

리버스 공학 / 기밀 레포트

태그	
체크박스	<input checked="" type="checkbox"/>
최종 편집 일시	@2024년 12월 6일 오후 6:04

문서 개요

- 해당 문서는 리버스 공학 기밀 프로젝트를 위해 작성되었다.
- 작성자 : 이창엽 / 20117669 / 컴퓨터소프트웨어학부 컴퓨터공학 전공

스타크래프트 시디키 알고리즘 분석

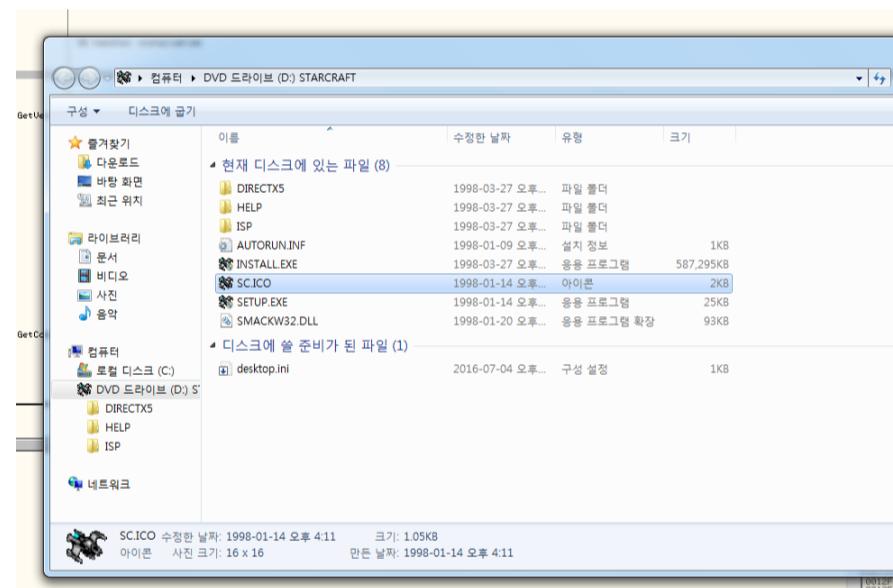
0. 설정 타겟

스타크래프트 ISO

- <https://m.blog.naver.com/lh6746/220579576600>
 - 스타크래프트 오리지널 버전 (시디키 알고리즘 분석)

설정 타겟은 스타크래프트 오리지널 버전 기준, 설치 과정에서 시리얼 키 입력을 요구한다.

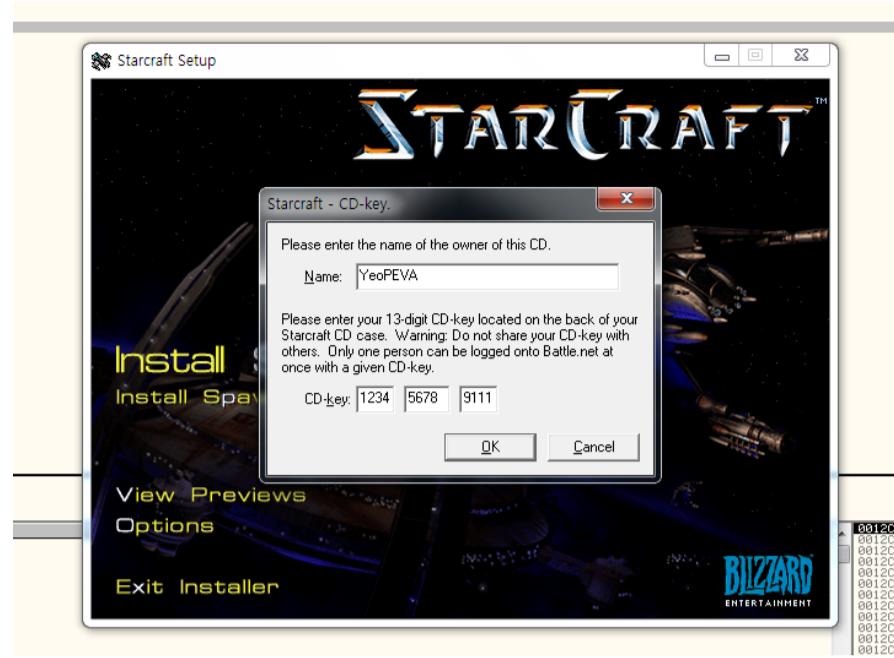
해당 시리얼 키 부분과 관련하여, 시리얼 키 인증 과정을 확인하고, 그에 따른 시리얼 키를 제작할 수 있는 별도의 프로그램을 제작하는 것을 목표로 진행하였다.



