

# 07.Intermediate level patching, Kanal in PEiD

2012년 1월 28일 토요일

오후 8:27

Hello everybody.

모두들 안녕.

Welcome to this Part 7 in my series about reversing for newbies/beginners.

나의 초보자 reversing series Part 7에 온 것을 환영해.

This "saga" is intended for complete starters in reversing, also for those without any programming experience at all.

이 "saga"는 완벽히 reversing 초보자를 맞춰서 만들어졌다. 또한 어떠한 programming 경험이 없어도 된다.

## 1. Abstract

This Part 7 is about reversing a "real" application to learn something about patching a registration scheme in the intermediate level patching method.

이번 Part 7에서는 "real" application을 중간 level patching 방법 중의 registration scheme patching 하는 법을 배우겠습니다.

Remember that Part #6 dealt with patching in the plain stupid way.

기억해? Part 6에서 명백히 명청한 방법으로 patch 했다.

A real application because indeed, the best practice is found in real applications.

Real application에서 최고의 연습 방법을 찾았다.

For better comprehension and if you are a newbie, I advise you to first see the previous parts in this series before seeing this movie.

네가 초보자라면 좀 더 좋은 이해력을 얻으려면, 이 movie를 보기 전에 이 series의 이전 part를 먼저 봐라.

The goal of this tutorial is to teach you something about a program's behaviour.

이 tutorial의 목표는 program's behaviour를 너에게 가르치는 것이다.

In my search not to harm authors, I came across MrBills.

나의 MrBills 연구는 제작자에게 피해를 주지 않는다.

This Program does not exist any longer : the company was sold and the program discontinued.

이 program은 더 이상 존재하지 않는다 : 회사는 program을 판매를 중단했다.

However, because it could be misused, I only included the main executable (not the install exe !) for your research in the shown techniques.

잘못된 사용을 하게 두지 않는다. 나는 보여지는 기술에서 너의 연구를 위해 오직 main executable을 포함했다.(install exe가 아니다)

This makes the program useless for other purposes than studying material.

Program 은 다른 목적으로 공부하는 것이 필요없다.

Taking a look in the specialized media, I also found this application to be "cracked" already.

특화된 media 를 봐라. 나는 또한 이 application 에서 이미 "cracked" 된 버전을 찾았다.

Here, this software is only chosen because it is ideal for this tutorial in reversing and it is targeted for educational purposes only.

여기, 이 software 는 오직 선택됐다. 왜냐하면 그것은 reversing 에서 이 tutorial 은 이상적이다.

그리고 그것은 오직 공부 목적의 target 이 됐다.

I hope you will exploit your newly acquired knowledge in a positive way.

In this matter, I also want to refer to Part 1.

네가 새롭게 얻은 지식을 긍정적인 방향으로 이용해.

Set your screen resolution to 1152\*864 and press F11 to see the movie full screen !!!

Again, I have made this movie interactive.

You screen 해상도를 1152\*864 로 설정해 그리고 full screen 으로 movie 를 보기 위해 F11 를 눌러

So, if you are a fast reader and you want to continue to the next screen, just click here on this invisible hotspot. You don't see it, but it IS there on text screens.

그래서, 네가 이것을 빨리 읽고 다음 screen 을 보고 싶다면, 보이는 hotspot 여기를 눌러. 보고 싶지 않을 때는 여기에 두지마.

Then the movie will skip the text and continue with the next screen.

Movie 는 text 와 다음 screen 을 skip 할 수 있다.

If something is not clear or goes too fast, you can always use the control buttons and the slider below on this screen.

무언가 명확하지 않거나 빨리 넘기고자 할 때, 항상 control button 과 이 screen 밑에 있는 slider 바를 사용해.

He, try it out and click on the hotspot to skip this text and to go to the next screen now!!!

도전해봐. 그리고 이 text 와 다음 screen 을 보기 위해 hotspot 을 click 해.

During the whole movie you can click this spot to leave immediately

이 movie 어디에서나 즉시 떠나기 위해 이 spot 을 click 할 수 있다.

## 2. Tools and Target

### 이것도 똑같음

The tools for today are : Ollydebug and... your brain.

오늘 이 tools : Ollydebug 와 너의 두뇌다.

The first can be obtained for free at

첫번째로 무료로 얻을 수 있다.

<http://www.ollydbg.de>

PEID is a free tool and can be downloaded :

PEID 는 공짜 tool 이고 download 할 수 있다.

<http://peid.has.it>

Again, the brain is your responsibility ;)

두뇌는 너의 책임감이다.

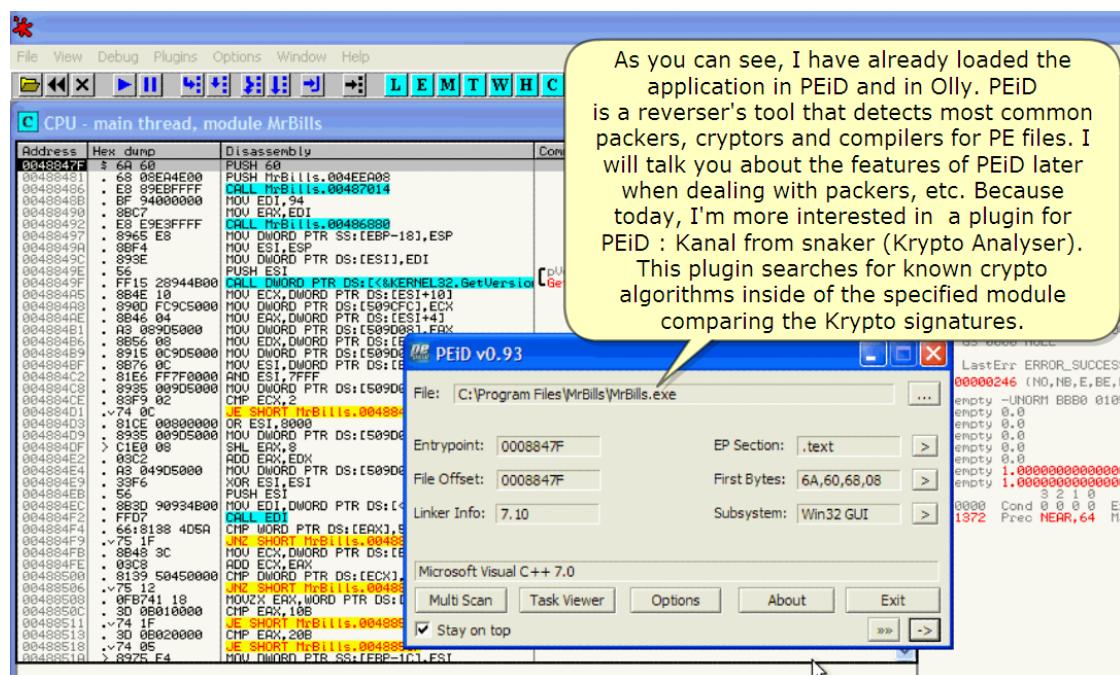
Todays target is a program called MrBills.

오늘 target program 은 MrBills 로 불린다.

Because it can no longer be downloaded, I have included the main executable-only in this package for your research.

왜냐하면 그것은 더 이상 download 되지 않는다. 나는 이 package 에서 너의 연구를 위해 오직 main executable 파일만 포함했다.

### 3. Behaviour of the program



As you can see, I have already loaded the application in PEID and in Olly.

네가 봤을 때, 나는 이미 PEID 와 Olly 에서 application 을 load 했다.

PEID is a reverser's tool that detects most common packers, cryptors and compilers for PE files.

번역 주)Compiler: 특정 프로그래밍 언어로 쓰여 있는 문서를 다른 프로그래밍 언어로 옮기는 프로그램을 말한다. 원래의 문서를 소스 코드 혹은 원시 코드라고 부르고, 출력된 문서를 목적 코드라고 부른다. 목적 코드는 주로 다른 프로그램이나 하드웨어가 처리하기에 용이한 형태로 출력되지만 사람이 읽을 수 있는 문서 파일이나 그림 파일 등으로 옮기는 경우도 있다. 원시

코드에서 목적 코드로 옮기는 과정을 Compile 이라고 한다. Compiler 는 소스 프로그램을 읽어서 즉시 결과를 출력하는 인터프리터와는 구분된다. 소스 코드를 Compile 하는 이유는 대부분 사람에게 이해하기 쉬운 형태의 고수준 언어로부터 실행 가능한 기계어 프로그램을 만들기 위해서이다. 좁은 의미의 Compiler 는 주로 고수준 언어로 쓰인 소스 코드를 저수준 언어(assemble)로 번역하는 프로그램을 가리킨다.

PEiD 는 reverser's tool 이다. 그것은 공통 packer, cryptor, compiler 를 찾을 수 있다.

I will talk you about the features of PEiD later when dealing with packers, etc.

나중에 우리가 packer 와 deal 할 경우 PEiD 의 특징에 대해서 이야기 할 것이다.

Because today, I'm more interested in a plugin for PEiD : kanal from snaker (Krypto Analyzer).

오늘은 PEiD 를 위한 plugin 에서 좀 더 흥미롭다. : kanal from snaker(Krypto 해석기)

This plugin searches for known crypto algorithms inside of the specified module comparing the Krypto signatures.

