

악성코드 분석 보고서

(sand-reversingwithlana-tutorials)

2025.07.01

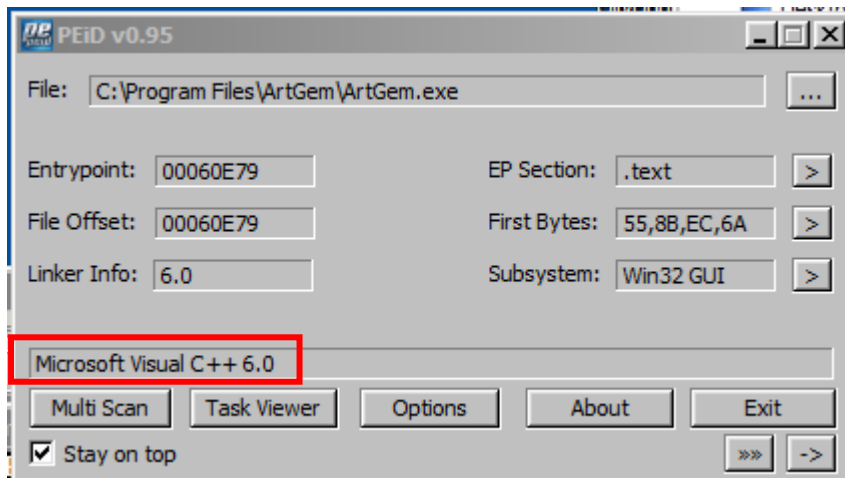
1. 문제



Info > register 들어가면 키 입력하라고 나온다. 키가 다르면 Invalid Key! 발생

위에 'UNREGISTERED! REGISTER NOW!'는 키 문제가 해결되면 없어질 가능성이 있어서 이것부터 해결해본다.

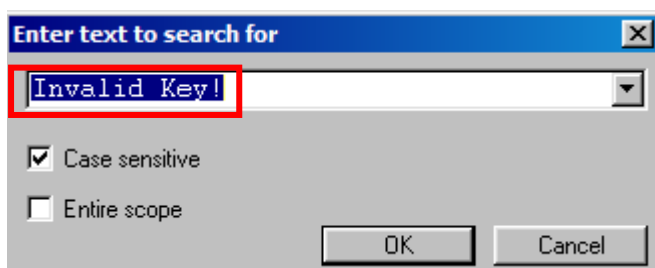
2. 해결 방법



PEID로 먼저 분석 시 압축되어 있지 않은 걸 확인할 수 있다.

00000110	00060E79	Address of Entry Point
00000114	00001000	Base of Code
00000118	0006A000	Base of Data
0000011C	00400000	Image Base

PEview로 확인 시 00460E79에서 시작하는 걸 확인할 수 있다. 코드 주소 확인 시 같은 주소에서 시작하는 것을 확인



Search for > All referenced text strings 눌러서 Invalid Key! 해당 구문을 찾아준다.

R Text strings referenced in ArtGem.text		
Address	Disassembly	Text string
004385D4	PUSH ArtGem.0046F9DC	ASCII "Thank You for Registering! Enjoy ArtGem!"
00438609	PUSH ArtGem.0046F90C	ASCII "ArtGem"
0043860E	PUSH ArtGem.0046F9CC	ASCII "Invalid Key!"

나오는 걸 볼 수 있고 클릭해서 들어가서 그 조건에 해당하는 분기문을 찾아준다.

004385C8	. A1 A8494900	MOV EAX,DWORD PTR DS:[4949A8]	Style = MB_OK MB_ICONASTERISK MB_APPLMODAL
004385CD	. 6A 40	PUSH 40	Title = "ArtGem"
004385CF	. 68 0CF94600	PUSH ArtGem.0046F90C	Text = "Thank You for Registering!Enjoy ArtGem!"
004385D4	. 68 DCF94600	PUSH ArtGem.0046F9DC	hOwner => NULL
004385D9	. 50	PUSH EAX	MessageBoxA
004385DA	. FF15 ACA14600	CALL DWORD PTR DS:[<&USER32.Messa	Result = 1
004385E0	> 6A 01	PUSH 1	hWnd
004385E2	. 53	PUSH EBX	EndDialog
004385E3	. C705 7CF84600	MOV DWORD PTR DS:[46F87C],0	
004385E5	. FF15 44A24600	CALL DWORD PTR DS:[<&USER32.EndD	
004385F3	. 5F	POP EDI	
004385F4	. 5E	POP ESI	
004385F5	. 33C0	XOR EAX,EAX	
004385F7	. 5B	POP EBX	
004385F8	. 81C4 38040000	ADD ESP,438	
004385FE	. C2 1000	RETN 10	
00438601	> 8B0D A8494900	MOV ECX,DWORD PTR DS:[4949A8]	Style = MB_OK MB_ICONHAND MB_APPLMODAL
00438607	. 6A 10	PUSH 10	Title = "ArtGem"
00438609	. 68 0CF94600	PUSH ArtGem.0046F90C	Text = "Invalid Key!"
0043860E	. 68 CCF94600	PUSH ArtGem.0046F9CC	hOwner => NULL
00438613	. 51	PUSH ECX	MessageBoxA
00438614	. FF15 ACA14600	CALL DWORD PTR DS:[<&USER32.Messa	

근데 위어를 보면 레지스터 키를 등록되었다는 구문이 보인다. 그럼 등록되었다는 구문은 지나고 'Invalid Key!'는 지나지 않는 분기문을 찾아준다.

