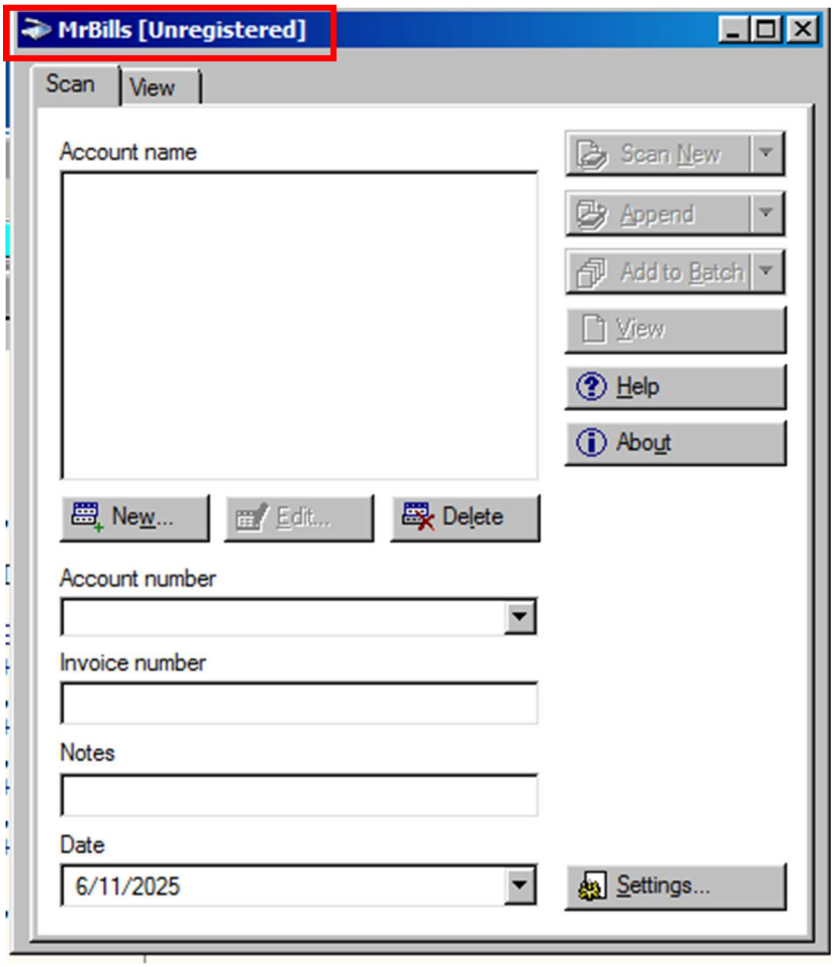
악성코드 분석 보고서

(sand-reversingwithlena-tutorials)

