Codeengn Challenges Advance RCE LEVEL1 풀이

Reverse2 L01 Start

Author : CodeEngn / Lee Kang-Seok

Korea :

이 프로그램은 몇 밀리세컨드 후에 종료 되는가

정답인증은 MD5 해쉬값(대문자) 변환 후 인증하시오

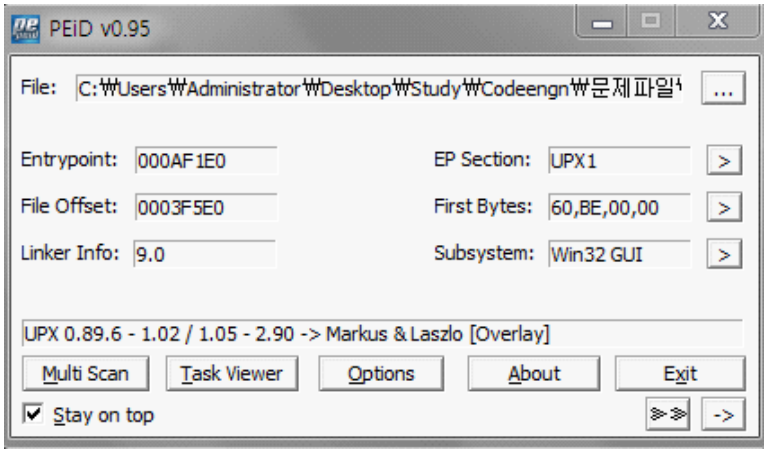
English :

How many milliseconds does it take for this program to terminate

The solution is the MD5 hash of the answer(in CAPITALS).

Down

먼저 PEID로 프로그램에 대한 정보를 알아보았다.



UPX 패킹이 되어있었다.

언패킹을 하고 올리로 열어서 분석을 진행해 보니 isDebuggerPresent로 안티 디버깅이 되어있었다.

```
0040E961   .  FF15 20D34700  CALL DWORD PTR DS:[<&KERNEL32.IsDebugge  IsDebuggerPresent
0040E967   .  85C0           TEST EAX,EAX
0040E969   .v 0F85 6F4F0200  JNZ _Reverse.004338DE
```

그 후 TEST를 이용해 비교 후 분기를 해주고있다.

여기서, TEST와 CMP의 차이점을 모르는 사람들이 많은 것 같다.

두 명령어 모두 값을 비교한다는 데에서의 기능은 같다 그리고, 둘다 연산 결과를 저장하지 않고 Flag에만 영향을 준다.

그런데 비교하는 방법이 다르다는 점에 주목해야 할 필요가 있는 것 같다.

TEST는 논리적 AND 연산을 통해 같고 다름을 비교한다.

CMP는 Destination 피연산자에서 Source 피연산자를 뺀 결과로 비교한다.

그렇다면 TEST와 CMP는 어느때 구분되어 사용할까 ?

TEST는 리턴값이 0(NULL)인지 아닌지를 비교할때 자주 쓰인다.

왜냐면 0 AND 0 을 하면 결과값이 0이 되기 때문이다. 하지만, 1 AND 1 을 하면 결과값은 1이다.

즉 ZF는 0 과 0 을 비교할때만 1이 된다.

그런데 CMP는 리턴값이 0이던 아니던 비교하는 값이 서로 같기만 하면 결과값은 0이 된다. 즉 같기만 하면 ZF가 1이 되는 것이다.

이런점이 TEST와 CMP의 차이점이라고 볼 수 있다.

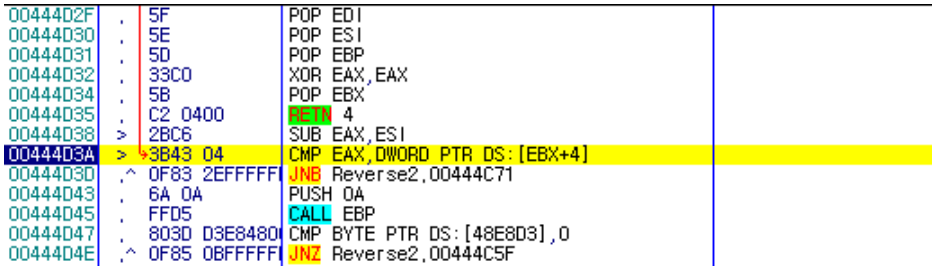
설명은 여기까지 하고 , 다시 분석으로 넘어가서

TEST후 JNZ 즉 ZF가 1이 아니면 4338DE지점으로 JUMP해주고 있다. 분석해보니 저곳으로 가면 이상한 에러창 하나가 뜬다.

isDebuggerPresent를 우회하는 방법은 여러가지가 있는데, 일단 나는 저기서JNZ를 JZ로 바꾸어 디버깅을 당하고 있을때 점프를 안하게 했다. (isDebuggerPresent의 리턴값이 0이면 디버깅상태가 아니고, 0이 아니면 디버깅 당하고 있음을 의미한다.)

그 후 계속 분석을 해보면 , timeGettime이라는 함수 근처 루틴을 주목해볼 필요가 있다.

이 함수는 시스템 시간을 밀리세컨드 단위로 반환하는 함수이다.



timeGettime 함수를 반복적으로 CALL 하고,

리턴값과 이미 있는 값을 뺀 다음 다른 무엇과 비교하는 루틴이 있는데

이 루틴을 잘 보면 답을 찾을 수 있다 ! :D