이 plugin 은 알고 있는 crypto algorithm 의 명시된 module 에서 Krypto signature 를 비교하여 찾는다.

But, we can also already see that MrBills is not packed and that it has been compiled in MS VC++7.0

그러나, 우리는 이미 볼 수 있다. MrBills 는 pack 되어있지 않고 MS VC++7.0 으로 compile 됐다.

Today's software is MrBills v.2.1.0.1

오늘 software 는 MrBills v.2.1.0.1 이다.



Mmmm, well ok.

We'll see .....

우리는 볼 수 있다.

BTW, we will look into CRC checks in later parts in this series. Just stay tuned :)

우리는 이 series 의 나중에 나오는 part 에서 CRC check 를 볼 수 있다. 돌릴 수 있다. :)

So, here the target is opened in Olly...

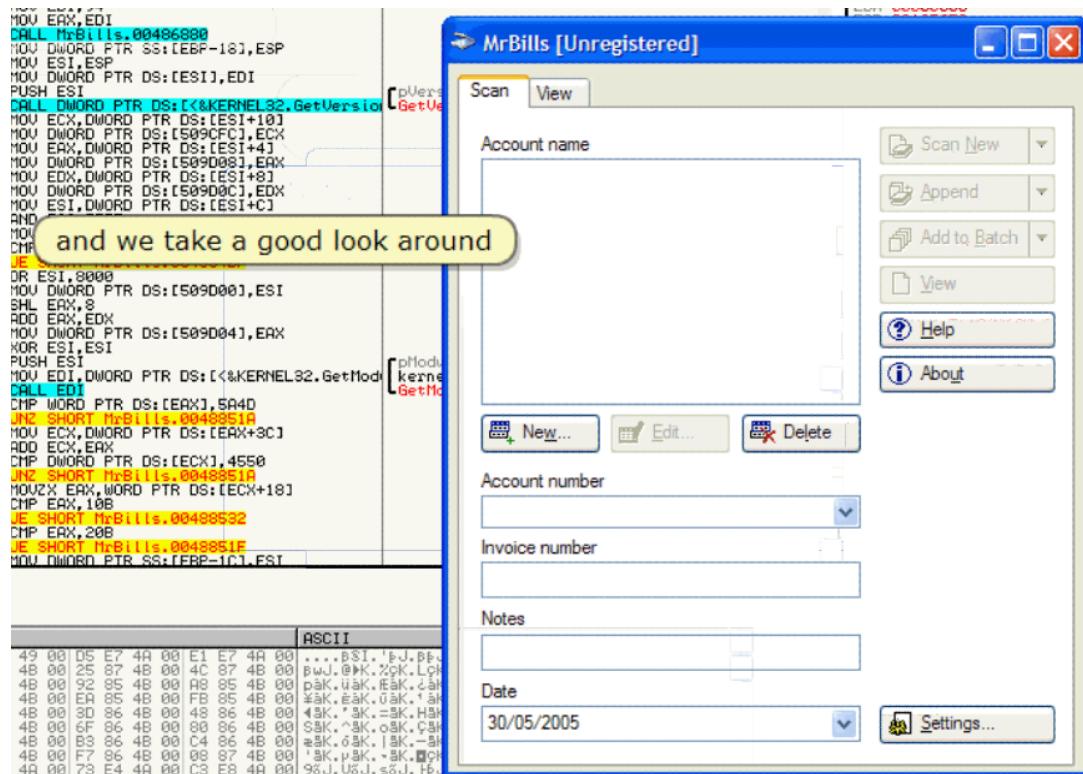
...and let's first explore

So, we run the software...

그래서, 여기 target 을 Olly 에서 열어놨다.

그리고 먼저 탐험하자.

그래서, 우리는 software 를 실행했다.



And we take a good look around

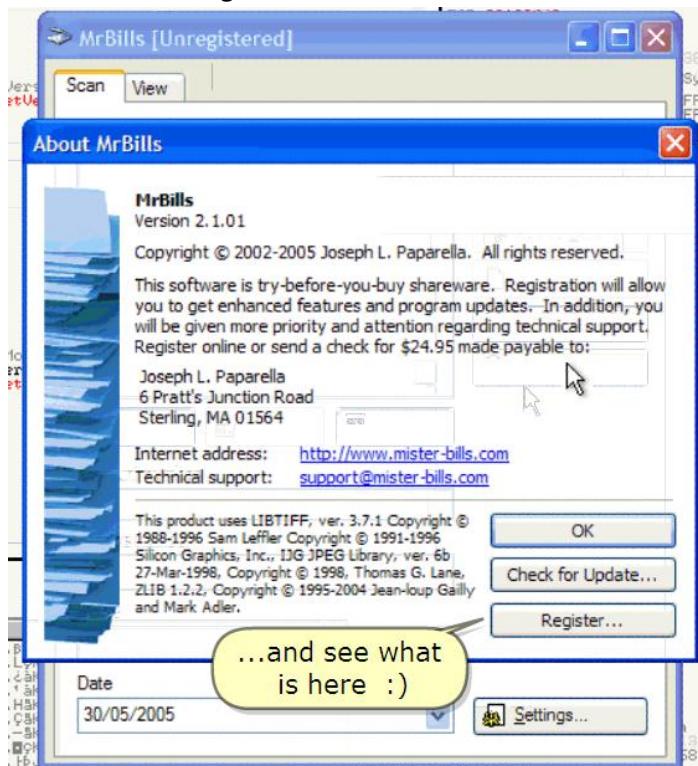
그리고 주변을 살펴봐.



Indeed, we are not registered

정말, 우리는 등록하지 않았다.

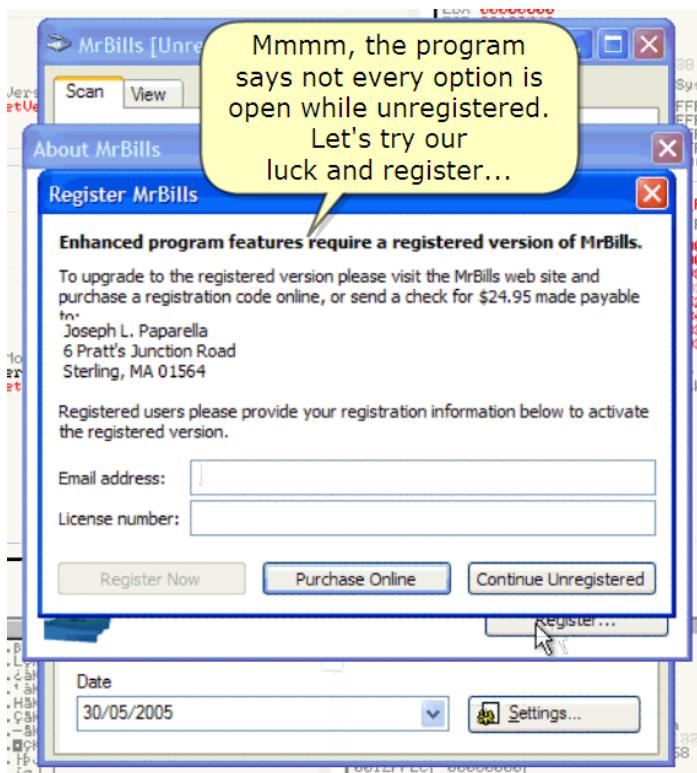
Mmmm, ok, let's go for it



...and see what is here :)

음, 이것을 위해 계속 가자.

그리고 이것이 무엇인지 봐.



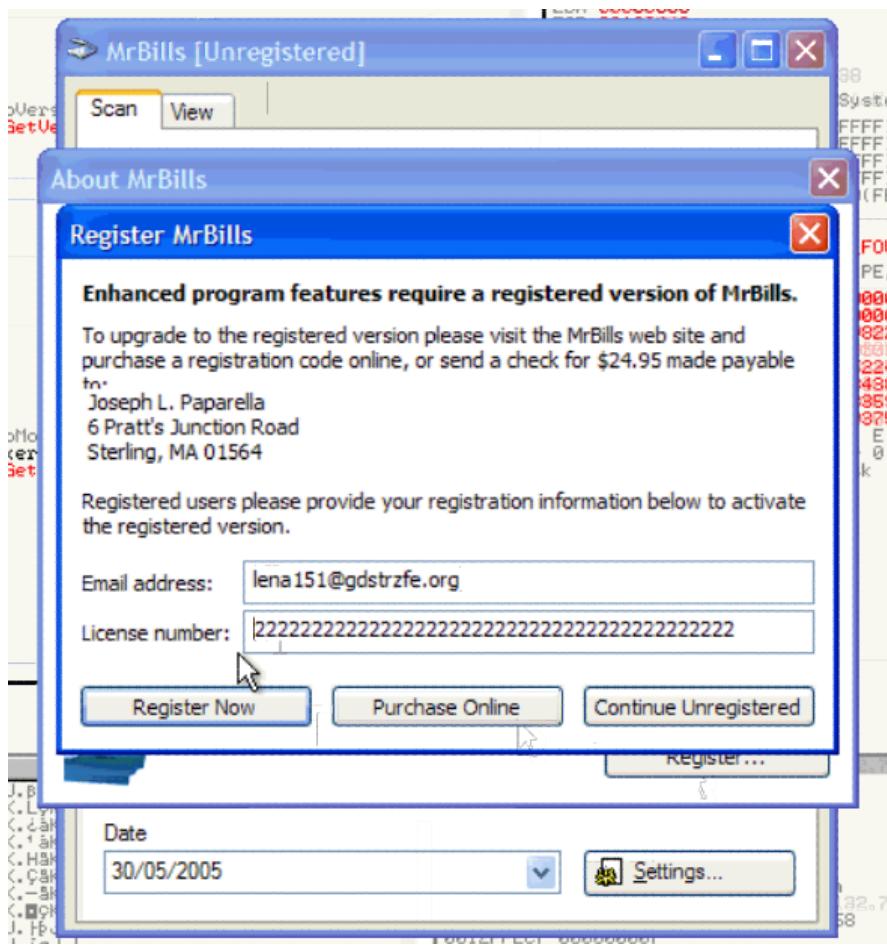
Mmmm, the program says not every option is open while unregistered.