- 분석 대상 : INSTALL.EXE

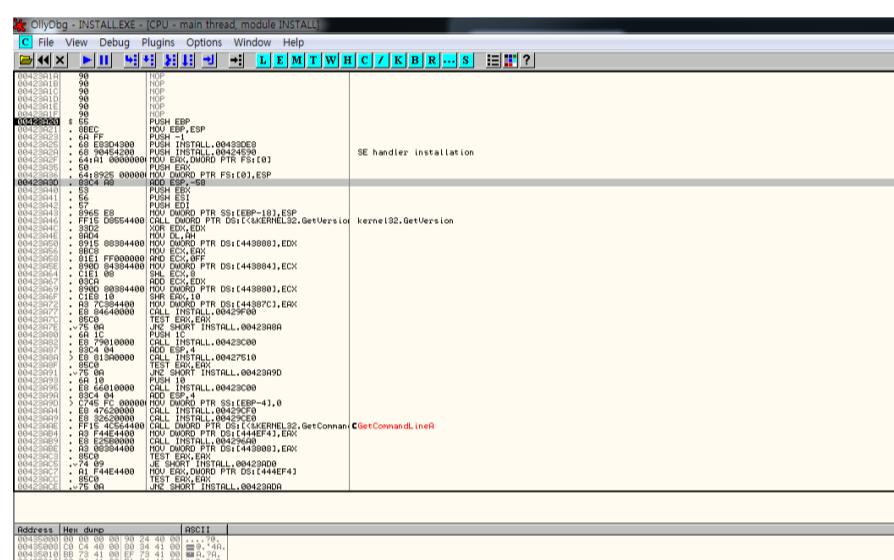


- 분석 대상 / 실행 화면



- 분석 대상 목표
 - CD-Key를 인증할 수 있는 키 제작
 - CD-Key 검증 과정 분석

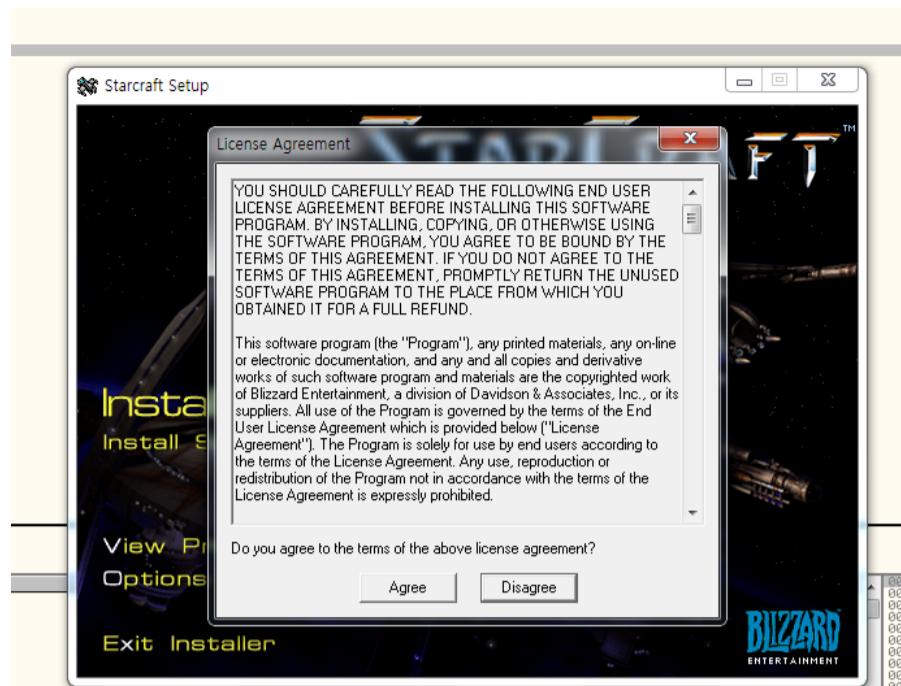
1. 타겟 분석



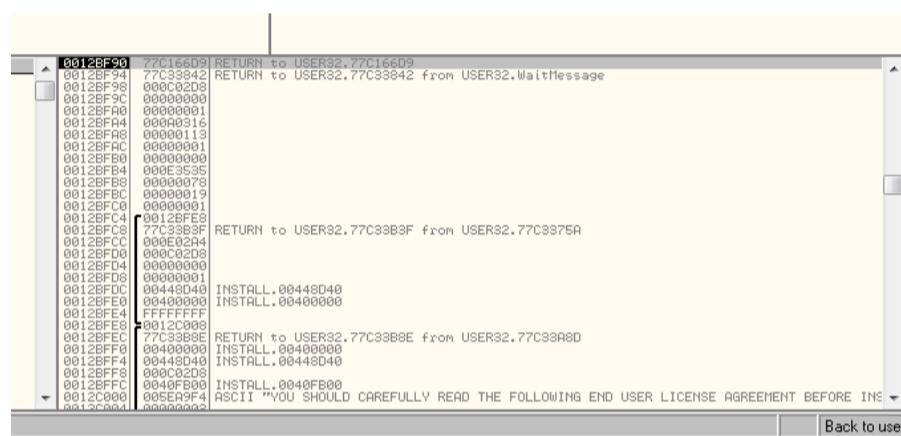
본격적인 타겟 분석을 위해, Ollydbg를 통해 설치 프로그램을 열었다.



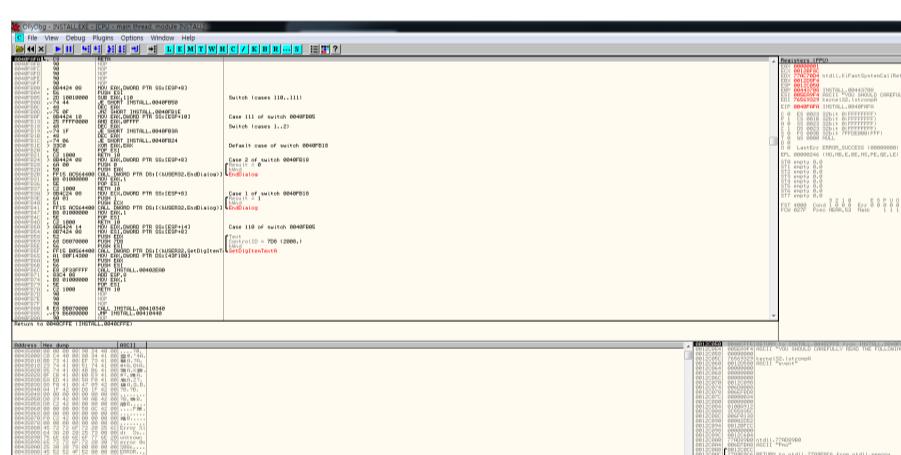
그 후 실행 과정을 통해, 프로그램을 실행하는 과정을 거친 이후



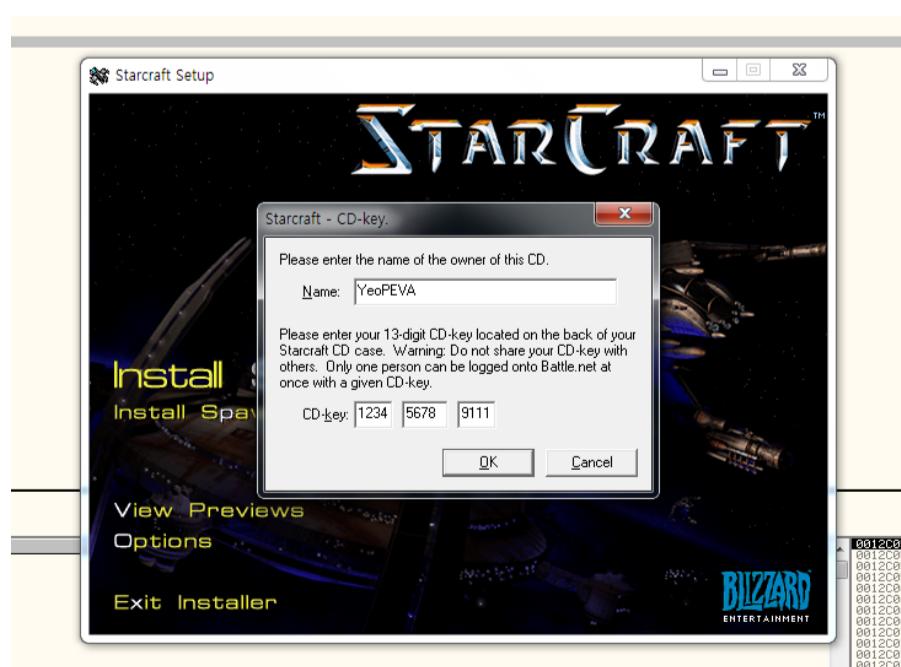
이용 약관 창에서, Back to User 기능을 통해, 인증 로직으로 접근을 하였다.



