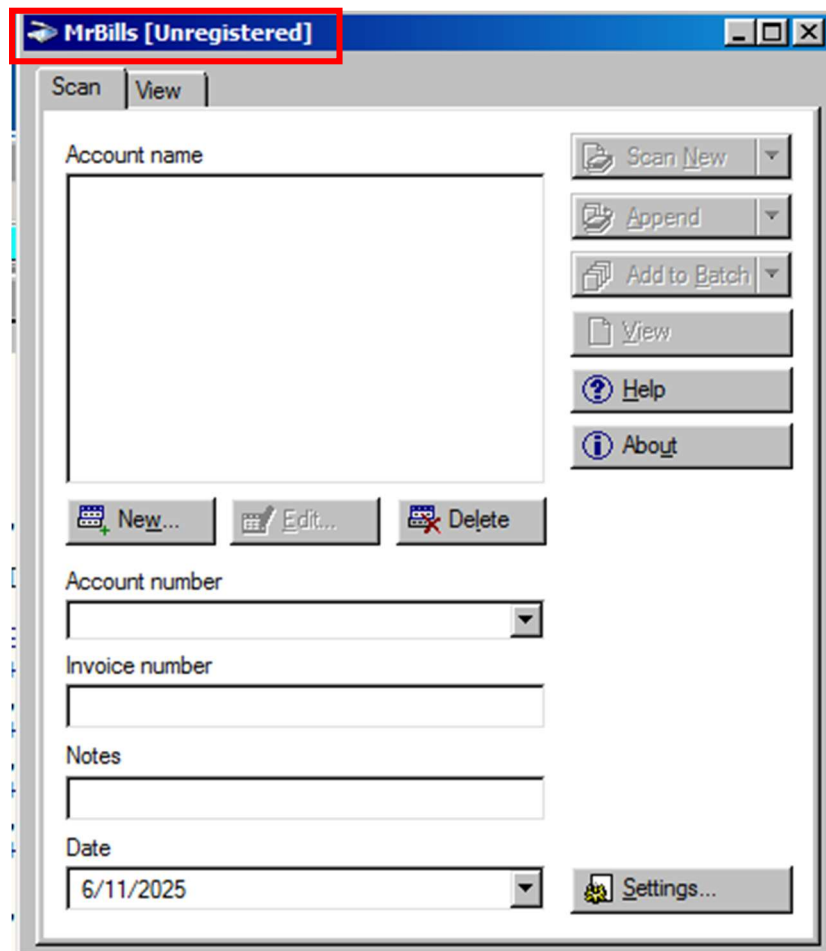


악성코드 분석 보고서

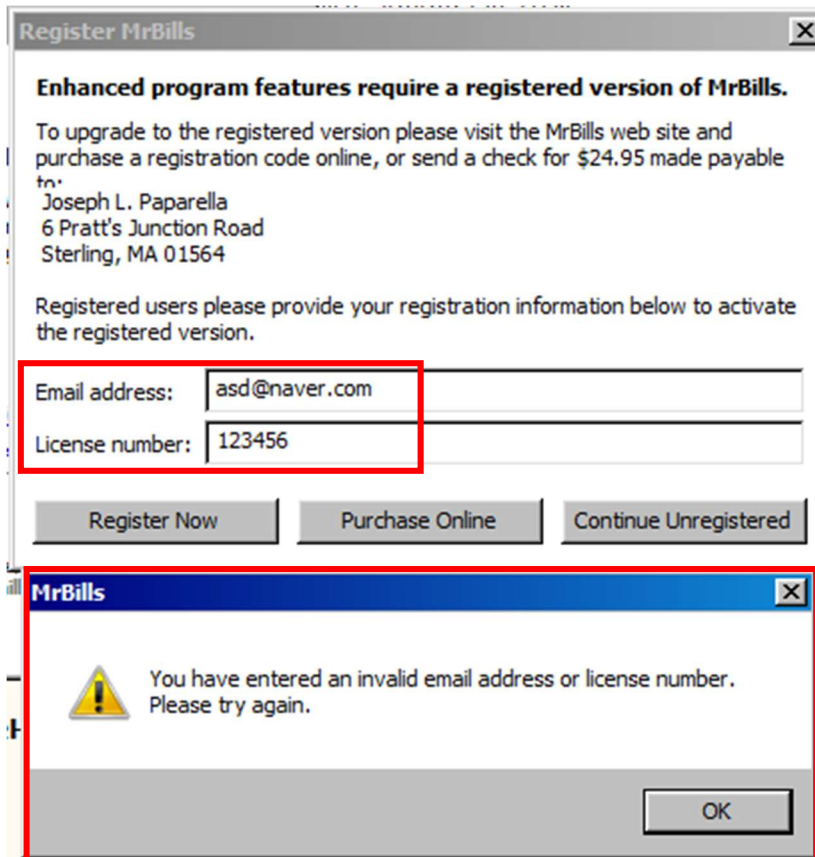
(sand-reversingwithlana-tutorials)

2025.06.11

1. 문제



MrBills [Unregistered] -> MrBills로 바꿔줘야한다.