Let's try our luck and register...

음, program 은 등록되지 않았을 때, 모든 option 을 열 수 없다.

우리의 운을 믿고 등록해보자.

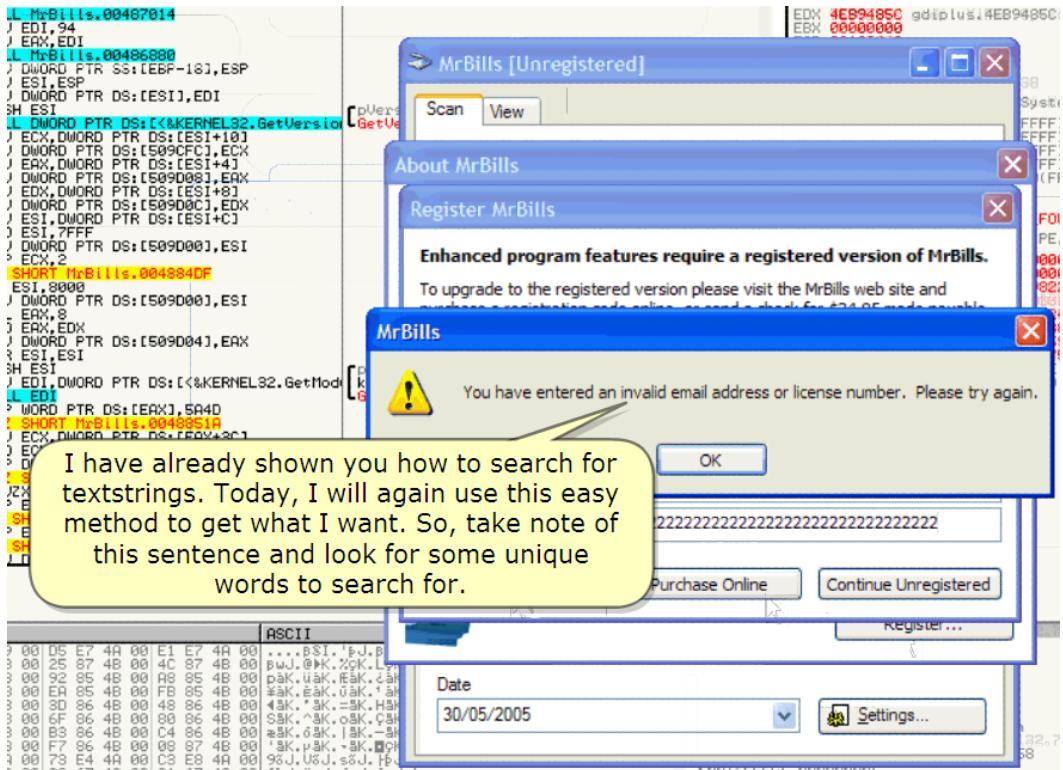
;)



All right. This should give us enough information. Let's go !

좋아. 너에게 충분한 정보를 주었다. 시작하자!

#### 4. Finding the patches



I have already shown you how to search for textstrings.

나는 이미 너에게 어떻게 textstring 을 찾는지 보여주었다.

Today, I will again use this easy method to get what I want.

오늘, 나는 다시 내가 원하는 쉬운 방법을 사용하겠다.

So, take note of this sentence and look for some unique words to search for.

이 문장을 적어 그리고 약간의 유일한 단어들을 찾아라.

Fine, let's study all this better in the code.

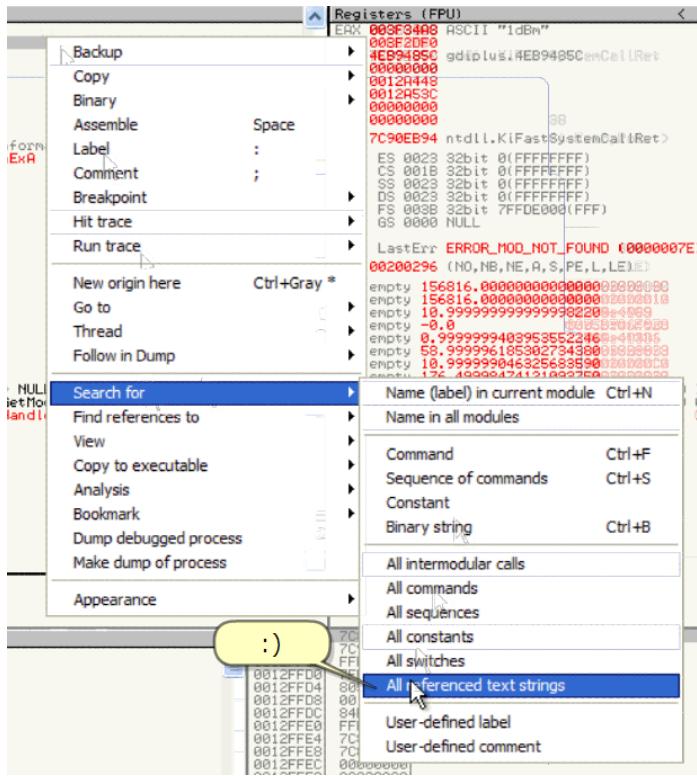
좋아, code 를 공부하자.

Return to Olly

And rightclick

Olly 로 돌아가.

그리고 rightclick



;)

When searching for textstrings, you need to remember to scroll up first.

Textstring 을 찾을 때, 먼저 scroll 을 올린 후에 찾는 기억이 필요하다.

Olly searches top to bottom and we don't want to miss anything. Now rightclick ...

Olly 는 top에서 bottom 까지 찾는다. 그리고 우리는 어떤 실수도 원하는지 않는다. 이제 rightclick...

And search for this textstring. Remember the beginning of the sentence?

그리고 textstring 을 찾아. 문장의 첫번째를 기억하니?

Best is to search case UNsensitive in the entire scope so we don't miss anything again

좋은 것은 모든 범위에서 case 구별없이 검색. 그래서 우리는 어떤 것이라도 빠뜨리지 않는다.

| Address  | Disassembly                              | Text string   |
|----------|--|---|
| 00426A99 | PUSH MrBills..004C079C                   | ASCII "Notes"   |
| 00426AA3 | PUSH MrBills..004C079D                   | ASCII "Notes extension?"  |
| 00426B6A | MOU DWORD PTR DS:[ESI],MrBills..004C0800 | ASCII "#fb"   |
| 00426C40 | PUSH MrBills..004C0898                   | ASCII "Full path to the document"   |
| 00426C67 | PUSH MrBills..004C0888                   | ASCII "Folder of the document"  |
| 00426C81 | PUSH MrBills..004C0859                   | ASCII "File name of the document (no file extension)"   |
| 00426C95 | PUSH MrBills..004C0859                   | ASCII "File extension of the document"  |
| 00426C8C | PUSH MrBills..004C0820                   | ASCII "Account name"  |
| 00426CD6 | PUSH MrBills..004C0810                   | ASCII "Account number"  |
| 00426CF0 | PUSH MrBills..004C0808                   | ASCII "Invoice number"  |
| 00426D0A | PUSH MrBills..004C07F8                   | ASCII "Date"  |
| 00426D1E | PUSH MrBills..004C07F8                   | ASCII "Time"  |
| 00426D51 | PUSH MrBills..004C0834                   | ASCII "%document%"  |
| 00426F24 | PUSH MrBills..004C0884                   | ASCII "%MrBills.log%"   |
| 004272F8 | MOV DWORD PTR DS:[ESI],MrBills..004C0B50 | ASCII "#fb"   |
| 00427797 | MOV DWORD PTR DS:[ESI],MrBills..004C0B50 | ASCII "#fb"   |
| 00427941 | MOV DWORD PTR DS:[ESI],MrBills..004C0B50 | ASCII "#fb..."  |
| 00427945 | PUSH MrBills..004C0BCC                   | ASCII "#fb..."  |
| 004281A3 | PUSH MrBills..004C0D08                   | ASCII "#fb"   |
| 004281E0 | PUSH MrBills..004C0DFC                   | ASCII "   |
| 00428EF1 | PUSH MrBills..004C0FFC                   | ASCII "PropPageFrameEx"   |
| 00429100 | PUSH MrBills..004C1000                   | UNICODE "#fb"   |
| 004291FD | PUSH MrBills..004C1000                   | UNICODE "#fb"   |
| 00429320 | PUSH MrBills..004C100C                   | UNICODE "#fb"   |
| 00429549 | PUSH MrBills..004C100D                   | UNICODE "#fb"   |
| 0042954E | PUSH MrBills..004B9E90                   | ASCII "http://www.mrbills.com/purchase.htm"   |
| 00429551 | PUSH MrBills..004C100B                   | ASCII "og"  |
| 00429598 | PUSH MrBills..004B9C90                   | ASCII " made available to registered version please visit the MrBills web site and purchase a r |
| 0042959C | PUSH MrBills..004B9C90                   | ASCII " Joseph L. Paparella#86 Pratt's Junction Road#Sterling, MA 01564"                        |
| 00429593 | PUSH MrBills..004B9E90                   | ASCII " Registered users please provide your registration information below to activate the reg |
| 00429563 | PUSH MrBills..004C1268                   | ASCII " You have entered an invalid email address or license number. Please try again."         |
| 00429580 | PUSH MrBills..004C1370                   | ASCII " Thank you for registering!"   |
| 00429580 | PUSH MrBills..004C1370                   | ASCII " Registration successful!"   |
| 0042960C | PUSH MrBills..004C1504                   | ASCII " PostBox"  |
| 00429707 | PUSH MrBills..004C14FC                   | ASCII " ToolbarWindow32"  |
| 004297CE | PUSH MrBills..004C1514                   | ASCII " Button"   |
| 004297E9 | PUSH MrBills..004C150C                   | ASCII " Static"   |
| 00429839 | PUSH MrBills..004C1504                   |   |