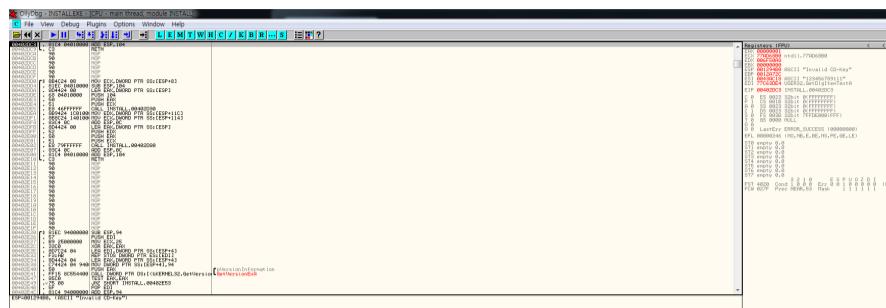
Back to User를 위와 같이 설정한 후,



위에서 나온 이용 약관을 클릭하면, 상단과 같이 Call 명령이 일어난 바로 다음 위치로 이동할 수 있었다.



상단 방법으로 Back to User 모드의 동작을 확인하였으며,
동일한 방식으로 키 인증 과정에 접근하기 위하여, CD-Key를 입력하고, 진행하였다.

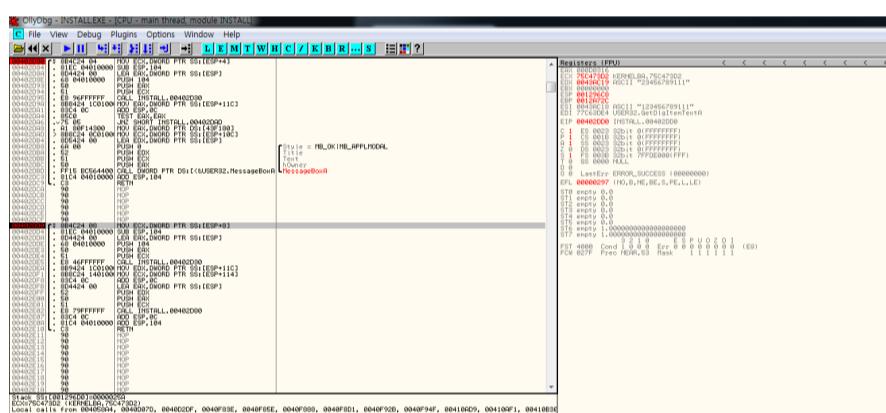


그 결과 위와 같이 이동할 수 있었다.

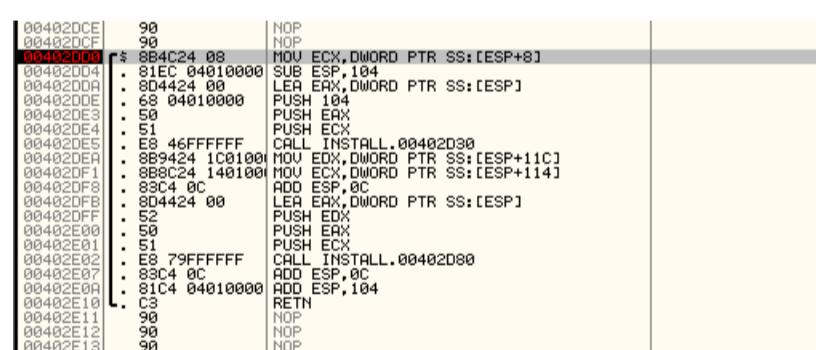


그 후, 이동한 측에 브레이크 포인트를 설정한 후, 계속하여 진행하였다.

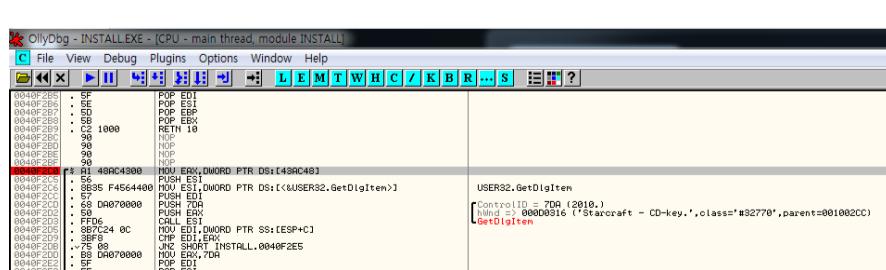
해당 부분은 메시지 박스 출력을 위해 활용되는 구문으로 확인 되었다.



이후, 분석을 이어서 진행하는 과정에서,

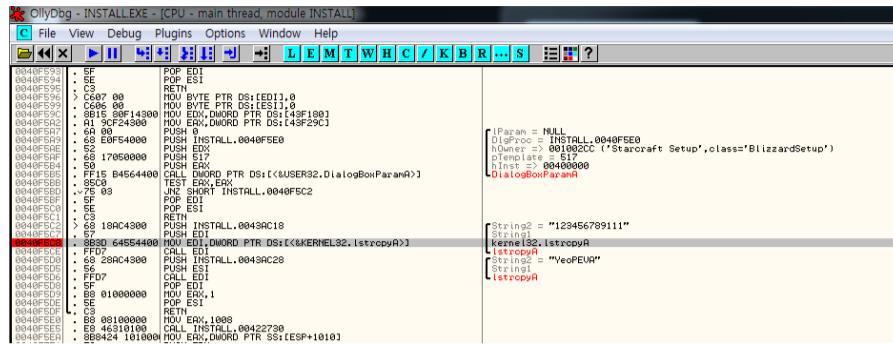


MOV ECX, DWORD PTR SS:[ESP+8] 내 다양한 주소에서 불려지는 명령어들이 존재하는 것을 확인하였으며,
해당 주소들을 확인해나가기 시작하였다.