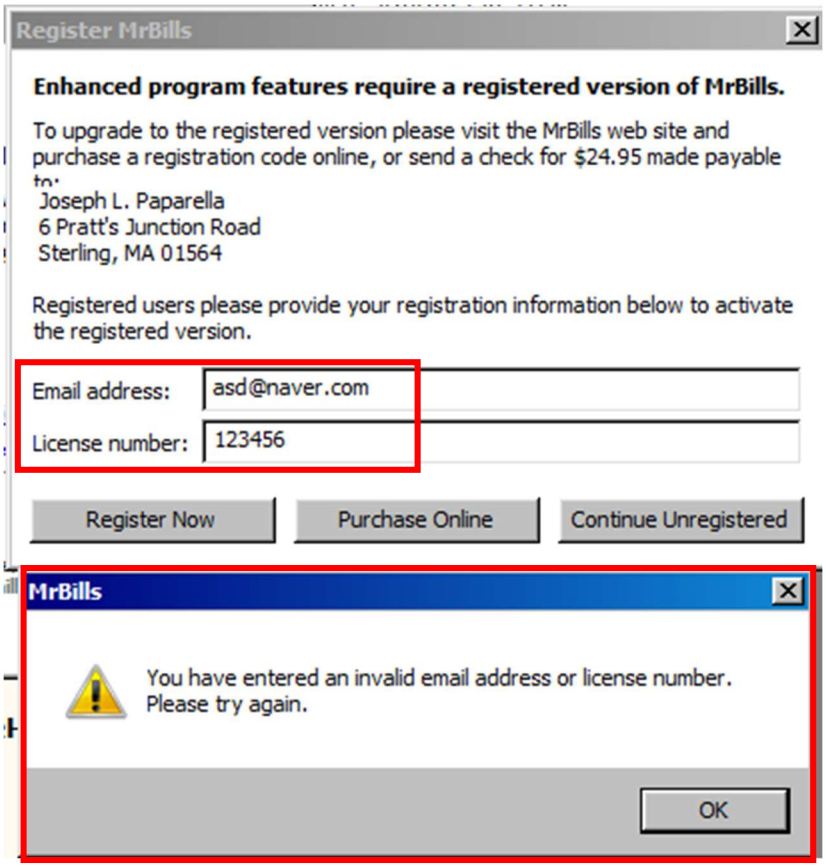
2025.06.11

07

1. 문제



MrBills [Unregistered] -> MrBills로 바꿔줘야한다.

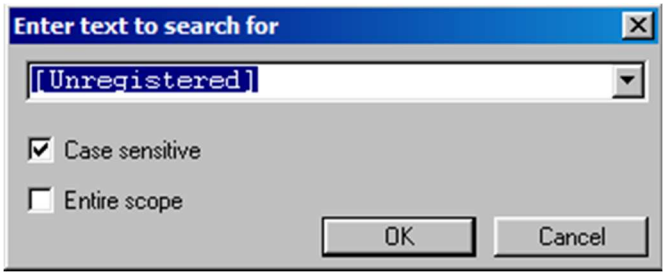


About > Register MrBills > 정보 입력 후 > Register Now 누르면 아래와 같은 경고 창이 발생한다. 이 경고 창이 발생하지 않게 해줘야한다.

2. 해결 방법

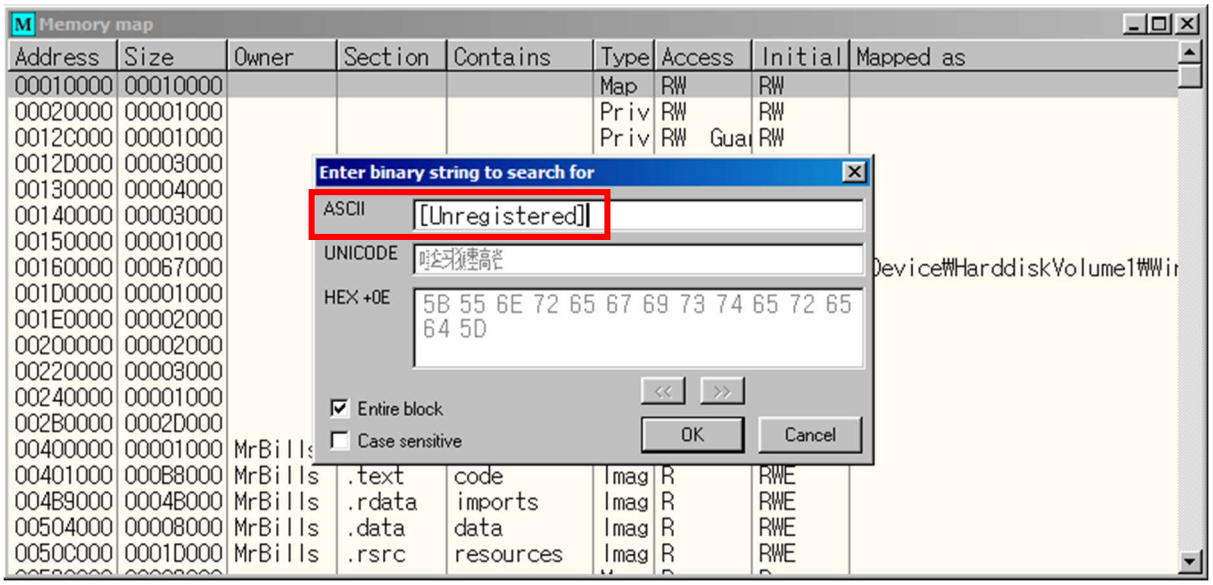
1) Main창

Search for > All referenced text strings 눌러서 [Unregistered] 해당 구문을 찾아준다.