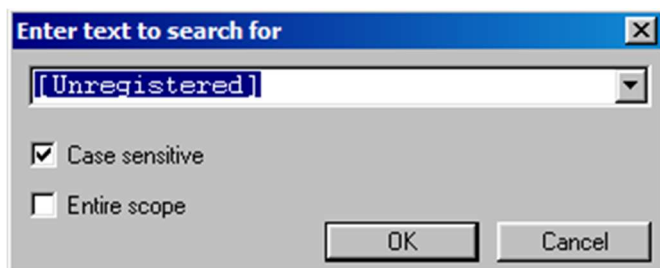


About > Register MrBills > 정보 입력 후 > Register Now 누르면 아래와 같은 경고 창이 발생한다. 이 경고 창이 발생하지 않게 해줘야한다.

2. 해결 방법

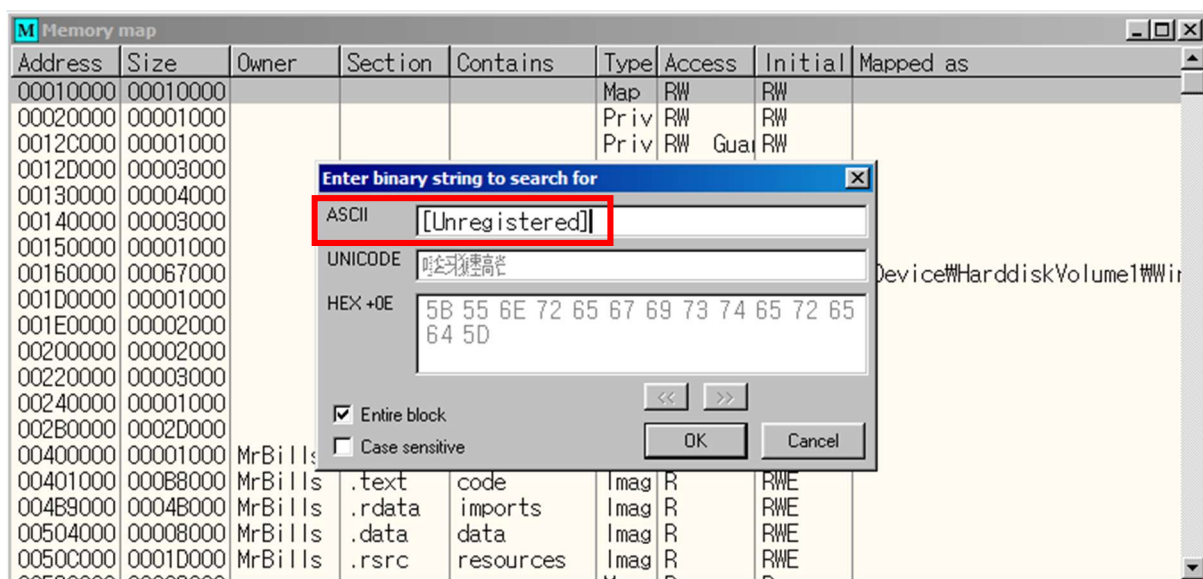
1) Main창

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

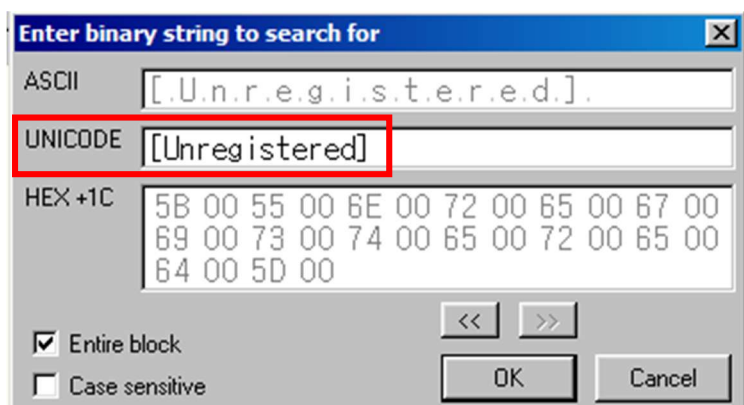


그럼 없다고 나오는데 이거는 참조하지 않고 있다는 뜻이다.