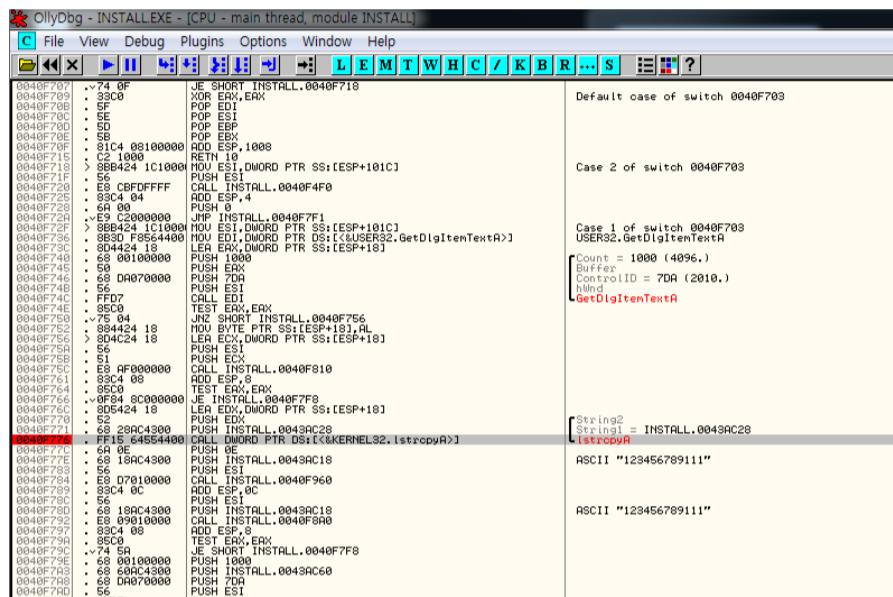


해당 주소들을 확인하는 과정에서, CD-key와 연계된 것으로 확인되는 부분을 확인하였으며,

해당 측으로 브레이크 포인트를 걸어준 이후, 분석을 이어나갔다.



그러는 과정에서, 키 값 및 유저 이름과 관련된 구문을 확인할 수 있었으며, 검증을 위해 준비하는 과정 중 하나로 파악되었다.



이후 추가적으로 확인하던 도중, 시리얼 키를 PUSH하고, 함수를 호출하는 구문들을 더 살펴보았다.

첫 번째 콜에 브레이크 포인트를 걸고, 분석을 진행하였으나 별다른 결과는 없었으며, 다음 호출 구문을 좀 더 상세히 분석하기로 하였다.



좀 더 상세한 확인을 위해, 브레이크 포인트 및 f7를 통해 step into를 진행하였다.

OllyDbg - INSTALL.EXE - [CPU - main thread, module INSTALL]

File View Debug Plugins Options Window Help

L E M T W H C / K B R ... S

Start - Key

String [strlenA]

```
0040F800 > $56 PUSH ESI
0040F801 . 8B7424 08 MOV ESI,DWORD PTR SS:[ESP+8]
0040F802 . 85F6 TEST ESI,ESI
0040F803 . . 57 PUSH EDI
0040F804 . . 55 PUSH ECX
0040F805 . . 56 0C JNE SHORT INSTALL.0040F8B6
0040F806 . . 6A 57 PUSH 57
0040F807 . . E8 B9700000 CALL INSTALL.0041696A
0040F808 . . 33C0 XOR EAX,EAX
0040F809 . . 5F POP EDI
0040F80A . . 5E POP ESI
0040F80B . . C3 RETN
0040F80C . . 56 PUSH ESI
0040F80D . . 55 PUSH EDI
0040F80E . . FF15 60554400 CALL QWORD PTR DS:[<&KERNEL32,strlenA>]
0040F80F . . 89C8 0D ADD ESP,0C
0040F810 . . 54 10 JE SHORT INSTALL.0040F8DE
0040F811 . . 8B4424 10 MOU EAX,DWORD PTR SS:[ESP+10]
0040F812 . . 50 PUSH EAX
0040F813 . . 68 50020000 PUSH 25A
0040F814 . . 68 50020000 PUSH 25B
0040F815 . . E8 FR34FFFF CALL INSTALL.004020D0
0040F816 . . 89C4 0C ADD ESP,0C
0040F817 . . 33C0 XOR EAX,EAX
0040F818 . . 5F POP EDI
0040F819 . . 5E POP ESI
0040F81A . . C3 RETN
0040F81B . > B8 00000000 MOU EAX,3
0040F81C . . 33D2 XOR EDX,EDX
0040F81D . > 8ABC32 CMP CL,30
0040F81E . . 7C 53 JL SHORT INSTALL.0040F940
0040F81F . . 80F9 39 CMP CL,39
0040F820 . . 74 00 JE SHORT INSTALL.0040F940
0040F821 . . 0FBEC9 MOVSX ECX,CX
0040F822 . . 80DC00 LEA EDI,DWORD PTR DS:[EAX+EAX]
0040F823 . . 83E9 30 SUB ECX,30
0040F824 . . 33F9 XOR EDI,ECX
0040F825 . . 03C7 ADD EAX,EDI
0040F826 . . 42 INC EDX
0040F827 . . 83FA 0C CMP EDX,0C
0040F828 . . 72 E0 JNE SHORT INSTALL.0040F8E5
0040F829 . . 33D2 XOR EDX,EDX
0040F82A . . 80F9 00 MOU EDX,0A
0040F82B . . 7F 71 DIV EDX,0A
0040F82C . . 0FBE46 0C MOVSX EAX,BYTE PTR DS:[ESI+C]
0040F82D . . 0FBE02 00 MOVSX EDX,DL
0040F82E . . 80C2 30 ADD EDX,30
0040F82F . . 3B2C 00 CMR EDX,EDX
0040F830 . . 74 1C JE SHORT INSTALL.0040F938
0040F831 . . 8B4C24 10 MOU ECX,DWORD PTR SS:[ESP+10]
0040F832 . . 51 PUSH ECX
0040F833 . . 68 50020000 PUSH 259
0040F834 . . 68 50020000 PUSH 25B
0040F835 . . E8 A034FFFF CALL INSTALL.004020D0
0040F836 . . 80C4 0C ADD ESP,0C
0040F837 . . 33C0 XOR EAX,EAX
0040F838 . . 5F POP EDI
0040F839 . . 5E POP ESI
0040F83A . . C3 RETN
0040F83B . > B8 01000000 MOU EAX,1
0040F83C . . 33D2 XOR EDI,EDX
0040F83D . . 5E POP ESI
0040F83E . . C3 RETN
0040F83F . > B85424 10 MOU EDX,DWORD PTR SS:[ESP+10]
0040F840 . . 52 PUSH EDX
0040F841 . . 68 50020000 PUSH 259
0040F842 . . 68 50020000 PUSH 25B
0040F843 . . E8 7C34FFFF CALL INSTALL.004020D0
0040F844 . . 89C4 0C ADD ESP,0C
0040F845 . . 33C0 XOR EAX,EAX
0040F846 . . 5F POP EDI
0040F847 . . 5E POP ESI
0040F848 . . C3 RETN
0040F849 . . 99 hno
```

그 결과, 해당 함수 내에서 진행되는 부분이 키 시리얼 인증과 관련된 구문임을 확인할 수 있었으며, 해당 구문들을 상세히 분석하기 시작하였다.