Found!

Doubleclick to go there

;)

Nice, we have found where the textstring is pushed on the stack. (== where the string is prepared to write it in the messagebox)

좋아, 우리는 textstring 이 stack에 넣어지는 곳을 찾았다. ( == string 은 messagebox에 쓰기 위해 준비됐다.)

Scroll down to get a better look at it

But see already what nice stuff is here

And now have a good look around

좀 더 좋게 보려면 Scroll 내려.

이미 좋은 재료가 여기 있는 것을 봤다.

그리고 이제 주변을 살펴봐.

GoodBoy

BadBoy

```
004299B8 53 PUSH EBX
004299B9 36 JNZ 30
004299B9 30
004299B0 68 70134C00 PUSH 30
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
004299D4 E8 4F7CFDFF CALL MrBills.00401628
004299D9 53 PUSH EBX
004299DA 8BCE MOV ECX,ESI
004299DC E8 D5A60700 CALL MrBills.004A40B6
004299E1 8D8E 7C010000 LEA ECX,DWORD PTR DS:[ESI+17C]
004299E7 E8 83D00700 CALL MrBills.004A6A6F
004299EC E9 29010000 JMP MrBills.00429B1A
004299F1 5A 40 PUSH 40
004299F3 68 00134C00 PUSH MrBills.004C1350
004299F8 E8 3E21 00 CALL MrBills.004AC13B
004299FD
004299FF
00429A01
00429A06
00429A0B
00429A0D
00429A12
00429A14
```

ASCII "You have entered a

ASCII "Thank you for regi

See the JNZ from above landing here to put the goodboy in the messagebox when all requirements are fulfilled

^ 표시는 jump 가 시작하는 곳

> 표시는 jump 가 도착하는 곳

See the JNZ from above landing here to put the goodboy in the messagebox when all requirements are fulfilled

JNZ 를 봐. 위에서 이곳에 도착한다. 모든 요구가 충족됐을 때 Messagebox에 goodboy를 넣는다.

C CPU - main thread, module MrBills

| Address                   | Hex dump        | Disassembly                       | Comment   |
|---------------------------|-----------------|-----------------------------------|---|
| 00429995                  | • 57            | PUSH EDI                          |   |
| 00429996                  | • 6A 01         | PUSH 1                            |   |
| 00429998                  | • 8F81          | MOU ESI,ECX                       |   |
| 0042999A                  | • E8 17A70700   | <b>CALL MrBills.004A40B6</b>      |   |
| 0042999C                  | • 80BE 1C010000 | LEA EDI,DWORD PTR DS:[ESI+11C]    |   |
| 00429995                  | • 80B6 20010000 | LEA EAX,DWORD PTR DS:[ESI+120]    |   |
| 00429998                  | • 57            | PUSH EDI                          |   |
| 004299AC                  | • 50            | PUSH EBX                          |   |
| 004299AD                  | • E8 9AD7FDFF   | <b>CALL MrBills.004A40B6</b>      |   |
| 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         | <b>JNZ SHORT MrBills.004299F1</b> | So, it is this conditional jump that needs to be taken to jump to the goodboy !!! |
| 004299B8                  | • 6A 90         | PUSH 30                           |   |
| 004299BD                  | • 68 70134C00   | PUSH MrBills.004C1370             |   |
| 004299C2                  | • E8 74270800   | <b>CALL MrBills.004AC13B</b>      |   |
| 004299C7                  | • 80BE 20010000 | LEA ECX,DWORD PTR DS:[ESI+120]    |   |
| 004299CD                  | • E8 567CFDFF   | <b>CALL MrBills.00401628</b>      |   |
| 004299D2                  | • 88CF          | MOU ECX,EDI                       |   |
| 004299D4                  | • E8 4F7CFDFF   | <b>CALL MrBills.00401628</b>      |   |
| 004299D9                  | • 53            | PUSH EBX                          |   |
| 004299DA                  | • 88CE          | MOU ECX,ESI                       |   |
| 004299DC                  | • E8 D5A60700   | <b>CALL MrBills.004A40B6</b>      |   |
| 004299E1                  | • 80BE 7C010000 | LEA ECX,DWORD PTR DS:[ESI+17C]    |   |
| 004299E7                  | • E8 83D00700   | <b>CALL MrBills.004A6A6F</b>      |   |
| 004299EC                  | • >E9 29810000  | <b>JMP MrBills.0042981A</b>       |   |
| 004299F1                  | • 6A 40         | PUSH 40                           |   |
| 004299F3                  | • 68 50134C00   | PUSH MrBills.004C1350             |   |
| 004299F8                  | • E8 8E270800   | <b>CALL MrBills.004AC13B</b>      |   |
| 004299FD                  | • 6A 01         | PUSH 1                            |   |
| 004299FF                  | • 88CE          | MOU ECX,ESI                       |   |
| 00429901                  | • E8 2F8E0700   | <b>CALL MrBills.004A2835</b>      |   |
| 00429906                  | • E8 C1E9FDFF   | <b>CALL MrBills.0040083C0</b>     |   |
| 00429908                  | • 88F0          | MOU ESI,EAX                       |   |
| 004299D0                  | • E8 C8DB0700   | <b>CALL MrBills.004A75D0</b>      |   |
| 00429912                  | • 8819          | MOU EDX,DWORD PTR DS:[EAX]        |   |
| 00429914                  | • 88C8          | MOU ECX,EAX                       |   |
| 00429916                  | • FF52 0C       | <b>CALL DWORD PTR DS:[EDX+C]</b>  |   |
| 00429919                  | • 89C0 10       | ADD EAX,10                        |   |
| 0042991C                  | • 8945 F0       | MOU DWORD PTR SS:[EBP-10],EAX     |   |
| 0042991F                  | • 8945 FA       | MOU ECX,DWORD PTR SS:[EFP-10]     |   |
| 004299F1=MrBills.004299F1 |                 |                                   |   |

So, it is this conditional jump that needs to be taken to jump to the goodboy !!!

그래서, 이것은 조건 jump 다. Goodboy로 jump 하는 것이 필요하다.

This TEST AL, AL is classic

TEST AL, AL은 classic 하다.

;))

AL will decide about GoodBoy or Badboy

AL이 Goodboy인지 Badboy인지에 대하여 결정할 수 있다.