0043855D	. 51	PUSH ECX	
0043856E	. E8 8DC6FFFF	CALL ArtGem.00434C00	
00438573	. 83C4 10	ADD ESP,10	
00438576	. 85C0	TEST EAX,EAX	
00438578	. 0F84 83000000	JE ArtGem.00438601	
0043857E	. 8D7C24 44	LEA EDI,DWORD PTR SS:[ESP+44]	

많은 분기문이 있는데 그 중 0x00438578이 어떤 메시지 박스를 보낼지 정하는 분기문이다. 그래서 위에 TEST 함수를 보면 EAX를 비교하는 함수가 있고 EAX는 위에 CALL 함수에서 나오는 걸 볼 수 있다. 이 함수로 들어가본다.

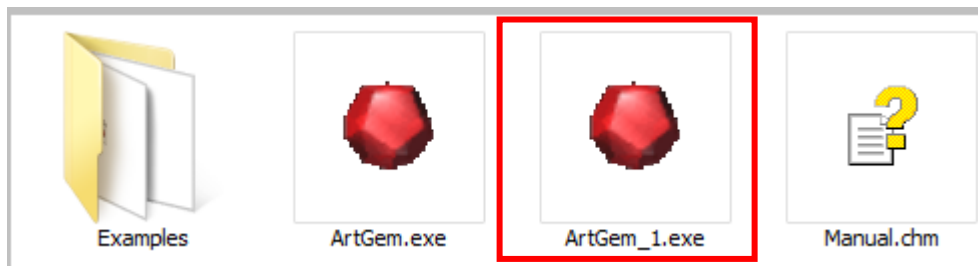
00434D8F	> 5F	POP EDI	
00434D90	. 5E	POP ESI	
00434D91	. 5D	POP EBP	
00434D92	. 33C0	XOR EAX,EAX	
00434D94	. 5B	POP EBX	
00434D95	. 83C4 24	ADD ESP,24	
00434D98	. C3	RETN	

함수에 들어가서 실행하다보면 'XOR EAX EAX' EAX를 초기화하는 것을 볼 수 있다.

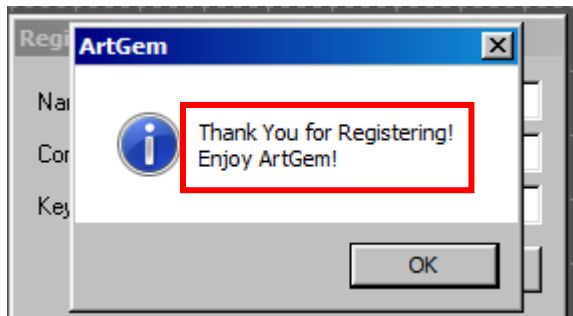
초기화를 하면 당연히 EAX=0, ZF=1 0x00438578이 JE이니까 점프를 하게되고 그럼 'Invalid Key!' 구문 쪽으로 이동하는 것을 볼 수 있다.

00434D8F	> 5F	POP EDI	
00434D90	. 5E	POP ESI	
00434D91	. 5D	POP EBP	
00434D92	. 90	NOP	
00434D93	. 90	NOP	
00434D94	. 5B	POP EBX	
00434D95	. 83C4 24	ADD ESP,24	
00434D98	. C3	RETN	

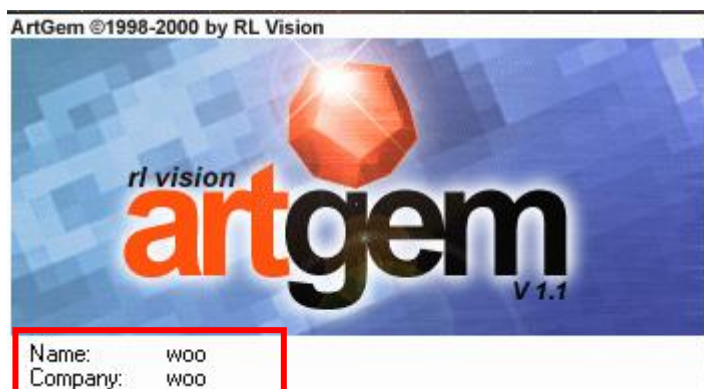
그렇게 안되긴 위해서 'XOR EAX EAX' 를 NOP으로 바꿔주워서 초기화를 안시켜줘야한다. Binary > Fill with NOPs로 해주고 저장해준다.



ArtGem_1.exe로 저장한다.



실행 후 레지스터 키 등록하면 키 등록이 완료되었다는 창이 발생한다.



다시 실행하면 처음에 뒀던 'UNREGISTERED! REGISTER NOW!'가 변경된 것을 볼 수 있다.

문제 해결!