2. 분석 시작위치 결정

OllyDbg - INSTALL.EXE - [CPU - main thread, module INSTALL]

C File View Debug Plugins Options Window Help

L E M T W H C / K B R ... S

Start - Key

[String [\[strlenA\]](#)

0040F8800 F5 56 PUSH ES
0040F8801 8B7424 08 MOV ESI,DWORD PTR SS:[ESP+8]
0040F8802 85F6 TEST ESI,ESI
0040F8803 .57 PUSH EDI
0040F8804 .75 0C JNC SHORT INSTALL.0040F886
0040F8805 .6A 57 PUSH 57
0040F8806 .EB 97000000 CALL INSTALL.0041696A
0040F8807 .3C00 XOR EDX,EDX
0040F8808 .SF POP EDI
0040F8809 .5E POP ESI
0040F880A .C3 RETN
0040F880B > 56 PUSH ES
0040F880C FF15 60554400 CALL DWORD PTR DS:[&KERNEL32.IstrlenA]
0040F880D 83F8 00 CMP EAX,0D
0040F880E .74 1C JE SHORT INSTALL.0040F8DE
0040F880F .8B4424 10 ADD ESP,0C
0040F8810 .3C00 XOR EDX,EDX
0040F8811 .SF PUSH EDI
0040F8812 .5E POP ESI
0040F8813 .C3 RETN
0040F8814 > B8 50020000 CALL INSTALL.00402DD0
0040F8815 .8B3C 0C ADD ESP,0C
0040F8816 .3C00 XOR EDX,EDX
0040F8817 .5F POP EDI
0040F8818 .5E POP ESI
0040F8819 .C3 RETN
0040F881A > B8 03000000 CALL INSTALL.00402DD0
0040F881B .3C02 XOR EDX,EDX
0040F881C .8B0C32 MOU CL,BYTE PTR DS:[EDX+ESI]
0040F881D .80F9 30 CMP CL,30
0040F881E .7C 53 JL SHORT INSTALL.0040F940
0040F881F .80F9 39 CMP CL,39
0040F8820 .7F 4E JO SHORT INSTALL.0040F940
0040F8821 .0FBEC9 MOVSX ECX,CL
0040F8822 .80D3C000 LEA EDI,DWORD PTR DS:[EAX+EAX]
0040F8823 .83F9 30 XOR ECX,ECX
0040F8824 .3C07 ADD EDX,EDI
0040F8825 .42 INC EDX
0040F8826 .83FA 0C CMP EDX,0C
0040F8827 .72 E0 JB SHORT INSTALL.0040F8E5
0040F8828 .33D2 XOR EDX,EDX
0040F8829 .B9 0A000000 MOV ECX,0A
0040F882A .F7F1 DIV ECX
0040F882B .0FBEE6 0C MOVSX EDX,BYTE PTR DS:[ESI+C]
0040F882C .80F9E000 MOVSX EDX,BYTE PTR DS:[EDX+DL]
0040F882D .3C02 XOR EDX,EDX
0040F882E .3C02 XOR EDX,EDX
0040F882F .74 1C JE SHORT INSTALL.0040F938
0040F8830 .8B4C24 10 MOV ECX,DWORD PTR SS:[ESP+10]
0040F8831 .51 PUSH ECX
0040F8832 .6A 59020000 PUSH 59
0040F8833 .68 58020000 PUSH 58
0040F8834 .EB A034FFFF CALL INSTALL.00402DD0
0040F8835 .3C00 XOR EDX,EDX
0040F8836 .SF POP EDI
0040F8837 .5E POP ESI
0040F8838 .C3 RETN
0040F8839 > B8 01000000 MOV EDX,1
0040F883A .5F POP EDI
0040F883B .5E POP ESI
0040F883C .C3 RETN
0040F883D > 8B5424 10 MOV EDX,DWORD PTR SS:[ESP+10]
0040F883E .6A 59020000 PUSH 59
0040F883F .68 58020000 PUSH 58
0040F8840 .EB 7C34FFFF CALL INSTALL.00402DD0
0040F8841 .88C4 0C ADD ESP,0C
0040F8842 .3C00 XOR EDX,EDX
0040F8843 .5F POP EDI
0040F8844 .5E POP ESI
0040F8845 .C3 RETN

해당 코드들을 확인하고, 브레이크 포인트를 활용하여 검증한 결과, `IstrlenA`를 통해 키의 길이가 13자리가 맞는지를 확인하는 구문이였다.