C CPU - main thread, module MrBills

| Address                   | Hex dump        | Disassembly                       | Comment                             |
|---------------------------|-----------------|-----------------------------------|-------------------------------------|
| 00429995                  | • 57            | PUSH EDI                          |                                     |
| 00429996                  | • 6A 01         | PUSH 1                            |                                     |
| 00429998                  | • 8F81          | MOU ESI,ECX                       |                                     |
| 0042999A                  | • E8 17A70700   | <b>CALL MrBills.004A40B6</b>      |                                     |
| 0042999C                  | • 80BE 1C010000 | LEA EDI,DWORD PTR DS:[ESI+11C]    |                                     |
| 00429995                  | • 80B6 20010000 | LEA EAX,DWORD PTR DS:[ESI+120]    |                                     |
| 00429998                  | • 57            | PUSH EDI                          |                                     |
| 004299AC                  | • 50            | PUSH EBX                          |                                     |
| 004299AD                  | • E8 9AD7FDFF   | <b>CALL MrBills.004A40B6</b>      |                                     |
| 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         | <b>JNZ SHORT MrBills.004299F1</b> | and AL is probably set in this call |
| 004299B8                  | • 6A 90         | PUSH 30                           |                                     |
| 004299BD                  | • 68 70134C00   | PUSH MrBills.004C1370             |                                     |
| 004299C2                  | • E8 74270800   | <b>CALL MrBills.004AC13B</b>      |                                     |
| 004299C7                  | • 80BE 20010000 | LEA ECX,DWORD PTR DS:[ESI+120]    |                                     |
| 004299CD                  | • E8 567CFDFF   | <b>CALL MrBills.00401628</b>      |                                     |
| 004299D2                  | • 88CF          | MOU ECX,EDI                       |                                     |
| 004299D4                  | • E8 4F7CFDFF   | <b>CALL MrBills.00401628</b>      |                                     |
| 004299D9                  | • 53            | PUSH EBX                          |                                     |
| 004299DA                  | • 88CE          | MOU ECX,ESI                       |                                     |
| 004299DC                  | • E8 D5A60700   | <b>CALL MrBills.004A40B6</b>      |                                     |
| 004299E1                  | • 80BE 7C010000 | LEA ECX,DWORD PTR DS:[ESI+17C]    |                                     |
| 004299E7                  | • E8 83D00700   | <b>CALL MrBills.004A6A6F</b>      |                                     |
| 004299EC                  | • >E9 29810000  | <b>JMP MrBills.0042981A</b>       |                                     |
| 004299F1                  | • 6A 40         | PUSH 40                           |                                     |
| 004299F3                  | • 68 50134C00   | PUSH MrBills.004C1350             |                                     |
| 004299F8                  | • E8 8E270800   | <b>CALL MrBills.004AC13B</b>      |                                     |
| 004299FD                  | • 6A 01         | PUSH 1                            |                                     |
| 004299FF                  | • 88CE          | MOU ECX,ESI                       |                                     |
| 00429901                  | • E8 2F8E0700   | <b>CALL MrBills.004A2835</b>      |                                     |
| 00429906                  | • E8 C1E9FDFF   | <b>CALL MrBills.0040083C0</b>     |                                     |
| 00429908                  | • 88F0          | MOU ESI,EAX                       |                                     |
| 004299D0                  | • E8 C8DB0700   | <b>CALL MrBills.004A75D0</b>      |                                     |
| 00429912                  | • 8819          | MOU EDX,DWORD PTR DS:[EAX]        |                                     |
| 00429914                  | • 88C8          | MOU ECX,EAX                       |                                     |
| 00429916                  | • FF52 0C       | <b>CALL DWORD PTR DS:[EDX+C]</b>  |                                     |
| 00429919                  | • 89C0 10       | ADD EAX,10                        |                                     |
| 0042991C                  | • 8945 F0       | MOU DWORD PTR SS:[EBP-10],EAX     |                                     |
| 0042991F                  | • 8945 FA       | MOU ECX,DWORD PTR SS:[EFP-10]     |                                     |
| 004299F1=MrBills.004299F1 |                 |                                   |                                     |

And AL is probably set in this call

AL은 아마 이 call에서 set 된다.

The screenshot shows the CPU pane of Immunity Debugger with the title "CPU - main thread, module MrBills". The assembly code is as follows:

```
00429995 . 57 PUSH EDI
00429996 . 6A 01 PUSH 1
00429998 . 8BF1 MOV ESI,ECX
0042999A . E8 17A70700 CALL MrBills.004A40B6
0042999F . 8DDE 1C010000 LEA EDI,DWORD PTR DS:[ESI+1]
004299A5 . 8D86 20010000 LEA EBX,DWORD PTR DS:[ESI+1]
004299A8 . 57 PUSH EDI
004299AC . 50 PUSH EAX
004299AD . E8 9AD7FDFF CALL MrBills.0040714C
004299E2 . 59 POP ECX
004299E3 . 33DB XOR EBX,EBX
004299E5 . 84C0 TEST AL,AL
004299E8 . 59 POP ECX
004299E9 . 53 PUSH EBX
004299E9 . 75 36 JNZ SHORT MrBills.004299F1
004299EB . 6A 30 PUSH 30
004299E9 . 63 78134C00 PUSH MrBills.004C1370
004299C2 . E8 74270800 LEA ECX,DWORD PTR DS:[ESI+120]
004299C7 . 8D8E 20010000 CALL MrBills.00401628
004299CD . E8 567CFDFF MOU ECX,EDI
004299D2 . 8BCF CALL MrBills.00401628
004299D4 . E8 4F7CFDFF PUSH EBX
004299D9 . 53 MOU ECX,ESI
004299CA . 88CE CALL MrBills.004A40B6
004299C3 . E8 D5A60700 LEA ECX,DWORD PTR DS:[ESI+17C]
004299E1 . 8D8E 7C010000 CALL MrBills.004A6A6F
004299E7 . E8 83D00700 JMP MrBills.0042991A
004299EC . E8 29010000 PUSH 40
004299F1 > 6A 40 PUSH MrBills.004C1350
004299F3 . 68 58134C00 CALL MrBills.004AC13B
004299F8 . E8 3E270800 PUSH 1
004299F9 . 6A 01 MOU ECX,ESI
004299FF . 88C8 CALL MrBills.004A2835
00429A01 . E8 2F8E0700 CALL MrBills.004083C0
00429A06 . E8 C1E9FDFF MOU ESI,EAX
00429A0B . 88F0 CALL MrBills.004A75D0
00429A0D . E8 C8D80700 MOU EDX,DWORD PTR DS:[EAX]
00429A12 . 8810 MOU ECX,EAX
00429A14 . 88C8 CALL DWORD PTR DS:[EDX+C0]
00429A16 . FF52 0C ADD ERX,10
00429A19 . 89C0 10 MOU DWORD PTR SS:[EBP-10],EAX
00429A1C . 8945 F0 LEA EBX,DWORD PTR SS:[EBP-10]
00429A1E . 8045 FB
```

A yellow callout box highlights the instruction `JNZ SHORT MrBills.004299F1`. The text inside the callout box reads:

Because that is even more classic : in the call just before the compare(test) is almost always the setting for the compare (test). This is the verification for the registration. There can only be one conclusion : we need to investigate in this call what sets AL.

ASCII "You have entered an invalid email add:"

ASCII "Thank you for registering!"

Because that is even more classic : in the call just before the compare(test) is almost always the setting for the compare (test).

그것은 훨씬 더 classic 하다. : 이 call에서 AL이 set 되고 compare(test) 된다.

This is the verification for the registration.

등록하기 위해 검증한다.

There can only be one conclusion : we need to investigate in this call what sets AL.

오직 한 가지 결론 : 우리는 이 call의 어느 곳에서 AL이 set 되는지 조사할 필요가 있다.

So, put a BP here(doubleclick opcode)

그래서, BP를 여기에 설정 해(doubleclick opcode)

Let's resume.

We have found the result for the verification "was the serial correct or not ?"

That result is held in AL

계속하자.

우리는 검증하기 위한 결과를 찾았다. "serial 이 정확하냐 아니냐?"

result 는 AL 에서 결정됩니다.

While that result was set in the call above the test al, al

그 result 는 이 call 에서 test al, al 의 위에서 set 됐다.

If the result is a positive verification

만약에 result 가 긍정적인 검증을 하게 되면

Then we jump to the goodboy to register the application

우리는 application 에 등록하기 위해 goodboy 로 jump 한다.

Else, we don't jump and get the badboy message

아니라면, 우리는 jump 하지 않는다. 그리고 badboy message 를 얻는다.

### Conclusion:

Because of the JNZ AL must be different from zero when arriving here to be registered

결론 ·

JNZ. 둘째된 곳에 도착하기 위해 AI 은 zero 와 달라야 한다.

번역 주) test al, al에 도착했을 때 al이 0이 아니어야 JNZ에서 goodboy로 jump 한다. Test 연산은 and 연산의 데 결과값을 저장하지 않는 assembly다.

Now, what is before all this?

이제, 이것 다음에 무엇이야?

Okay, only the strings for the About box

They are not important for us here.

Okay, 오직 About box 를 위한 strings 이다.

그들은 현재 우리에게 중요하지 않다.

Let's re-run registration

등록하기 위해 재시작 하자.

