

CPU	로그	메모	중단점	메모리 맵	호출 스택	SEH	스크립트	기호	소스	참조	스레드	행들
EIP			00445834	55	push ebp							
			00445835	8BEC	mov ebp,esp							
			00445837	83C4 F4	add esp,FFFFFFF4							
			0044583A	B8 F4564400	mov eax,10.4456F4							
			0044583F	E8 0408FCFF	call 10.406048							
			00445844	A1 6C6C4400	mov eax,dword ptr ds:[446C6C]							
			00445849	8B00	mov eax,dword ptr ds:[eax]							
			0044584B	E8 F0C0FFFF	call 10.442540							
			00445850	8B00 386D4400	mov ecx,dword ptr ds:[446D38]							
			00445856	A1 6C6C4400	mov eax,dword ptr ds:[446C6C]							
			0044585B	8B00	mov eax,dword ptr ds:[eax]							
			0044585D	8B15 88514400	mov edx,dword ptr ds:[445188]							
			00445863	E8 F0C0FFFF	call 10.442558							
			00445868	8B00 586D4400	mov ecx,dword ptr ds:[446D58]							
			0044586E	A1 6C6C4400	mov eax,dword ptr ds:[446C6C]							
			00445873	8B00	mov eax,dword ptr ds:[eax]							
			00445875	8B15 104F4400	mov edx,dword ptr ds:[444F10]							
			0044587B	E8 D8C0FFFF	call 10.442558							
			00445880	A1 6C6C4400	mov eax,dword ptr ds:[446C6C]							
			00445885	8B00	mov eax,dword ptr ds:[eax]							
			00445887	E8 4CC0FFFF	call 10.442508							
			0044588C	E8 17DFFBFF	call 10.4037A8							



해당 파일을 Scylla 플러그인을 통해 IAT autosearch 및 get imports를 시키고 Dump를 만든 후에 fix dump로 저장한다

아래와 같이 10_dump_SCY라는 exe파일이 생성되었으며 해당 프로그램을 디버깅한다

08_unp	2018-12-17 오전 2:27	응용 프로그램	112KB
10	2018-12-17 오전 2:27	응용 프로그램	136KB
10_dump	2021-05-30 오후 7:38	응용 프로그램	310KB
10_dump_SCY	2021-05-30 오후 7:38	응용 프로그램	318KB

성공했을 때의 메시지 주소가 0044550C이므로

주소	디스어셈블리	문지열
00441CEA	push 10_dump_scy.441FA0	"RegisterAutomation"
0044550C	mov edx,10_dump_scy.445660	"Registered ... well done!"
73E125AF	push comctl32.73DB327C	"RegisterDragDrop"
7536260D	push apphelp.75343028	"L\\Registry\\Machine\\Software\\\\
753624C0	push apphelp.75343028	"L\\Registry\\Machine\\Software\\\\

해당 주소를 cpu에서 찾아간다

004454F3	E8 B4F5FDFF	call 10_dump_scy.424AAC	
004454F8	8B87 D8020000	mov eax,dword ptr ds:[edi+2D6]	
004454FE	8B55 FC	mov edx,dword ptr ss:[ebp-4]	edx:EntryPoint
00445501	E8 A6F5FDFF	call 10_dump_scy.424AAC	
00445506	8B87 E8020000	mov eax,dword ptr ds:[edi+2E8]	
0044550C	BA 60564400	mov edx,10_dump_scy.445660	edx:EntryPoint, 445660: "Registered ... well done!"
00445511	E8 96F5FDFF	call 10_dump_scy.424AAC	
00445516	8B87 E8020000	mov edx,dword ptr ds:[edi+2E8]	
0044551C	8B40 58	mov eax,dword ptr ds:[eax+58]	

해당 break point 위에 분기문이 있는 것이므로 확인해본다

004454C0	8B55 FC	mov edx,dword ptr ss:[ebp-4]	edx:EntryPoint
004454C7	E8 9CE7FBFF	call 10_dump_scy.403C70	
004454D1	75 55	jne 10_dump_scy.445528	
004454D6	8D85 F4FDFFFF	lea eax,dword ptr ss:[ebp-20C]	
004454DC	8D95 17FEFFFF	lea edx,dword ptr ss:[ebp-1E9]	edx:EntryPoint
004454E2	E8 1DE6FBFF	call 10_dump_scy.403804	
004454E7	8B95 F4FDFFFF	mov edx,dword ptr ss:[ebp-20C]	
004454ED	8B87 D4020000	mov eax,dword ptr ds:[edi+2D4]	edx:EntryPoint
004454F3	E8 B4F5FDFF	call 10_dump_scy.424AAC	
004454F8	8B87 D8020000	mov eax,dword ptr ds:[edi+2D8]	
004454FE	8B55 FC	mov edx,dword ptr ss:[ebp-4]	edx:EntryPoint
00445501	E8 A6F5FDFF	call 10_dump_scy.424AAC	
00445506	8B87 E8020000	mov edx,dword ptr ds:[edi+2E8]	
0044550C	BA 60564400	mov edx,10_dump_scy.445660	edx:EntryPoint, 445660: "Registered ... well done!"
00445511	E8 96F5FDFF	call 10_dump_scy.424AAC	
00445516	8B87 E8020000	mov eax,dword ptr ds:[edi+2E8]	
0044551C	8B40 58	mov eax,dword ptr ds:[eax+58]	
0044551F	BA 00800000	mov edx,8000	
00445524	E8 8FF2CFFF	call 10_dump_scy.4147E8	edx:EntryPoint
00445529	EB 0A	jmp 10_dump_scy.445535	
0044552B	33C0	xor eax,eax	
0044552D	5A	pop edx	edx:EntryPoint
0044552E	59	pop ecx	ecx:EntryPoint
0044552F	5A	pop ecx	ecx:EntryPoint
00445530	64:8910	mov dword ptr [eax],edx	edx:EntryPoint
00445533	EB 27	jmp 10_dump_scy.44555C	
00445535	33C0	xor eax,eax	
00445537	5A	pop edx	edx:EntryPoint
00445538	59	pop ecx	ecx:EntryPoint
00445539	5A	pop ecx	ecx:EntryPoint
0044553A	64:8910	mov dword ptr [eax],edx	edx:EntryPoint
0044553D	EB 1D	jmp 10_dump_scy.44555C	

jne분기문을 통해서 확인할 수 있다

정답은 004458347755