그렇기에 본격적인 시리얼 검증 과정과 관련된 부분은 `mov eax,3`이라는 것을 확인할 수 있었다.

```

0040F8D0: .SE      POP    ESI
0040F8D1: .RE     RETN
0040F8D2: > B8 03000000 MOU   EDX,3
0040F8D3: .33D2 XOR   EDX,EDX
0040F8D4: > 8A0C32 MOV    CL,BYTE PTR DS:[EDX+ESI]
0040F8D5: .80F9 30 CMP   CL,30
0040F8D6: .7C 53 JL SHORT INSTALL.0040F940
0040F8D7: .80F9 39 CMP   CL,39
0040F8D8: .7E 46 JE SHORT INSTALL.0040F940
0040F8D9: .0FBEC9 MOV    ECX,CL
0040F8DA: .8D3C00 LEA    EDI,DWORD PTR DS:[EAX+EAX]
0040F8DB: .83E9 30 ADD   EDX,30
0040F8DC: .33F9 XOR   EDI,ECX
0040F8DD: .03C7 ADD   EDX,EDI
0040F8DE: .42 INC   EDX
0040F8DF: .83FA 0C CMP   EDX,0C
0040F8E0: ^72 E0 JB SHORT INSTALL.0040F8E5
0040F8E1: .80F9 30 MOU   ECX,CL
0040F8E2: .80F9 30 XOR   EDX,EDX
0040F8E3: .F7F1 DIV   ECX
0040F8E4: .0FBED2 ADD   EDX,DL
0040F8E5: .83C2 30 ADD   EDX,30
0040F8E6: .33C0 XOR   ECX,ECX
0040F8E7: .03C7 ADD   EDX,EDI
0040F8E8: .42 INC   EDX
0040F8E9: .884C24 10 JE SHORT INSTALL.0040F938
0040F8EA: .B9 0A000000 MOU   ECX,DWORD PTR SS:[ESP+10]
0040F8EB: .51 PUSH ECX
0040F8EC: .68 50020000 PUSH EBP
0040F8ED: .E8 A034FFF CALN  INSTALL.004020D0
0040F8EE: .33D2 XOR   EBP,0C
0040F8EF: .33D0 POP   EDI
0040F8F0: .5F POP   ESI
0040F8F1: .5E POP   ECX
0040F8F2: .7C 46 RETN
0040F8F3: > B8 01000000 MOU   EDX,1
0040F8F4: .5F POP   EDI
0040F8F5: .5E POP   ESI
0040F8F6: .C3 RETN
0040F8F7: > B8 01000000 MOU   EDX,1
0040F8F8: .5F POP   EDI
0040F8F9: .5E POP   ESI
0040F8FA: .7C 46 RETN
0040F8FB: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8FC: .68 50020000 PUSH EBP
0040F8FD: .68 50020000 PUSH EBP
0040F8FE: .E8 A034FFF CALN  INSTALL.004020D0
0040F8FF: .33D2 XOR   EBP,0C
0040F800: .33C0 ADD   EBP,0C
0040F801: .33C0 XOR   ECX,ECX
0040F802: .33F9 POP   EDI
0040F803: .03C7 ADD   EDX,EDI
0040F804: .42 INC   EDX
0040F805: .83FA 0C CMP   EDX,0C
0040F806: .^72 E0 \JB SHORT INSTALL.0040F8E5
0040F807: .33D2 XOR   EDX,EDX
0040F808: .B9 0A000000 MOU   ECX,0A
0040F809: .F7F1 DIV   ECX
0040F80A: .51 PUSH ECX
0040F80B: .68 50020000 PUSH EBP
0040F80C: .E8 A034FFF CALN  INSTALL.004020D0
0040F80D: .33D2 XOR   EBP,0C
0040F80E: .33D0 POP   EDI
0040F80F: .5F POP   ESI
0040F810: .5E POP   ECX
0040F811: .7C 46 RETN
0040F812: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F813: .68 50020000 PUSH EBP
0040F814: .68 50020000 PUSH EBP
0040F815: .E8 A034FFF CALN  INSTALL.004020D0
0040F816: .33D2 XOR   EBP,0C
0040F817: .33C0 ADD   EBP,0C
0040F818: .33C0 XOR   ECX,ECX
0040F819: .33F9 POP   EDI
0040F81A: .03C7 ADD   EDX,EDI
0040F81B: .42 INC   EDX
0040F81C: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F81D: .68 50020000 PUSH EBP
0040F81E: .68 50020000 PUSH EBP
0040F81F: .E8 A034FFF CALN  INSTALL.004020D0
0040F820: .33D2 XOR   EBP,0C
0040F821: .33D0 POP   EDI
0040F822: .5F POP   ESI
0040F823: .5E POP   ECX
0040F824: .7C 46 RETN
0040F825: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F826: .68 50020000 PUSH EBP
0040F827: .68 50020000 PUSH EBP
0040F828: .E8 A034FFF CALN  INSTALL.004020D0
0040F829: .33D2 XOR   EBP,0C
0040F82A: .33D0 POP   EDI
0040F82B: .5F POP   ESI
0040F82C: .5E POP   ECX
0040F82D: .7C 46 RETN
0040F82E: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F82F: .68 50020000 PUSH EBP
0040F830: .68 50020000 PUSH EBP
0040F831: .E8 A034FFF CALN  INSTALL.004020D0
0040F832: .33D2 XOR   EBP,0C
0040F833: .33D0 POP   EDI
0040F834: .5F POP   ESI
0040F835: .5E POP   ECX
0040F836: .7C 46 RETN
0040F837: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F838: .68 50020000 PUSH EBP
0040F839: .68 50020000 PUSH EBP
0040F83A: .E8 A034FFF CALN  INSTALL.004020D0
0040F83B: .33D2 XOR   EBP,0C
0040F83C: .33D0 POP   EDI
0040F83D: .5F POP   ESI
0040F83E: .5E POP   ECX
0040F83F: .7C 46 RETN
0040F840: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F841: .68 50020000 PUSH EBP
0040F842: .68 50020000 PUSH EBP
0040F843: .E8 A034FFF CALN  INSTALL.004020D0
0040F844: .33D2 XOR   EBP,0C
0040F845: .33D0 POP   EDI
0040F846: .5F POP   ESI
0040F847: .5E POP   ECX
0040F848: .7C 46 RETN
0040F849: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F84A: .68 50020000 PUSH EBP
0040F84B: .68 50020000 PUSH EBP
0040F84C: .E8 A034FFF CALN  INSTALL.004020D0
0040F84D: .33D2 XOR   EBP,0C
0040F84E: .33D0 POP   EDI
0040F84F: .5F POP   ESI
0040F850: .5E POP   ECX
0040F851: .7C 46 RETN
0040F852: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F853: .68 50020000 PUSH EBP
0040F854: .68 50020000 PUSH EBP
0040F855: .E8 A034FFF CALN  INSTALL.004020D0
0040F856: .33D2 XOR   EBP,0C
0040F857: .33D0 POP   EDI
0040F858: .5F POP   ESI
0040F859: .5E POP   ECX
0040F85A: .7C 46 RETN
0040F85B: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F85C: .68 50020000 PUSH EBP
0040F85D: .68 50020000 PUSH EBP
0040F85E: .E8 A034FFF CALN  INSTALL.004020D0
0040F85F: .33D2 XOR   EBP,0C
0040F860: .33D0 POP   EDI
0040F861: .5F POP   ESI
0040F862: .5E POP   ECX
0040F863: .7C 46 RETN
0040F864: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F865: .68 50020000 PUSH EBP
0040F866: .68 50020000 PUSH EBP
0040F867: .E8 A034FFF CALN  INSTALL.004020D0
0040F868: .33D2 XOR   EBP,0C
0040F869: .33D0 POP   EDI
0040F86A: .5F POP   ESI
0040F86B: .5E POP   ECX
0040F86C: .7C 46 RETN
0040F86D: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F86E: .68 50020000 PUSH EBP
0040F86F: .68 50020000 PUSH EBP
0040F870: .E8 A034FFF CALN  INSTALL.004020D0
0040F871: .33D2 XOR   EBP,0C
0040F872: .33D0 POP   EDI
0040F873: .5F POP   ESI
0040F874: .5E POP   ECX
0040F875: .7C 46 RETN
0040F876: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F877: .68 50020000 PUSH EBP