To break in the breakpoint and see what is in the call

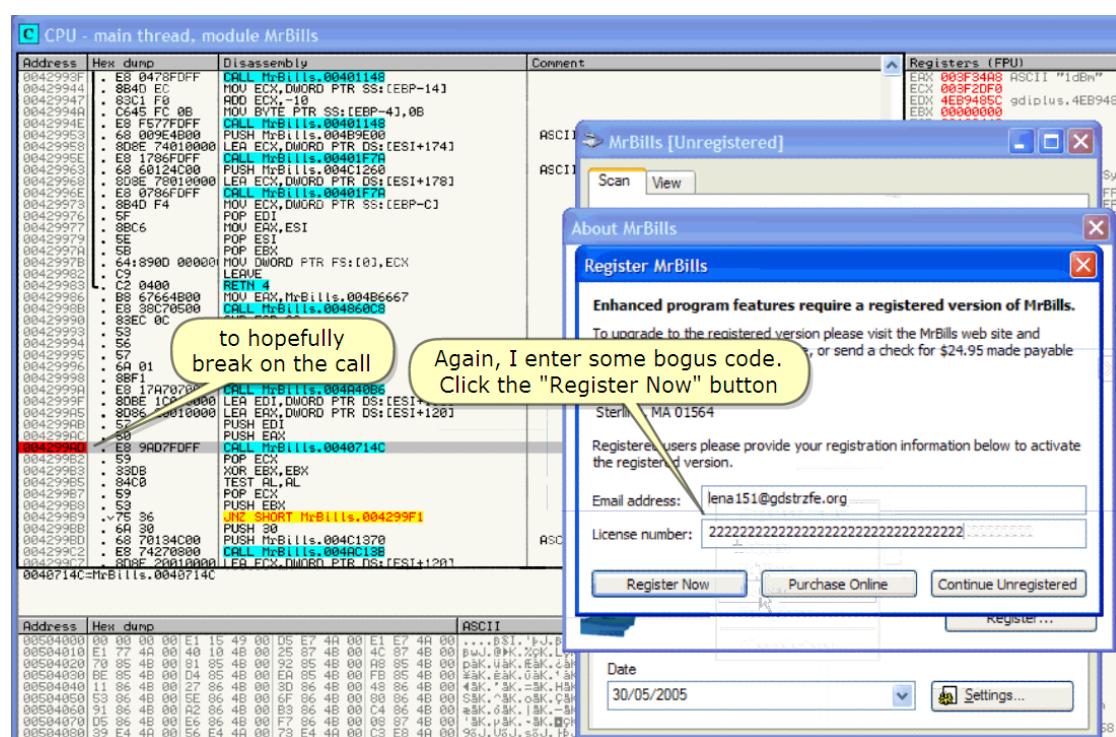
Breakpoint에서 멈추자. 그리고 call 안에 무엇이 있는지 보자.

Resume : the plain stupid patching method would only patch conditional jumps to jump the badboy(s). Mostly, this doesn't suffice to also register an application.

재개 : 분명히 명청한 patching 방법은 오직 badboy 로 조건 jump 를 한다. 대부분, application 에 등록하기 위해 충분하지 않다.

So, today, we will go dig deeper in the call that sets the deciding register (here AL) to patch the setting itself into "registered".

그래서, 오늘, 우리는 call 안으로 깊게 파 보겠다. 결정하는 Register 를 patch 해서 등록하기 위해 Set 한다.



Again, I enter some bogus code.

Click the "Register Now" button

To hopefully break on the call

다시, 가짜의 code 에 들어간다.

"Register Now" button 을 click 해.

여기에서 멈추기를 바란다.

Great!

We land on the call.

Press F7 to step into

좋아!

우리는 call 에 도착했다.

F7 을 눌러 step 안으로 들어가자.

We land here in the call

Step with F8 now to take an overview of what's all happening

우리는 call 안에 도착했다.

F8 을 눌러. 어떤 일이 일어나는지 관점을 가져.

And I think it's clear we need to keep an eye on the value for AL

그리고 이것이 명확하다. 우리는 AL value 을 유지하기 위해 필요하다.

| Address  | Hex dump         | Disassembly                        |
|----------|------------------|------------------------------------|
| 0040714C | \$ 55            | PUSH EBP                           |
| 0040714D | . 8BED           | MOV EBP,ESP                        |
| 0040714F | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]          |
| 00407152 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]          |
| 00407155 | . E8 77FEFFFF    | CALL MrBills.00406FD1              |
| 0040715A | 84C0             | TEST AL,AL                         |
| 0040715C | . 59             | POP ECX                            |
| 0040715D | . 59             | POP ECX                            |
| 0040715E | . A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL        |
| 00407163 | > 75 1B          | JNZ SHORT MrBills.00407130         |
| 00407165 | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]          |
| 00407168 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]          |
| 0040716B | . E8 ADFFFFFF    | CALL MrBills.00407010              |
| 00407170 | 84C0             | TEST AL,AL                         |
| 00407172 | . 59             | POP ECX                            |
| 00407173 | . 59             | POP ECX                            |
| 00407174 | . A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL        |
| 00407179 | . A2 A2765000    | MOV BYTE PTR DS:[5076A2],AL        |
| 0040717E | > 74 0D          | JE SHORT MrBills.00407130          |
| 00407180 | > FF75 0C        | PUSH DWORD PTR SS:[EBP+C]          |
| 00407183 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]          |
| 00407186 | . E8 45F8FFFF    | CALL MrBills.00406900              |
| 0040718B | 59               | POP ECX                            |
| 0040718C | 59               | POP ECX                            |
| 0040718D | > SD             | POP EBP                            |
| 0040718E | ^E9 D6FFFFFF     | JMP MrBills.00407069               |
| 00407193 | \$ 56            | PUSH ESI                           |
| 00407194 | . FF7424 08      | PUSH DWORD PTR SS:[ESP+8]          |
| 00407198 | . 8BF1           | MOU ESI,ECX                        |
| 0040719A | . 8366 04 00     | AND DWORD PTR DS:[ESI+4],0         |
| 0040719E | . C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1         |
| 004071A5 | . E8 B6E30800    | CALL MrBills.00495560              |
| 004071AA | . 8906           | MOV DWORD PTR DS:[ESI],EAX         |
| 004071AC | . 8BC6           | MOU EAX,ESI                        |
| 004071AE | . 5E             | POP ESI                            |
| 004071AF | . C2 0400        | RETN 4                             |
| 004071B2 | \$ 56            | PUSH ESI                           |
| 004071B3 | . FF7424 08      | PUSH DWORD PTR SS:[ESP+8]          |
| 004071B7 | . 8BF1           | MOU ESI,ECX                        |
| 004071B9 | . 8366 04 00     | AND DWORD PTR DS:[ESI+4],0         |
| 004071BD | . C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1         |
| 004071C4 | . FF15 40944B00  | CALL DWORD PTR DS:[<&OLEAUT32.#2>] |
| 004071C9 | 85C0             | TEST FOX,FOX                       |

**C CPU - main thread, module MrBills**

| Address  | Hex dump         | Disassembly                      | Comments |
|----------|------------------|----------------------------------|----------|
| 0040714C | \$ 55            | PUSH EBP                         |          |
| 0040714D | . 8BED           | MOV EBP,ESP                      |          |
| 0040714F | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |          |
| 00407152 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |          |
| 00407155 | . E8 77FEFFFF    | CALL MrBills.00406FD1            | Mmmmm    |
| 0040715A | . 84C0           | TEST AL,AL                       |          |
| 0040715C | . 59             | POP ECX                          |          |
| 0040715D | . 59             | POP ECX                          |          |
| 0040715E | . A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL      |          |
| 00407163 | . ^75 1B         | JNZ SHORT MrBills.00407180       |          |
| 00407165 | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |          |
| 00407168 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |          |
| 0040716B | . E8 ADFFFFFF    | CALL MrBills.00407010            |          |
| 00407170 | . 84C0           | TEST AL,AL                       |          |
| 00407172 | . 59             | POP ECX                          |          |
| 00407173 | . 59             | POP ECX                          |          |
| 00407174 | . A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL      |          |
| 00407179 | . A2 A2765000    | MOV BYTE PTR DS:[5076A2],AL      |          |
| 0040717E | . ^74 0D         | JE SHORT MrBills.00407180        |          |
| 00407180 | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |          |
| 00407183 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |          |
| 00407186 | . E8 45F8FFFF    | CALL MrBills.00406900            |          |
| 00407188 | . 59             | POP ECX                          |          |
| 0040718D | . > SD           | POP EBP                          |          |
| 0040718E | . ^E9 D6FEFFFF   | JMP MrBills.00407069             |          |
| 00407193 | . ^56            | PUSH ESI                         |          |
| 00407194 | . FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |          |
| 00407198 | . 8BF1           | MOV ESI,ECX                      |          |
| 0040719A | . 8BC6           | MOU EAX,ESI                      |          |
| 0040719C | . SE             | POP ESI                          |          |
| 0040719F | . C2 0400        | RETN 4                           |          |
| 004071A2 | . ^56            | PUSH ESI                         |          |
| 004071A3 | . FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |          |
| 004071A7 | . 8BF1           | MOV ESI,ECX                      |          |
| 004071A9 | . 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |          |
| 004071AC | . C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1       |          |
| 004071BD | . FF15 40944B00  | CALL DWORD PTR DS:[&OLEAUT32.#2] | OLERI    |
| 004071C0 | . 85C0           | TEST FAX,FAX                     |          |