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



UNICODE에 넣어보면 나오는 걸 볼 수 있다.



D Dump - MrBills..rsrc 0050C000..00528FFF																	
0052552C	5B	00	55	00	6E	00	72	00	65	00	67	00	69	00	73	00	[.U.n.r.e.g.i.s.
0052553C	74	00	65	00	72	00	65	00	64	00	5D	00	08	00	26	00	t.e.r.e.d.]&
0052554C	48	00	65	00	6C	00	70	00	2E	00	2E	00	2E	00	00	00	H.e.l.p.....
0052555C	00	00	00	00	12	00	4E	00	65	00	77	00	20	00	41	00t.N.e.w..A.

0x0052552C을 아래 덤프 부분에서 찾아본다.

Address	Hex dump	ASCII
0052552C	5B 00 55 00 6E 00 72 00 65 00 67 00 69 00 73 00	[.U.n.r.e.g.i.s.
0052553C	74 00 65 00 72 00 65 00 64 00 5D 00 08 00 26 00	t.e.r.e.d.]&
0052554C	48 00 65 00 6C 00 70 00 2E 00 2E 00 2E 00 00 00	H.e.l.p.....
0052555C	00 00 00 00 12 00 4E 00 65 00 77 00 20 00 41 00t.N.e.w..A.

이 부분 [Unregistered]를 제거 해줄거다.

Edit data at 0052552C

ASCII: [.U.n.r.e.g.i.s.t.e.r.e.d.]

UNICODE: [Unregistered]

HEX +00: 5B 00 55 00 6E 00 72 00 65 00 67 00 69 00 73 00 74 00 65 00 72 00 65 00 64 00 5D 00

☒ Keep size

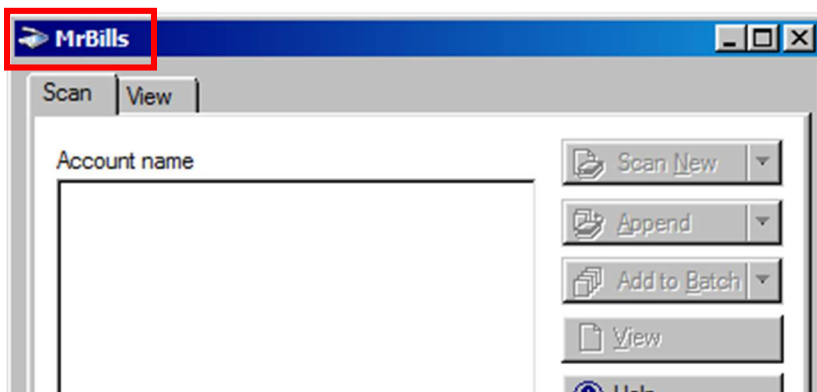
OK Cancel

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 이용하여 어디서 쓰이는지 찾아준다.

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

R Text strings referenced in MrBills_.text		
Address	Disassembly	Text string
0042990B	PUSH MrBills_.004B9C9C	ASCII " made payable to:"
00429953	PUSH MrBills_.004B9E00	ASCII "Joseph L. Paparella, 156 Pratt's Junction Road,
00429963	PUSH MrBills_.004C1260	ASCII "Registered users please provide your registra
004299BD	PUSH MrBills_.004C1370	ASCII "You have entered an invalid email address or
004299F3	PUSH MrBills_.004C1350	ASCII "Thank you for registering!"

찾은 구문을 더블 클릭

004299AD	E8 9AD7FDFF	CALL MrBills_.0040714C	
004299B2	59	POP ECX	
004299B3	33DB	XOR EBX,EBX	
004299B5	84C0	TEST AL,AL	
004299B7	59	POP ECX	
004299B8	53	PUSH EBX	
004299B9	75 36	JNZ SHORT MrBills_.004299F1	
004299BB	6A 30	PUSH 30	
004299BD	68 70134C00	PUSH MrBills_.004C1370	ASCII "You have entered an invalid email address or license numbers."
004299C2	E8 74270800	CALL MrBills_.004AC13B	
004299C7	8DBE 20010000	LEA ECX,DWORD PTR DS:[ESI+120]	
004299CD	E8 567CFDFF	CALL MrBills_.00401628	
004299D2	8BCF	MOV ECX,EDI	
004299D4	E8 4F7CFDFF	CALL MrBills_.00401628	

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.