0040F878: .68 50020000 PUSH EBP
0040F879: .E8 A034FFF CALN  INSTALL.004020D0
0040F87A: .33D2 XOR   EBP,0C
0040F87B: .33D0 POP   EDI
0040F87C: .5F POP   ESI
0040F87D: .5E POP   ECX
0040F87E: .7C 46 RETN
0040F87F: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F880: .68 50020000 PUSH EBP
0040F881: .68 50020000 PUSH EBP
0040F882: .E8 A034FFF CALN  INSTALL.004020D0
0040F883: .33D2 XOR   EBP,0C
0040F884: .33D0 POP   EDI
0040F885: .5F POP   ESI
0040F886: .5E POP   ECX
0040F887: .7C 46 RETN
0040F888: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F889: .68 50020000 PUSH EBP
0040F88A: .68 50020000 PUSH EBP
0040F88B: .E8 A034FFF CALN  INSTALL.004020D0
0040F88C: .33D2 XOR   EBP,0C
0040F88D: .33D0 POP   EDI
0040F88E: .5F POP   ESI
0040F88F: .5E POP   ECX
0040F890: .7C 46 RETN
0040F891: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F892: .68 50020000 PUSH EBP
0040F893: .68 50020000 PUSH EBP
0040F894: .E8 A034FFF CALN  INSTALL.004020D0
0040F895: .33D2 XOR   EBP,0C
0040F896: .33D0 POP   EDI
0040F897: .5F POP   ESI
0040F898: .5E POP   ECX
0040F899: .7C 46 RETN
0040F89A: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F89B: .68 50020000 PUSH EBP
0040F89C: .68 50020000 PUSH EBP
0040F89D: .E8 A034FFF CALN  INSTALL.004020D0
0040F89E: .33D2 XOR   EBP,0C
0040F89F: .33D0 POP   EDI
0040F8A0: .5F POP   ESI
0040F8A1: .5E POP   ECX
0040F8A2: .7C 46 RETN
0040F8A3: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8A4: .68 50020000 PUSH EBP
0040F8A5: .68 50020000 PUSH EBP
0040F8A6: .E8 A034FFF CALN  INSTALL.004020D0
0040F8A7: .33D2 XOR   EBP,0C
0040F8A8: .33D0 POP   EDI
0040F8A9: .5F POP   ESI
0040F8AA: .5E POP   ECX
0040F8AB: .7C 46 RETN
0040F8AC: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8AD: .68 50020000 PUSH EBP
0040F8AE: .68 50020000 PUSH EBP
0040F8AF: .E8 A034FFF CALN  INSTALL.004020D0
0040F8B0: .33D2 XOR   EBP,0C
0040F8B1: .33D0 POP   EDI
0040F8B2: .5F POP   ESI
0040F8B3: .5E POP   ECX
0040F8B4: .7C 46 RETN
0040F8B5: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8B6: .68 50020000 PUSH EBP
0040F8B7: .68 50020000 PUSH EBP
0040F8B8: .E8 A034FFF CALN  INSTALL.004020D0
0040F8B9: .33D2 XOR   EBP,0C
0040F8BA: .33D0 POP   EDI
0040F8BB: .5F POP   ESI
0040F8BC: .5E POP   ECX
0040F8BD: .7C 46 RETN
0040F8BE: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8BF: .68 50020000 PUSH EBP
0040F8C0: .68 50020000 PUSH EBP
0040F8C1: .E8 A034FFF CALN  INSTALL.004020D0
0040F8C2: .33D2 XOR   EBP,0C
0040F8C3: .33D0 POP   EDI
0040F8C4: .5F POP   ESI
0040F8C5: .5E POP   ECX
0040F8C6: .7C 46 RETN
0040F8C7: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8C8: .68 50020000 PUSH EBP
0040F8C9: .68 50020000 PUSH EBP
0040F8CA: .E8 A034FFF CALN  INSTALL.004020D0
0040F8CB: .33D2 XOR   EBP,0C
0040F8CD: .33D0 POP   EDI
0040F8CE: .5F POP   ESI
0040F8CF: .5E POP   ECX
0040F8D0: .7C 46 RETN
0040F8D1: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D2: .68 50020000 PUSH EBP
0040F8D3: .68 50020000 PUSH EBP
0040F8D4: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D5: .33D2 XOR   EBP,0C
0040F8D6: .33D0 POP   EDI
0040F8D7: .5F POP   ESI
0040F8D8: .5E POP   ECX
0040F8D9: .7C 46 RETN
0040F8D0: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D1: .68 50020000 PUSH EBP
0040F8D2: .68 50020000 PUSH EBP
0040F8D3: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D4: .33D2 XOR   EBP,0C
0040F8D5: .33D0 POP   EDI
0040F8D6: .5F POP   ESI
0040F8D7: .5E POP   ECX
0040F8D8: .7C 46 RETN
0040F8D9: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D0: .68 50020000 PUSH EBP
0040F8D1: .68 50020000 PUSH EBP
0040F8D2: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D3: .33D2 XOR   EBP,0C
0040F8D4: .33D0 POP   EDI
0040F8D5: .5F POP   ESI
0040F8D6: .5E POP   ECX
0040F8D7: .7C 46 RETN
0040F8D8: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D9: .68 50020000 PUSH EBP
0040F8D0: .68 50020000 PUSH EBP
0040F8D1: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D2: .33D2 XOR   EBP,0C
0040F8D3: .33D0 POP   EDI
0040F8D4: .5F POP   ESI
0040F8D5: .5E POP   ECX
0040F8D6: .7C 46 RETN
0040F8D7: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D8: .68 50020000 PUSH EBP
0040F8D9: .68 50020000 PUSH EBP
0040F8D0: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D1: .33D2 XOR   EBP,0C
0040F8D2: .33D0 POP   EDI
0040F8D3: .5F POP   ESI
0040F8D4: .5E POP   ECX
0040F8D5: .7C 46 RETN
0040F8D6: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D7: .68 50020000 PUSH EBP
0040F8D8: .68 50020000 PUSH EBP
0040F8D9: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D0: .33D2 XOR   EBP,0C
0040F8D1: .33D0 POP   EDI
0040F8D2: .5F POP   ESI
0040F8D3: .5E POP   ECX
0040F8D4: .7C 46 RETN
0040F8D5: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D6: .68 50020000 PUSH EBP
0040F8D7: .68 50020000 PUSH EBP
0040F8D8: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D9: .33D2 XOR   EBP,0C
0040F8D0: .33D0 POP   EDI
0040F8D1: .5F POP   ESI
0040F8D2: .5E POP   ECX
0040F8D3: .7C 46 RETN
0040F8D4: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D5: .68 50020000 PUSH EBP
0040F8D6: .68 50020000 PUSH EBP
0040F8D7: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D8: .33D2 XOR   EBP,0C
0040F8D9: .33D0 POP   EDI
0040F8D0: .5F POP   ESI
0040F8D1: .5E POP   ECX
0040F8D2: .7C 46 RETN
0040F8D3: .885424 10 MOU   EDX,DWORD PTR SS:[ESP+10]
0040F8D4: .68 50020000 PUSH EBP
0040F8D5: .68 50020000 PUSH EBP
0040F8D6: .E8 A034FFF CALN  INSTALL.004020D0
0040F8D7: .33D
```