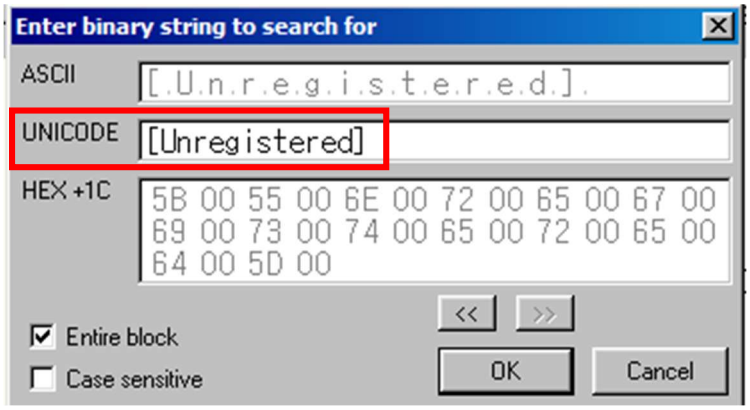


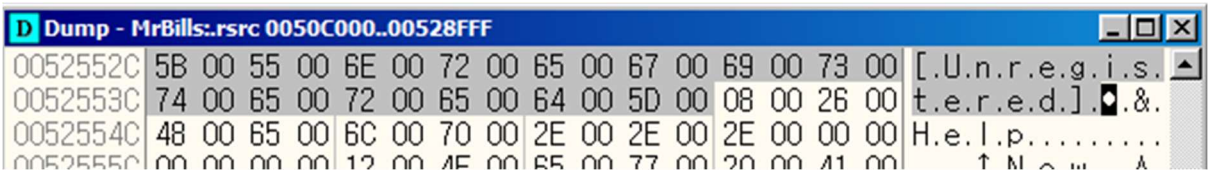
그럼 없다고 나오는데 이거는 참조하지 않고 있다는 뜻이다.

Memory map에 들어가 ASCII에서 먼저 찾아보면 찾을 수 없다는 걸 알 수 있다

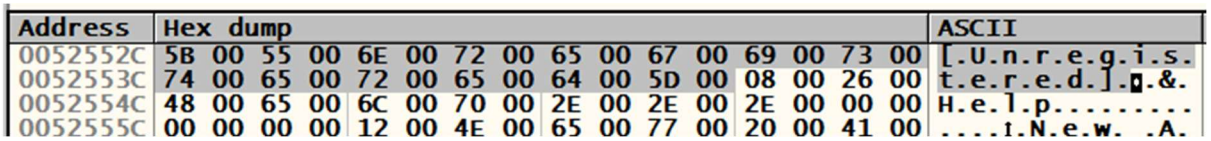


UNICODE에 넣어보면 나오는 걸 볼 수 있다.

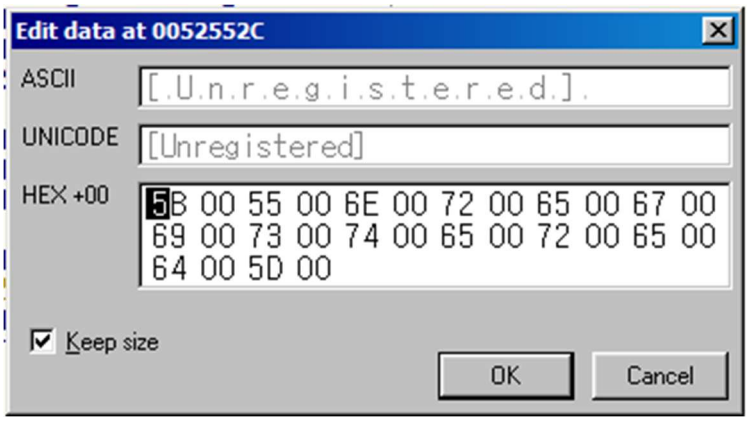




0x0052552C을 아래 덤프 부분에서 찾아본다.



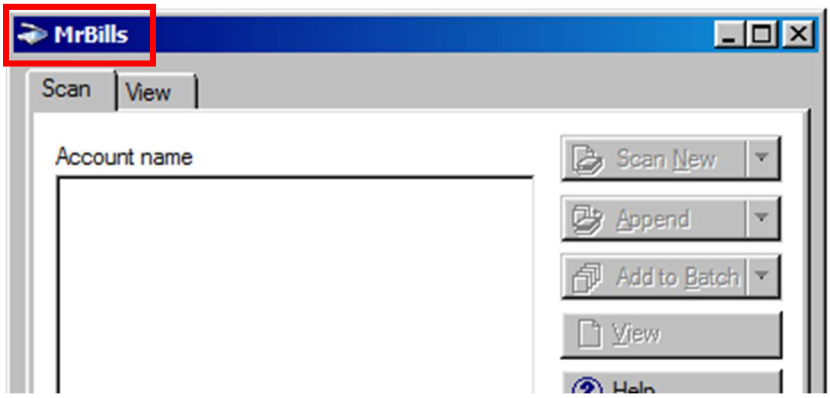
이 부분 [Unregistered]를 제거 해줄거다.