CPU - main thread, module MrBills_			
004299B7	59	POP ECX	
004299B8	53	PUSH EBX	
004299B9	75 36	JNZ SHORT MrBills_.004299F1	
004299BB	6A 30	PUSH 30	
004299BD	68 70134C00	PUSH MrBills_.004C1370	ASCII "You have entered an invalid email address or license numbers."
004299C2	E8 74270800	CALL MrBills_.004AC13B	

004299AD	E8 9AD7FDFF	CALL MrBills_.0040714C	
004299B2	59	POP ECX	
004299B3	33DB	XOR EBX,EBX	
004299B5	84C0	TEST AL,AL	
004299B7	59	POP ECX	
004299B8	53	PUSH EBX	
004299B9	75 36	JNZ SHORT MrBills_.004299F1	
004299BB	6A 30	PUSH 30	
004299BD	68 70134C00	PUSH MrBills_.004C1370	ASCII "You have entered an invalid email address or license numbers."
004299C2	E8 74270800	CALL MrBills_.004AC13B	
004299C7	8DBE 20010000	LEA ECX,DWORD PTR DS:[ESI+120]	
004299CD	E8 567CFDFF	CALL MrBills_.00401628	
004299D2	8BCF	MOV ECX,EDI	
004299D4	E8 4F7CFDFF	CALL MrBills_.00401628	
004299D9	53	PUSH EBX	
004299DA	8BCE	MOV ECX,ESI	
004299DC	E8 D5A60700	CALL MrBills_.004A40B6	
004299E1	8DBE 7C010000	LEA ECX,DWORD PTR DS:[ESI+17C]	
004299E7	E8 83D00700	CALL MrBills_.004A6A6F	
004299EC	E9 29010000	JMP MrBills_.00429B1A	
004299F1	6A 40	PUSH 40	
004299F3	68 50134C00	PUSH MrBills_.004C1350	ASCII "Thank you for registering!"
004299F8	E8 3F270800	CALL MrBills_.004AC13B	
004299FD	6A 01	PUSH 1	

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

JNZ -> JMP로 바꿔주고 저장해주고 실행한다.

MrBills.exe
MrBills
Joseph L. Paparella

MrBills_patch1.exe
MrBills
Joseph L. Paparella

MrBills_patch2.exe
MrBills
Joseph L. Paparella

Register MrBills

Enhanced program features require a registered version of MrBills.

To upgrade to the registered version please visit the MrBills web site and purchase a registration code online, or send a check for \$24.95 made payable to:

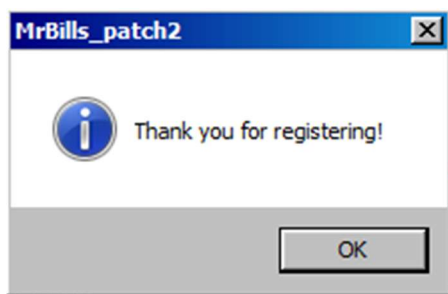
Joseph L. Paparella
6 Pratt's Junction Road
Sterling, MA 01564

Registered users please provide your registration information below to activate the registered version.

Email address:

License number:

값들을 넣어주고 Register Now를 눌러주면



해당 창이 나오는 걸 볼 수 있다.

문제 해결!

※ 추가사항

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

004299AC	- 50	PUSH EAX	
004299AD	- E8 9AD7FDF	CALL MrBills_.0040714C	
004299B2	- 59	POP ECX	
004299B3	- 33DB	XOR EBX,EBX	
004299B5	- 84C0	TEST AL,AL	
004299B7	- 59	POP ECX	
004299B8	- 53	PUSH EBX	
004299B9	- EB 36	JMP SHORT MrBills_.004299F1	
004299BB	- 6A 30	PUSH 30	
004299BD	- 68 70134C00	PUSH MrBills_.004C1370	
004299C2	- E8 74270800	CALL MrBills_.004AC13B	
004299C7	- 8D8E 20010000	LEA ECX,DWORD PTR DS:[ESI+120]	
004299CD	- E8 567CFDFF	CALL MrBills_.00401628	
004299D2	- 8BCF	MOV ECX,EDI	

ASCII "You have entered an invalid email address"

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

EBX를 0으로 초기화 했는데 쓰레기 값인 EBX를 PUSH하는 걸 볼 수 있고 ECX를 번이나 POP하는 걸 볼 수 있다.