

REPORT:

코드엔진 Basic

RCE 08 Writeup

COLONY
1824275 정상지

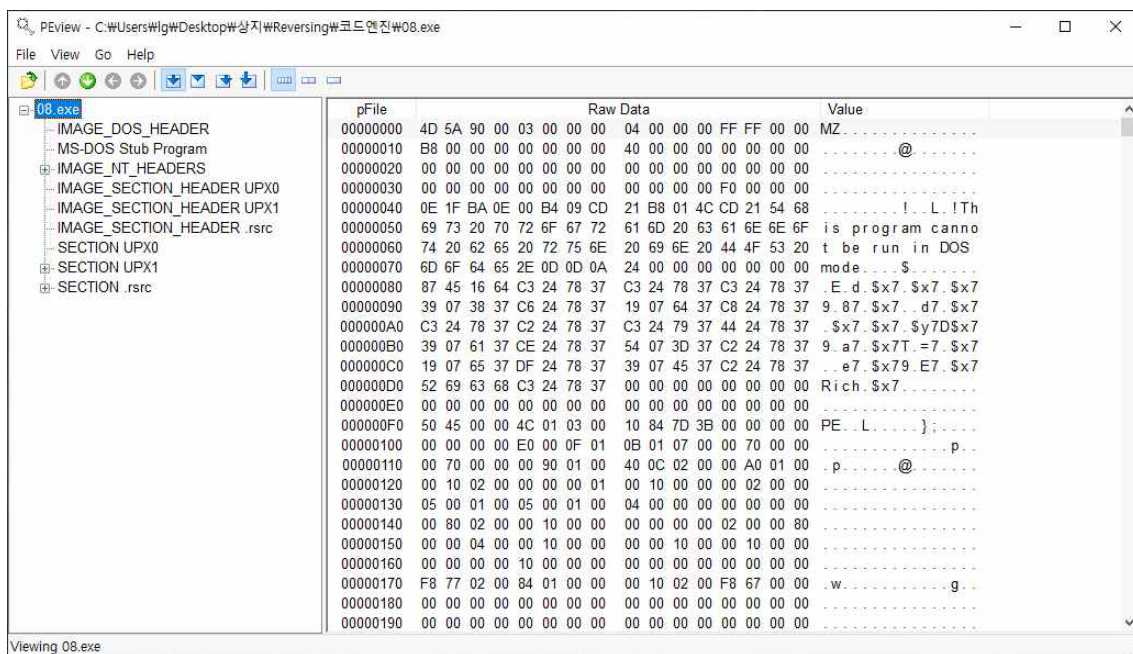
2021.05.30

OEP를 구하시오

프로그램 실행



PE 구조 확인 시 UPX 패키징이 되어있는 것을 확인할 수 있다



해당 프로그램을 UPX로 언패킹한 후 디버깅을 진행한다

디버깅시 x32dbg가 진입하는 진입점이 OEP이다 --> 언패킹을 진행하였기 때문

The screenshot shows the x32dbg interface with the CPU window active. The instruction list on the right shows the entry point at address 01012475, which is highlighted in blue. The instruction at this address is 'push 70'. The comment on the right indicates 'EntryPoint'. The instruction pointer (EIP) is shown as 01012475. The register window on the left shows the values of EIP, ECX, EDX, ESI, and EDI. The instruction list on the right shows the following instructions: 'pop esi', 'pop ebp', 'ret 8', 'push 70', 'push 08_unp.10015E0', 'call 08_unp.10127C8', 'xor ebx,ebx', 'push ebx', 'mov edi,dword ptr ds:[&GetModuleHandle', 'call edi', 'cmp word ptr ds:[eax],5A4D', 'jne 08_unp.1012482', 'mov ecx,dword ptr ds:[eax+3C]', 'add ecx,eax', 'cmp dword ptr ds:[ecx],4550', 'jne 08_unp.1012482', 'movzx eax,word ptr ds:[ecx+18]', 'cmp eax,10B', 'je 08_unp.10124CA', 'cmp eax,20B', 'je 08_unp.10124B7', 'mov dword ptr ss:[ebp-1C],ebx'.

Address	Disassembly	Comment
01012470	pop esi	
01012471	pop ebp	
01012472	ret 8	
01012475	push 70	EntryPoint
01012477	push 08_unp.10015E0	
0101247C	call 08_unp.10127C8	
01012481	xor ebx,ebx	
01012483	push ebx	
01012484	mov edi,dword ptr ds:[&GetModuleHandle	edi:EntryPoint
0101248A	call edi	edi:EntryPoint
0101248C	cmp word ptr ds:[eax],5A4D	
01012491	jne 08_unp.1012482	
01012493	mov ecx,dword ptr ds:[eax+3C]	ecx:EntryPoint
01012496	add ecx,eax	ecx:EntryPoint
01012498	cmp dword ptr ds:[ecx],4550	ecx:EntryPoint
0101249E	jne 08_unp.1012482	
010124A0	movzx eax,word ptr ds:[ecx+18]	
010124A4	cmp eax,10B	
010124A9	je 08_unp.10124CA	
010124AB	cmp eax,20B	
010124B0	je 08_unp.10124B7	
010124B2	mov dword ptr ss:[ebp-1C],ebx	

해당 프로그램의 OEP는 01012475이다