Keep size를 체크한 후 전부 다'00'으로 바꿔준다.

Copy to executable file > Save file 저장해준다.

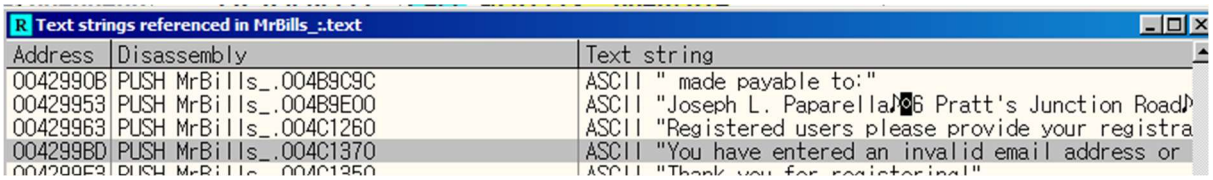
그리고 MrBills_patch1를 실행하면 없어진 걸 볼 수 있다.



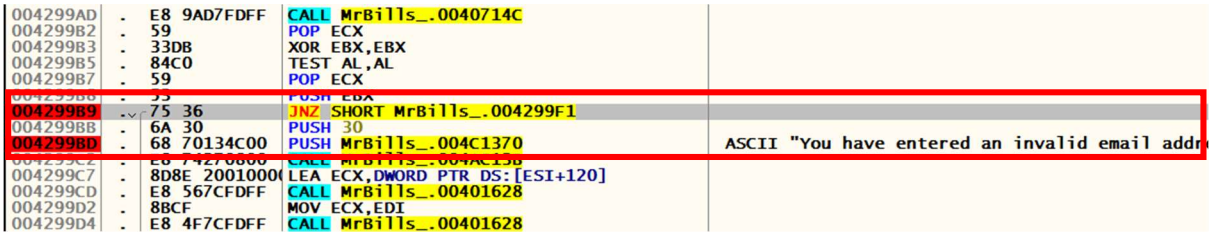
2) About 레지스터 키

경고 창의 구문인 'You have entered an invalid email address or license numbers.' 를 이용해서 어디서 쓰이는지 찾아준다.

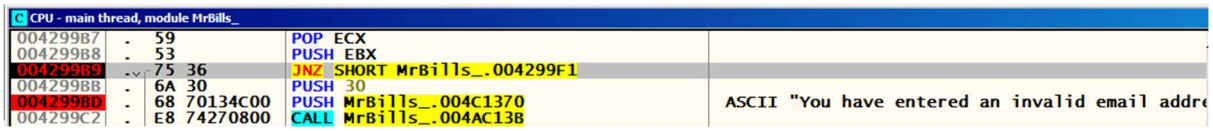
Search for > All referenced text strings 눌러서 You have entered an invalid email address or license numbers 해당 구문을 찾아준다.