**C CPU - main thread, module MrBills**

| Address  | Hex dump         | Disassembly                      | Comments |
|----------|------------------|----------------------------------|----------|
| 0040714C | \$ 55            | PUSH EBP                         |          |
| 0040714D | . 8BED           | MOV EBP,ESP                      |          |
| 0040714F | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |          |
| 00407152 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |          |
| 00407155 | . E8 77FEFFFF    | CALL MrBills.00406FD1            |          |
| 0040715A | . 84C0           | TEST AL,AL                       |          |
| 0040715C | . 59             | POP ECX                          |          |
| 0040715D | . 59             | POP ECX                          |          |
| 0040715E | . A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL      |          |
| 00407163 | . ^75 1B         | JNZ SHORT MrBills.00407180       | notice   |
| 00407165 | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |          |
| 00407168 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |          |
| 0040716B | . E8 ADFFFFFF    | CALL MrBills.00407010            |          |
| 00407170 | . 84C0           | TEST AL,AL                       |          |
| 00407172 | . 59             | POP ECX                          |          |
| 00407173 | . 59             | POP ECX                          |          |
| 00407174 | . A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL      |          |
| 00407179 | . A2 A2765000    | MOV BYTE PTR DS:[5076A2],AL      |          |
| 0040717E | . ^74 0D         | JE SHORT MrBills.00407180        |          |
| 00407180 | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |          |
| 00407183 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |          |
| 00407186 | . E8 45F8FFFF    | CALL MrBills.00406900            |          |
| 00407188 | . 59             | POP ECX                          |          |
| 0040718D | . 59             | POP ECX                          |          |
| 0040718E | . > SD           | POP EBP                          |          |
| 0040718F | . ^E9 D6FEFFFF   | JMP MrBills.00407069             |          |
| 00407193 | . ^56            | PUSH ESI                         |          |
| 00407194 | . FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |          |
| 00407198 | . 8BF1           | MOV ESI,ECX                      |          |
| 0040719A | . 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |          |
| 0040719C | . C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1       |          |
| 0040719D | . E8 B6E308000   | CALL MrBills.00495560            |          |
| 004071AC | . 8906           | MOU DWORD PTR DS:[ESI],EAX       |          |
| 0040719C | . 8BC6           | MOU EAX,ESI                      |          |
| 0040719E | . SE             | POP ESI                          |          |
| 0040719F | . C2 0400        | RETN 4                           |          |
| 004071A2 | . ^56            | PUSH ESI                         |          |
| 004071A3 | . FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |          |
| 004071A7 | . 8BF1           | MOV ESI,ECX                      |          |
| 004071A9 | . 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |          |
| 004071AC | . C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1       |          |
| 004071BD | . FF15 40944B00  | CALL DWORD PTR DS:[&OLEAUT32.#2] |          |
| 004071C0 | . 85C0           | TEST FAX,FAX                     |          |

| Address  | Hex dump       | Disassembly                      |
|----------|----------------|----------------------------------|
| 0040714C | 55             | PUSH EBP                         |
| 0040714D | 8BED           | MOV EBP,ESP                      |
| 0040714F | FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |
| 00407150 | FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |
| 00407152 | E8 77FFFFFF    | CALL MrBills.00406FD1            |
| 00407155 | 34C0           | TEST AL,AL                       |
| 0040715A | 59             | POP ECX                          |
| 0040715C | 59             | POP ECX                          |
| 0040715D | A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL      |
| 00407163 | 75 1B          | JNZ SHORT MrBills.00407180       |
| 00407165 | FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |
| 00407168 | FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |
| 0040716B | E8 ADFFFFFF    | CALL MrBills.0040701D            |
| 00407170 | 84C0           | TEST AL,AL                       |
| 00407172 | 59             | POP ECX                          |
| 00407173 | 59             | POP ECX                          |
| 00407174 | A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL      |
| 00407179 | A2 A2765000    | MOV BYTE PTR DS:[5076A2],AL      |
| 0040717E | 74 00          | JE SHORT MrBills.00407180        |
| 00407180 | FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |
| 00407183 | FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |
| 00407186 | E8 45F8FFFF    | CALL MrBills.00406900            |
| 00407188 | 59             | POP ECX                          |
| 0040718C | 59             | POP ECX                          |
| 0040718D | > SD           | POP EBP                          |
| 0040718E | ^E9 D6FFFFFF   | JMP MrBills.00407069             |
| 00407193 | 56             | PUSH ESI                         |
| 00407194 | FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |
| 00407198 | 8BF1           | MOV ESI,ECX                      |
| 0040719A | 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |
| 0040719E | C746 08 010000 | MOV DWORD PTR DS:[ESI+8],1       |
| 004071A5 | E8 B6E30800    | CALL MrBills.004095560           |
| 004071AC | 8906           | MOV DWORD PTR DS:[ESI],EAX       |
| 004071AE | 8BC6           | MOV EAX,ESI                      |
| 004071AF | SE             | POP ESI                          |
| 004071B0 | C2 0400        | RETN 4                           |
| 004071B2 | 56             | PUSH ESI                         |
| 004071B3 | FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |
| 004071B7 | 8BF1           | MOV ESI,ECX                      |
| 004071B9 | 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |
| 004071BD | C746 08 010000 | MOV DWORD PTR DS:[ESI+8],1       |
| 004071C4 | FF15 40944B00  | CALL DWORD PTR DS:[&OLEAUT32.#2] |
| 004071C9 | 85C0           | TEST FAX,FBX                     |

| Address  | Hex dump       | Disassembly                      | Comment |
|----------|----------------|----------------------------------|---------|
| 0040714C | 55             | PUSH EBP                         |         |
| 0040714D | 8BED           | MOV EBP,ESP                      |         |
| 0040714F | FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |         |
| 00407150 | FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |         |
| 00407152 | E8 77FFFFFF    | CALL MrBills.00406FD1            |         |
| 00407155 | 34C0           | TEST AL,AL                       |         |
| 0040715A | 59             | POP ECX                          |         |
| 0040715C | 59             | POP ECX                          |         |
| 0040715D | A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL      |         |
| 00407163 | 75 1B          | JNZ SHORT MrBills.00407180       |         |
| 00407165 | FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |         |
| 00407168 | FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |         |
| 0040716B | E8 ADFFFFFF    | CALL MrBills.0040701D            |         |
| 00407170 | 84C0           | TEST AL,AL                       |         |
| 00407172 | 59             | POP ECX                          |         |
| 00407173 | 59             | POP ECX                          |         |
| 00407174 | A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL      |         |
| 00407179 | A2 A2765000    | MOV BYTE PTR DS:[5076A2],AL      |         |
| 0040717E | 74 00          | JE SHORT MrBills.00407180        |         |
| 00407180 | FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |         |
| 00407183 | FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |         |
| 00407186 | E8 45F8FFFF    | CALL MrBills.00406900            |         |
| 00407188 | 59             | POP ECX                          |         |
| 0040718C | 59             | POP ECX                          |         |
| 0040718D | > SD           | POP EBP                          |         |
| 0040718E | ^E9 D6FFFFFF   | JMP MrBills.00407069             |         |
| 00407193 | 56             | PUSH ESI                         |         |
| 00407194 | FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |         |
| 00407198 | 8BF1           | MOV ESI,ECX                      |         |
| 0040719A | 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |         |
| 0040719E | C746 08 010000 | MOV DWORD PTR DS:[ESI+8],1       |         |
| 004071A5 | E8 B6E30800    | CALL MrBills.004095560           |         |
| 004071AC | 8906           | MOV DWORD PTR DS:[ESI],EAX       |         |
| 004071AE | 8BC6           | MOV EAX,ESI                      |         |
| 004071AF | SE             | POP ESI                          |         |
| 004071B0 | C2 0400        | RETN 4                           |         |
| 004071B2 | 56             | PUSH ESI                         |         |
| 004071B3 | FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |         |
| 004071B7 | 8BF1           | MOV ESI,ECX                      |         |
| 004071B9 | 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |         |
| 004071BD | C746 08 010000 | MOV DWORD PTR DS:[ESI+8],1       |         |
| 004071C4 | FF15 40944B00  | CALL DWORD PTR DS:[&OLEAUT32.#2] | OLEAUT3 |
| 004071C9 | 85C0           | TEST FAX,FBX                     |         |

| Address  | Hex dump         | Disassembly                        | Comment |
|----------|------------------|------------------------------------|---------|
| 0040714C | \$ 55            | PUSH EBP                           |         |
| 0040714D | . 8BED           | MOU EFP,ESP                        |         |
| 0040714F | . FF75 0C        | PUSH DMORD PTR SS:[EBP+C]          |         |
| 00407150 | . FF75 08        | PUSH DMORD PTR SS:[EBP+8]          |         |
| 00407152 | . E8 77FEFFFF    | CALL MrBills.00406FD1              |         |
| 00407155 | . 84C8           | TEST AL,AL                         |         |
| 00407156 | . S9             | POP ECX                            |         |
| 0040715D | . S9             | POP ECX                            |         |
| 0040715E | . A2 A0765000    | MOU BYTE PTR DS:[5076A0],AL        |         |
| 00407163 | .~75 1B          | JNZ SHORT MrBills.00407180         |         |
| 00407165 | . FF75 0C        | PUSH DMORD PTR SS:[EBP+C]          |         |
| 00407168 | . FF75 08        | PUSH DMORD PTR SS:[EBP+8]          |         |
| 0040716B | . E8 ADFFFFFF    | CALL MrBills.00407010              |         |
| 00407170 | . 84C8           | TEST AL,AL                         |         |
| 00407172 | . S9             | POP ECX                            |         |
| 00407173 | . S9             | POP ECX                            |         |
| 00407174 | . A2 A0765000    | MOU BYTE PTR DS:[5076A0],AL        |         |
| 00407179 | . A2 A2765000    | MOU BYTE PTR DS:[5476A2],AL        |         |
| 0040717E | .~74 0D          | JE SHORT MrBills.00407180          |         |
| 00407190 | > FF75 0C        | PUSH DMORD PTR SS:[EBP+C]          |         |
| 00407193 | > FF75 08        | PUSH DMORD PTR SS:[EBP+8]          |         |
| 00407196 | > E8 45F8FFFF    | CALL MrBills.00406900              |         |
| 00407198 | . S9             | POP ECX                            |         |
| 0040719C | . S9             | POP ECX                            |         |
| 0040719D | > S0             | POP EBP                            |         |
| 0040719E | ^E9 D6FEFFFF     | JMP MrBills.00407069               |         |
| 00407199 | ^ 56             | PUSH ESI                           |         |
| 0040719A | . FF7424 08      | PUSH DMORD PTR SS:[ESP+8]          |         |
| 0040719B | . 8BF1           | MOU ESI,ECX                        |         |
| 0040719C | . 8366 04 00     | AND DWORD PTR DS:[ESI+4],0         |         |
| 0040719D | . C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1         |         |
| 0040719E | . E8 B6E30800    | CALL MrBills.00495560              |         |
| 0040719F | . 8906           | MOU DWORD PTR DS:[ESI],EAX         |         |
| 004071AC | . 8BC6           | MOU EAX,ESI                        |         |
| 004071AE | . SE             | POP ESI                            |         |
| 004071AF | C2 0400          | RETN 4                             |         |
| 004071B2 | ^ 56             | PUSH ESI                           |         |
| 004071B3 | . FF7424 08      | PUSH DMORD PTR SS:[ESP+8]          |         |
| 004071B7 | . 8BF1           | MOU ESI,ECX                        |         |
| 004071B9 | . 8366 04 00     | AND DWORD PTR DS:[ESI+4],0         |         |
| 004071BD | . C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1         |         |
| 004071C4 | . FF1E 40944B00  | CALL DMORD PTR DS:[<&OLEAUT32.#2>] |         |
| 004071CD | . 85C0           | TEST EBX,EBX                       |         |

