

# REPORT:

## 코드엔진 Basic

### RCE 19 Writeup

COLONY  
1824275 정상지

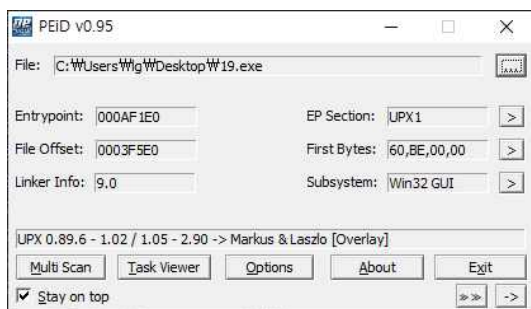
2021.07.24

이 프로그램은 몇 밀리세컨드 후에 종료되는가



프로그램 실행 시 위와 같이 메시지 박스를 띄워준다

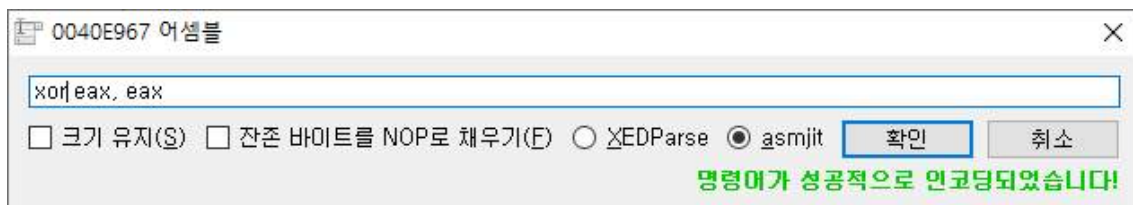
해당 프로그램을 PEid로 확인 결과 upx로 패킹되어있는 것을 볼 수 있다



언패킹 후 프로그램 디버깅 시 정상실행이 되지 않는 것으로 보아 안티디버깅이 있는 것으로 유추할 수 있다



따라서 모듈 간 호출에서 IsDebuggerPresent함수를 발견한다



test를 xor로 변경하여 안티디버깅을 회피한다

004338D9	E9 5D9FCFF	jmp 19_ump_4012B3	
004338DE	6A 10	push 10	
004338E0	68 3EF64700	push 19_ump_47F69E	
004338E5	68 A0F64700	push 19_ump_47F6A0	47F6A0: This is a compiled AutoIt script. Av researchers please email avsupport
004338EA	6A 00	push 0	
004338EC	F3D DCD64700	CALL dword ptr ds:[cMessageBoxA]	
004338F2	E9 49B1DFFF	jmp 19_ump_40EA40	
004338F7	8B0D 44F44900	mov ecx, dword ptr ds:[49F444]	ecx:EntryPoint
004338FD	6A FF	push 0xFFFFFFFF	
004338FF	51	push ecx	ecx:EntryPoint
00433900	6A 01	push 1	
00433902	320B	xor b1, b1	
00433904	E8 47CFFDFF	CALL 19_ump_401050	
00433909	8A15 CCE48A00	mov dl, byte ptr ds:[48E8C0]	
0043390F	8B15 32044A00	mov byte ptr ds:[4A0432], dl	

주소	디스어셈블리	대상
00410834	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00412571	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0041ADDE	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0041AE3A	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0041AE8B	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0041AED4	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
004298FE	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0042E404	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00430D8D	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00430E46	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00430EC2	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
004330AC	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433197	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433D5C	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433E72	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433ED4	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433F33	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433F64	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433CCE	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
004332FE	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433333	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00433337	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00434D4A	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00434D63	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
004446C9	mov ebp,dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00444D44	mov edi,dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00444E15	mov edi,dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0044D106	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0044D114	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0044D1FA	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00453335	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
004568F0	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
004568F6	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00461E31	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0046F47C	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
0046FC63	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>
00472F94	call dword ptr ds:[<Sleep>]	<kernel32.Sleep>

esi에 들어온 값과 eax의 값을 비교하여 eax가 esi보다 크거나 같을 경우 jmp를 실행

Address	Disassembly	Comment
00444C3D	57	push edi
00444C3E	8B3D 58D74700	mov edi,dword ptr ds:[<timeGetTime>]
00444C44	FFD7	call edi
00444C46	803D D3E48000 00	cmp byte ptr ds:[48E8D3],0
00444C4D	8BF0	mov esi,eax
00444C4F	0F84 FF000000	je 19_unp.444D54
00444C55	8B5C24 14	mov ebx,dword ptr ss:[esp+14]
00444C59	8B2D 58D14700	mov ebp,dword ptr ds:[<Sleep>]
00444C5F	FFD7	call edi
00444C61	3BC6	cmp eax,esi
00444C63	0F83 CF000000	jae 19_unp.444D38
00444C69	2BC6	sub eax,esi
00444C6B	48	dec eax

EIP	00444D34	5B	pop ebx
	00444D35	C2 0400	ret 4
	00444D38	2BC6	sub eax,esi
	00444D3A	3B43 04	cmp eax,dword ptr ds:[ebx+4]
	00444D3D	0F83 2EFFFFFF	jae 19_unp.444C71
	00444D43	6A 0A	push A
	00444D45	FFD5	call ebp
	00444D47	803D D3E84800 00	cmp byte ptr ds:[48E8D3],0
	00444D4E	0F85 0BFFFFFF	jne 19_unp.444C5F
	00444D54	5F	pop edi

eax는 시스템에서 시간을 받아온 후부터 지금까지의 시간

정답 : 11120밀리세컨드