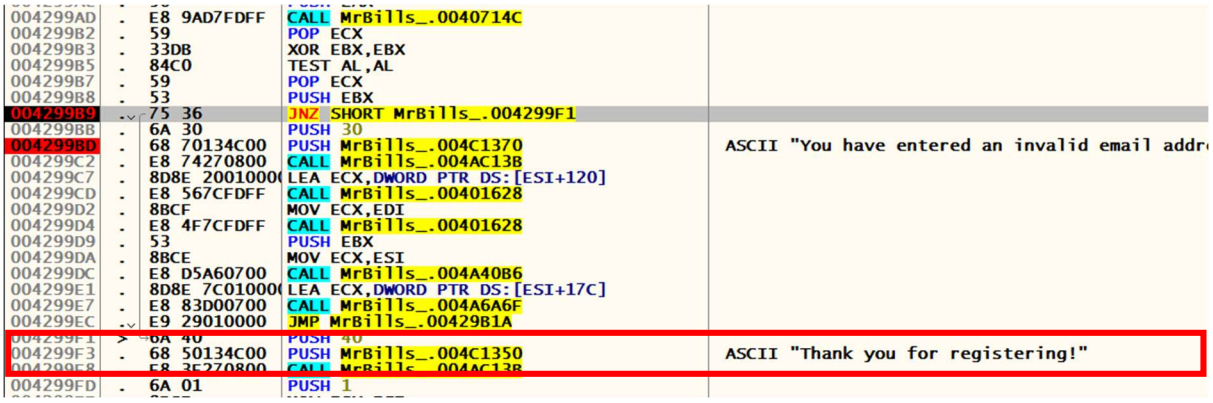


찾은 구문을 더블 클릭



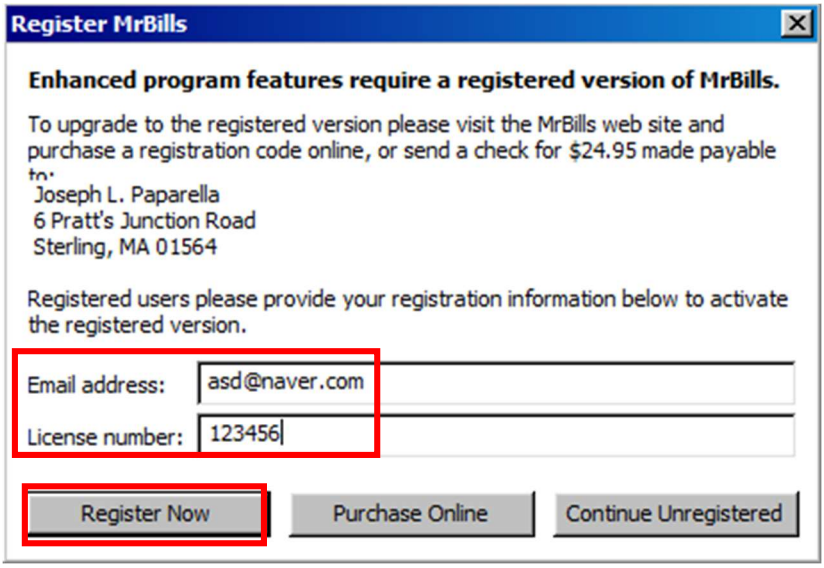
구문에다가 breakpoint를 그 주변에 분기문 찾아서 그 부분에도 breakpoint를 걸어주고 실행 해주면 Mrbill이 실행되는 걸 볼 수 있다. 그 다음 레지스터 정보를 입력해주고 Register Now 눌러주면 breakpoint 걸었던 곳에서 멈추는 것을 볼 수 있다.



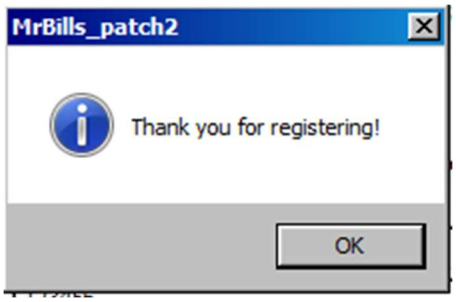


해당 창이 나오게 만들어야한다. 그럼 0x004299B9에서 점프해야하는 걸 볼 수 있다.

JNZ -> JMP로 바꿔주고 저장해주고 실행한다.



값들을 넣어주고 Register Now를 눌러주면

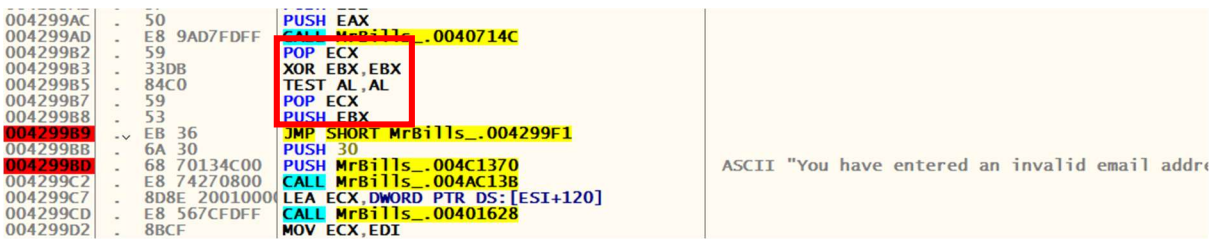


해당 창이 나오는 걸 볼 수 있다.

문제 해결!

※ 추가사항

처음부터 레지스터 키를 등록하면 Main창 위에 [Unregistered]가 없어진다.



빨간 박스있는 부분은 헷갈리게 하기 위해서 쓰레기 값을 넣는 걸 볼 수 있다.

EBX를 으로 초기화 했는데 쓰레기 값인 EBX를 PUSH하는 걸 볼 수 있고 ECX를 번이나 POP하는 걸 볼 수 있다.