Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Duelist’s Crack me 2 |
| 파일명 | due-cm2.exe / due-cm2.dat |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/12/26 ~ 2017/01/01 |
| 문제 내용 | 알맞은 unlock code(문자열)을 가지는 dat 파일을 생성하라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



내용은 제한 시간이 끝났다는 것과 keyfile을 등록 후 같은 경로에 복사하라는 내용입니다. 즉, 정상적인 실행에는 keyfile이 필요함을 확인할 수 있습니다.



실행 첫 루틴 지점입니다. createFileA 메소드를 호출하는데 파일명이 due-cm2.dat임을 확인할 수 있습니다. 즉, keyfile의 이름은 due-cm2.dat입니다.

우선 임시로 내용이 "test"인 동명의 파일을 생성 후 진행합니다.



파일이 존재할 경우 진행된 루틴입니다. 파일을 읽고 값을 0040211A에 저장하고 byte 길이를 00402173 주소에 저장합니다.



실제로 주소에 파일의 내용이 저장되었음을 확인할 수 있습니다.



파일을 읽은 후의 루틴입니다. loop가 2개 보이고 아래에 invalid 결과창이 보입니다.

먼저 루프전 4010F7의 값과 0x12(=18)을 비교해 작으면 invalid 창으로 점프합니다. 4010F7의 값은 읽은 code 길이였으므로 code의 길이는 적어도 18 이상이어야 합니다.

그 후, 첫번째 루프에 진입하는데 code의 처음 위치부터 값을 읽어 0,1과 비교합니다. 0이면 루프를 빠져나오고 1이면 ESI 증가를 증가, 그 외의 값은 루프만 돕니다. 루프를 빠져나오면 ESI를 2와 비교해 작으면 invalid입니다.

즉, code에서 1의 값은 반드시 2개 이상 존재해야 합니다.(0은 어차피 code의 마지막 부분이므로)

첫번째 루프를 통과했으면 두번째 루프에 진입하고 code를 순서대로 읽으면서 0,1값일 경우 루프를 벗어나고 그 외의 값은 자신의 값을 ESI에 더합니다. 루프를 벗어난후 ESI의 값이 0x1D5(=469)이 아니면 invalid로 진행하게 됩니다. 즉, code에서 첫번째 1값 전의 값들의 합은 469이어야 합니다.



두 번의 검사를 통과한 후의 루틴입니다. 여기서도 두 개의 루프가 존재합니다.

루틴을 진행할 때 EBX는 초기화하지 않으므로 위의 루프에서 EBX 즉, code의 index는 첫 번째 1 value의 다음 위치부터 시작하게 됩니다.

첫 번째 루프에서 code의 값이 0,1 또는 읽은 갯수가 0x0F(=15)이면 루프를 빠져나가고 그 동안의 값을 XOR 연산을 하여 402160 주소에 저장합니다.

두 번째 루프에서 EBX가 초기화 되지 않으므로 시작 위치는 두 번째 1 이후나 첫 번째 1 이후의 15번째 값 이후입니다.

두 번째 루프는 0 value을 읽을 때만 빠져나오고 그 때까지의 값은 1을 제외하면 ESI에 더해져 이 값이 0x1B2(=434)이어야만 통과가 됩니다.

지금까지의 code의 조건을 전부 살펴보면 code의 길이는 18자 이상이어야 하고 0이 맨 마지막에 나와야 하며 0x01이 2개 이상 존재해야하며 첫 번째 0x01 이전의 값들의 합이 0x1D5(=469)이어야 하고 두 번째 0x01 다음의 값들의 합이 0x1B2(=434)이어야 합니다.

이에 맞는 코드 중 하나인 凝 箔. (0xEA 0xEB 0x01 0x02 ~ 0x01 0xDA 0xD8 0x00 을 파일에 넣어 실행하였습니다.



실행 결과 정답 화면이 나온것을 확인할 수 있습니다.