4. 취약점 검증

취약점을 검증하기 위하여, 위에서 분석된 내용을 기반으로, python 코드를 작성하여 시리얼 키 인증을 통과할 수 있는 시리얼 키를 제작하는 프로그램을 만들었다.

```
def generate_serial():
    import random

    # 12자리 숫자를 랜덤으로 생성
    serial_base = [random.randint(0, 9) for _ in range(12)]

    eax = 3  # 초기화
    for num in serial_base:
        ecx = num
        edi = eax + eax
        eax += edi ^ ecx

    # 나머지 계산
    remainder = eax % 10

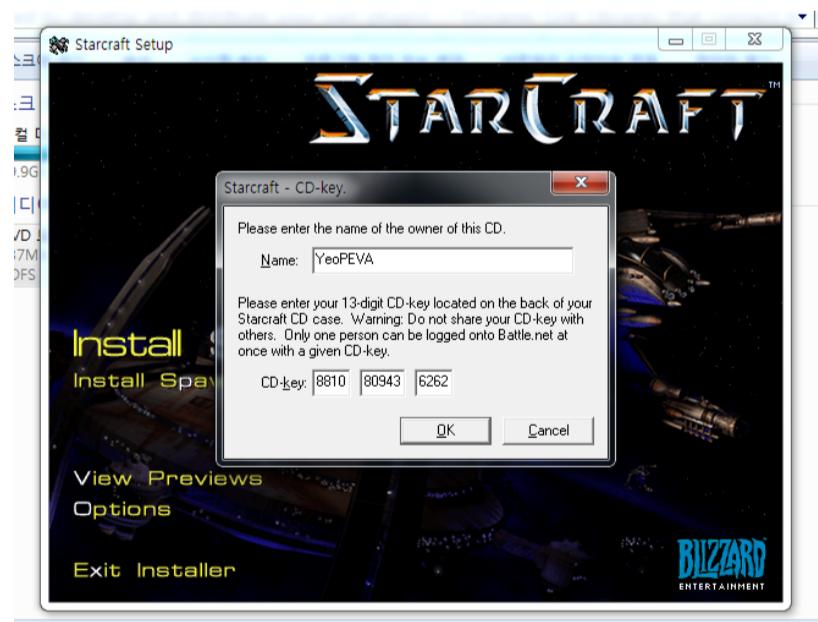
    # 13번째 자리값 추가
    serial_base.append(remainder)

    # 시리얼 키 문자열로 반환
    return ''.join(map(str, serial_base))

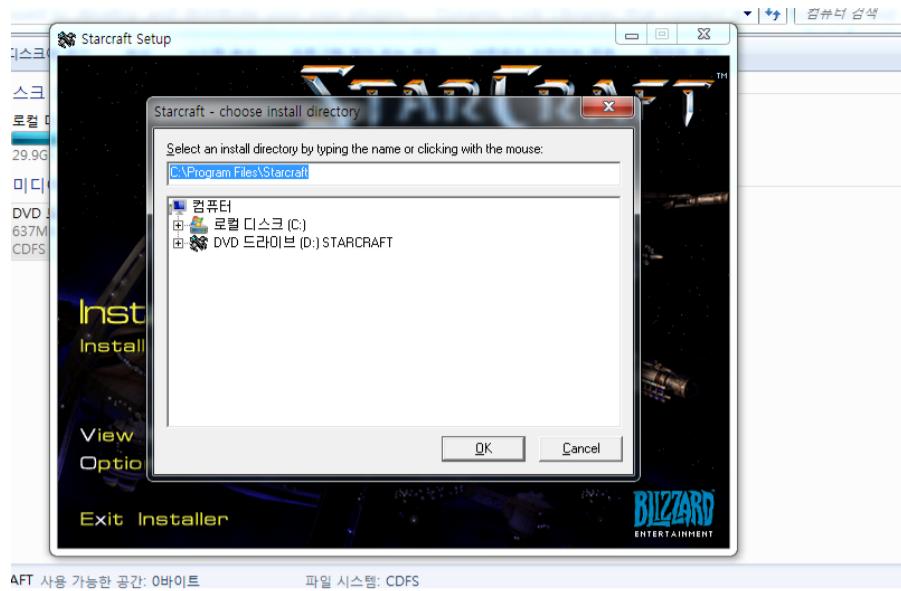
if __name__ == "__main__":
    serial_key = generate_serial()
    print(f"Generated Serial Key: {serial_key}")
```

```
> python solve.py
Generated Serial Key: 4994854882323
> python
solve.py
Generated Serial Key: 8810809436262
> python
solve.py
Generated Serial Key: 5451556667087
```

그 결과, 위와 같은 시리얼 키를 확보할 수 있었으며, 해당 키 구문을 통해 인증을 시도하였다.



- 8810-80943-6262 (설치 시도)



- 인증 성공

5. 결론

타겟 분석 결과, 시리얼 키 인증 과정에서 별도로 인터넷 연결이 없어도 설치가 가능한 프로그램이기에, 시리얼 키 인증 로직을 프로그램 내에서 진행한다고 파악하였으며, 이를 분석하기 위해 back-to-user-mode를 활용하여 키 로직 근처로 이동 후, 분석을 함으로써 시리얼 키 검증 로직을 찾을 수 있었다.

찾아낸 키 검증 로직을 분석하여, 별도의 파이썬 코드를 작성한 후, 시리얼 키를 제작하고 이를 설치 프로그램에 실제로 활용함으로써 취약점을 검증할 수 있었으며, 이를 통해 시리얼 키를 생성하여 프로그램을 지속하여 인증할 수 있기에 해당 취약점 검증 결과는 활용이 가능하다.