

REPORT:

코드엔진 Basic

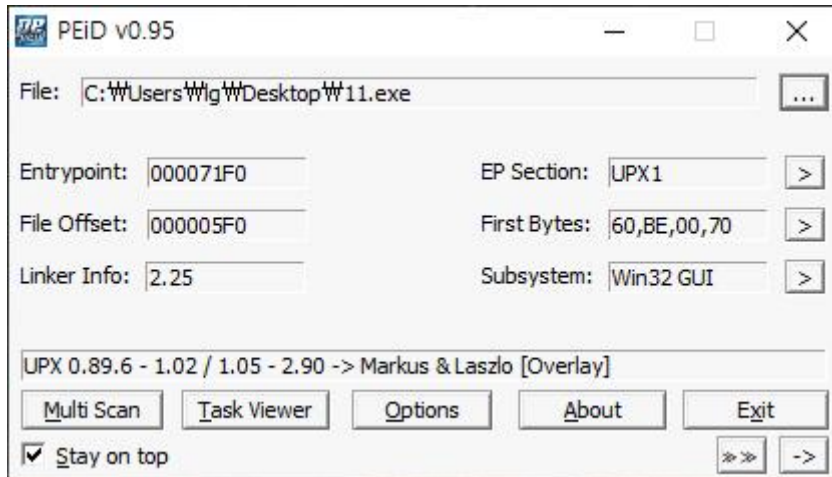
RCE 11 Writeup

COLONY
1824275 정상지

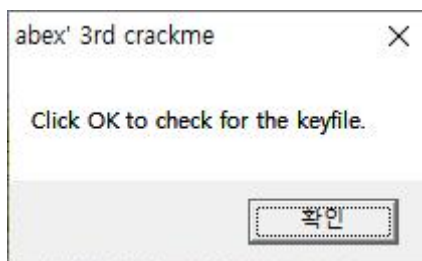
2021.05.30

OEP를 찾으시오. Ex) 00401000 / Stolenbyte 를 찾으시오.

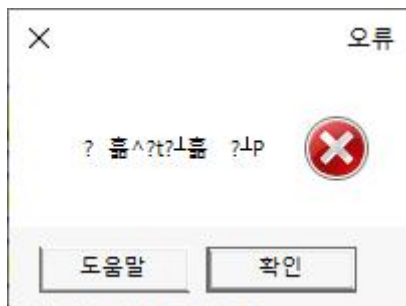
해당 프로그램을 PEiD로 분석 시 UPX로 패킹되어있다



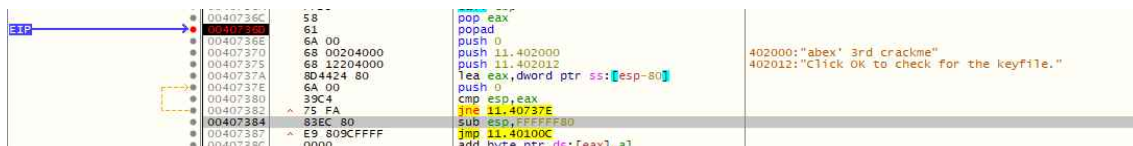
프로그램 실행시



언패킹후 프로그램 실행시



위와 같은 오류가 발생하며 codeengn basic 09번에서 StolenByte를 확인한 것처럼



popad 이후에 있는 push를 통해 값이 입력되는 것을 알 수 있다

StolenByte는 6A0068002040006812204000

이후 OEP 값을 확인해보면 0040100C로 나온다

CPU	로그	메모	중단점	메모리 맵	호출 스택	SEH	스크립트	가호	소스	참조	스레드	행들	Trace
00401002	6A 00								push 0				
00401003	E8 8C000000								call <JMP.&MessageBoxA>				
00401004	6A 00								push 0				
00401005	68 80000000								push 80				
00401006	6A 03								push 3				
00401007	6A 00								push 0				
00401008	6A 00								push 0				
00401009	68 00000080								push 80000000				
0040100A	68 89204000								push 11.402089				
0040100B	E8 5E000000								call <JMP.&CreateFileA>				402089:"abex.12c"
0040100C	A3 CA204000								mov dword ptr ds:[4020CA],eax				
0040100D	83F8 FF								cmp eax,FFFFFFF				
0040100E	74 3C								jle 11.401075				
0040100F	6A 00								push 0				
00401010	FF35 CA204000								push dword ptr ds:[4020CA]				
00401011	E8 40000000								call <JMP.&GetFileSize>				
00401012	83F8 12								cmp eax,12				
00401013	75 15								jne 11.401060				
00401014	6A 00								push 0				
00401015	68 35204000								push 11.402035				402035:"Well done!"
00401016	68 40204000								push 11.402040				402040:"Yep, keyfile found!"
00401017	6A 00								push 0				
00401018	E8 41000000								call <JMP.&MessageBoxA>				
00401019	EB 28								jmp 11.401088				
0040101A	6A 00								push 0				
0040101B	68 79204000								push 11.402079				402079:"Error"
0040101C	68 7F204000								push 11.40207F				40207F:"The found file is not a valid keyfile!"
0040101D	6A 00								push 0				
0040101E	E8 2C000000								call <JMP.&MessageBoxA>				
0040101F	EB 13								jmp 11.401088				
00401020	6A 00								push 0				
00401021	68 54204000								push 11.402054				402054:"Error"
00401022	68 5A204000								push 11.40205A				40205A:"Hmmm, I can't find the file!"
00401023	6A 00								push 0				
00401024	E8 17000000								call <JMP.&MessageBoxA>				
00401025	E8 0C000000								call <JMP.&ExitProcess>				
00401026	FF25 54304000								jmp dword ptr ds:[<CreateFileA>]				JMP.&CreateFileA
00401027	FF25 58304000								jmp dword ptr ds:[<GetFileSize>]				JMP.&GetFileSize
00401028	FF25 5C304000								jmp dword ptr ds:[<ExitProcess>]				JMP.&ExitProcess
00401029	FF25 64304000								jmp dword ptr ds:[<MessageBoxA>]				JMP.&MessageBoxA
0040102A	0000								add byte ptr ds:[eax],al				
0040102B	0000								add byte ptr ds:[eax],al				
0040102C	0000								add byte ptr ds:[eax],al				

정답은 0040100C6A0068002040006812204000