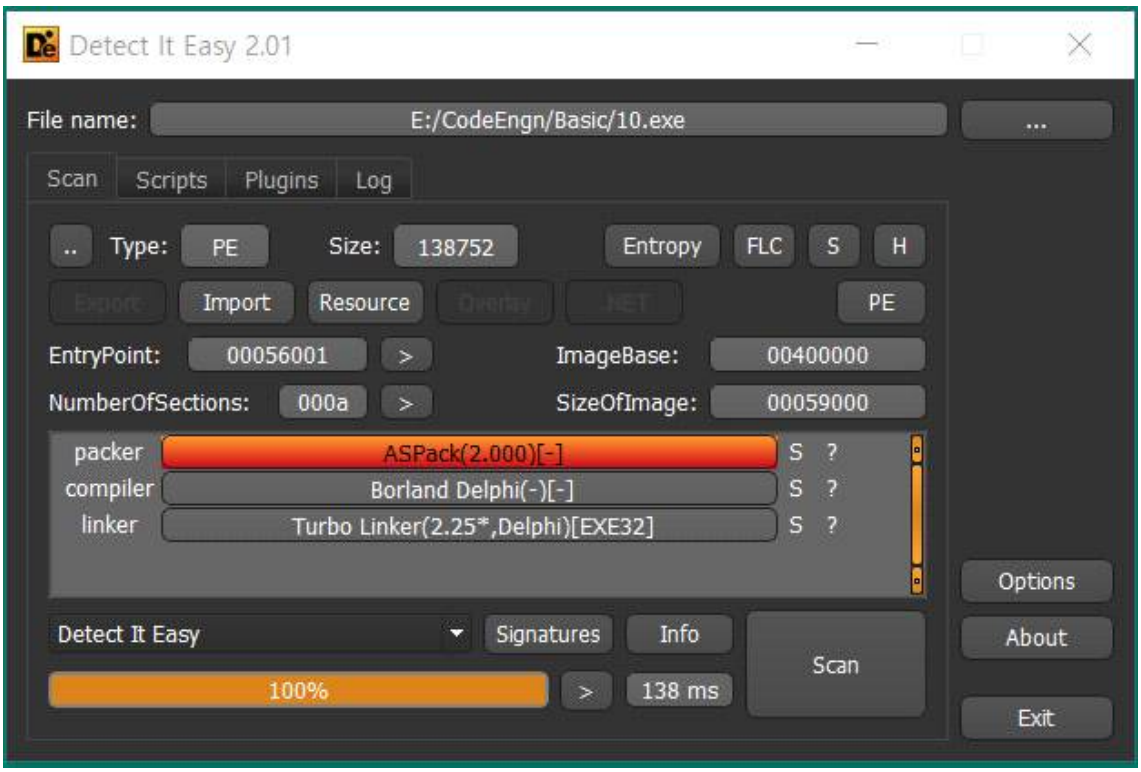
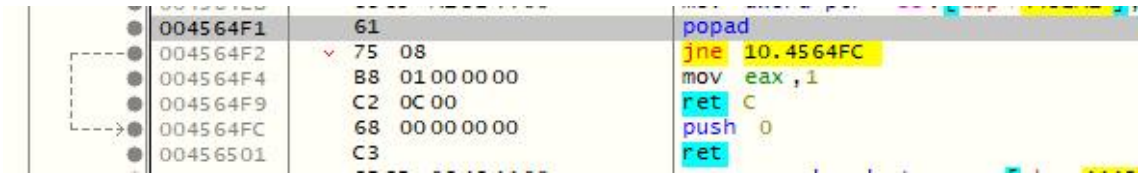
19.02.15 CodeEngn Basic RCE L10

Tree to Tree

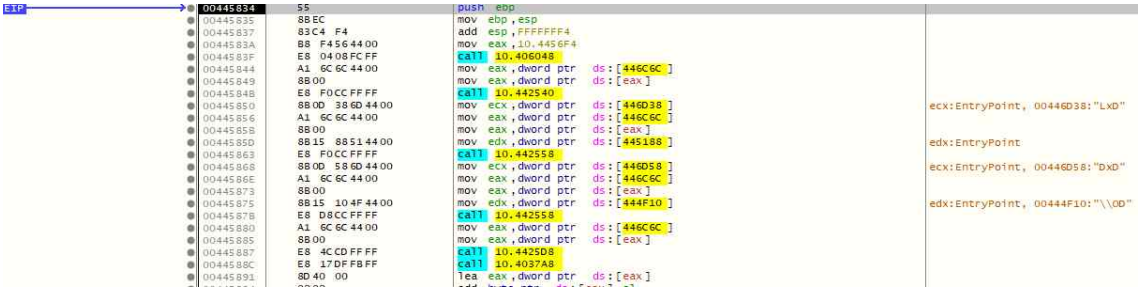


어떤 패커인지 확인 ASPack 을 사용중

UPX와 언팩하는 과정은 똑같다. 다른점이 있다면 ret과 jmp정도
pushad지점에서 멈춘 밑으로 쭉 내리면 popad를 발견할 수 있다.
popad에 breakpoint를 걸어준다.



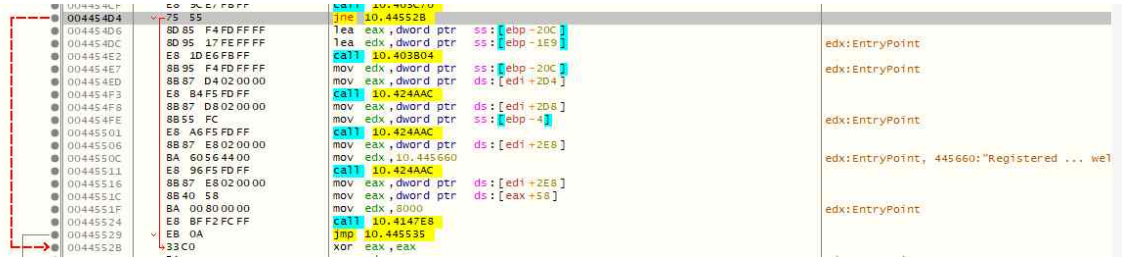
set into 를 4번만 눌러주면ret에 도달하는데 한번더 눌러서ret이 반환하는 주소로 가면 OEP를 만난다.



이제 등록성공 코드를 찾는일만 남았다.

실행시키면 name과 Serial에 입력이 안된다. 필터를 걸어놓거나 인터럽트를 막았다라고 생각해본 후에 제일 손쉬운 주변 문구를 검색

검색해보니 등록완료를 노골적으로 알려주는 문구 발견 따라가서 원하는 분기점을 찾아주면된다.



이제 조합해보면 OEP 값 00445834와
분기점 OPCODE 7555를 합치면
004458347555
Clear