Look carefully.  
Do you see what I see ???

But soon we see important stuff

Notice

Mmmmm

Notice

Notice

Notice

Look carefully.

Do you see what I see ???

그러나 우리는 곧 중요한 재료를 본다.

내가 무엇을 봤는지 봐어 ???

It seems ...

AL is already set in this call

AL 은 이미 이 call 에서 set 됐다.

So, let's enter the call to see what it has to offer (push <enter>)

Code 안으로 (PUSH <enter>)를 누가 제공하는지 보기 위해 들어가자.

BTW, when pressing <enter> you can follow the code without effectively executing the code.

<enter>를 누를 때, 효과적인 실행 code 가 없이 code 를 따라갈 수 있다.

So, we go now see the code in the call without executing it

그래서, 우리는 그것을 실행하지 않고 code 를 보기 위해 call 안으로 들어간다.

Mmmm, let's see ....

Study the code here

음, 보자....

Code 를 공부하자.

C CPU - main thread, module MrBills

| Address  | Hex dump         | Disassembly                   |
|----------|------------------|-------------------------------|
| 00406FD1 | # B8 AB374B00    | MOU EAX,MrBills.004B37AB      |
| 00406FD6 | . E8 EDF00700    | <b>CALL MrBills.004860C8</b>  |
| 00406FDB | . 51             | PUSH ECX                      |
| 00406FDC | . 53             | PUSH EBX                      |
| 00406FDD | . FF35 A4415000  | PUSH DWORD PTR DS:[5041A4]    |
| 00406FE3 | . 804D F0        | LEA ECX,DWORD PTR SS:[EBP-10] |
| 00406FE6 | . E8 8481FFFF    | <b>CALL MrBills.0048216F</b>  |
| 00406FEB | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]     |
| 00406FEE | . 8365 FC 00     | AND DWORD PTR SS:[EBP-4],0    |
| 00406FF2 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]     |
| 00406FF5 | . 8045 F0        | LEA EAX,DWORD PTR SS:[EBP-10] |
| 00406FF8 | . 50             | PUSH EBX                      |
| 00406FF9 | . E8 40FFFFFF    | <b>CALL MrBills.00406F48</b>  |
| 00406FFE | . 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10] |
| 00407001 | . 83C4 0C        | ADD ESP,0C                    |
| 00407004 | . 83C1 F0        | ADD ECX,-10                   |
| 00407007 | . 8AD8           | MOV BL,AL                     |
| 00407009 | . E8 3AA1FFFF    | <b>CALL MrBills.00401148</b>  |
| 0040700E | . 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |
| 00407011 | . 89C3           | MOV AL,BL                     |
| 00407013 | . 5B             | POP EBX                       |
| 00407014 | . 64:8900 000000 | MOU DWORD PTR FS:[0],ECX      |
| 00407018 | . C9             | LEAVE                         |
| 0040701C | . C3             | <b>RETN</b>                   |
| 0040701D | # B8 AB374B00    | MOU EAX,MrBills.004B37AB      |
| 00407022 | . E8 A1F00700    | <b>CALL MrBills.004860C8</b>  |
| 00407027 | . 51             | PUSH ECX                      |
| 00407028 | . 53             | PUSH EBX                      |
| 00407029 | . FF35 A0415000  | PUSH DWORD PTR DS:[5041A0]    |
| 0040702F | . 804D F0        | LEA ECX,DWORD PTR SS:[EBP-10] |
| 00407032 | . E8 3881FFFF    | <b>CALL MrBills.0048216F</b>  |
| 00407037 | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]     |
| 0040703A | . 8365 FC 00     | AND DWORD PTR SS:[EBP-4],0    |
| 0040703E | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]     |
| 00407041 | . 8045 F0        | LEA EAX,DWORD PTR SS:[EBP-10] |
| 00407044 | . 50             | PUSH EBX                      |
| 00407045 | . E8 01FFFFFF    | <b>CALL MrBills.00406F48</b>  |
| 00407048 | . 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10] |
| 0040704D | . 83C4 0C        | ADD ESP,0C                    |
| 00407050 | . 83C1 F0        | ADD ECX,-10                   |
| 00407053 | . 8AD8           | MOV BL,AL                     |
| 00407055 | . E8 EEA0FFFF    | <b>CALL MrBills.00401148</b>  |
| 00407058 | . 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |

004B37AB=MrBills.004B37AB  
Local calls from 004070CB, 00407155

:)

C CPU - main thread, module MrBills

| Address  | Hex dump         | Disassembly                   | Comment          |
|----------|------------------|-------------------------------|------------------|
| 00406FD1 | # B8 AB374B00    | MOU EAX,MrBills.004B37AB      |                  |
| 00406FD6 | . E8 EDF00700    | <b>CALL MrBills.004860C8</b>  |                  |
| 00406FDB | . 51             | PUSH ECX                      |                  |
| 00406FDC | . 53             | PUSH EBX                      |                  |
| 00406FDD | . FF35 A4415000  | PUSH DWORD PTR DS:[5041A4]    | MrBills.004BA704 |
| 00406FE3 | . 804D F0        | LEA ECX,DWORD PTR SS:[EBP-10] |                  |
| 00406FE6 | . E8 3881FFFF    | <b>CALL MrBills.0048216F</b>  |                  |
| 00406FEB | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]     |                  |
| 00406FEE | . 8365 FC 00     | AND DWORD PTR SS:[EBP-4],0    |                  |
| 00406FF2 | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]     |                  |
| 00406FF5 | . 8045 F0        | LEA EAX,DWORD PTR SS:[EBP-10] |                  |
| 00406FF8 | . 50             | PUSH EBX                      |                  |
| 00406FF9 | . E8 40FFFFFF    | <b>CALL MrBills.00406F48</b>  |                  |
| 00406FFE | . 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10] |                  |
| 00407001 | . 83C4 0C        | ADD ESP,0C                    |                  |
| 00407004 | . 83C1 F0        | ADD ECX,-10                   |                  |
| 00407007 | . 8AD8           | MOV BL,AL                     |                  |
| 00407009 | . E8 3AA1FFFF    | <b>CALL MrBills.00401148</b>  |                  |
| 0040700E | . 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |                  |
| 00407011 | . 89C3           | MOV AL,BL                     |                  |
| 00407013 | . 5B             | POP EBX                       |                  |
| 00407014 | . 64:8900 000000 | MOU DWORD PTR FS:[0],ECX      |                  |
| 00407018 | . C9             | LEAVE                         |                  |
| 0040701C | . C3             | <b>RETN</b>                   |                  |
| 0040701D | # B8 AB374B00    | MOU EAX,MrBills.004B37AB      |                  |
| 00407022 | . E8 A1F00700    | <b>CALL MrBills.004860C8</b>  |                  |
| 00407027 | . 51             | PUSH ECX                      |                  |
| 00407028 | . 53             | PUSH EBX                      |                  |
| 00407029 | . FF35 A0415000  | PUSH DWORD PTR DS:[5041A0]    | MrBills.004BA710 |
| 0040702F | . 804D F0        | LEA ECX,DWORD PTR SS:[EBP-10] |                  |
| 00407032 | . E8 3881FFFF    | <b>CALL MrBills.0048216F</b>  |                  |
| 00407037 | . FF75 0C        | PUSH DWORD PTR SS:[EBP+C]     |                  |
| 0040703A | . 8365 FC 00     | AND DWORD PTR SS:[EBP-4],0    |                  |
| 0040703E | . FF75 08        | PUSH DWORD PTR SS:[EBP+8]     |                  |
| 00407041 | . 8045 F0        | LEA EAX,DWORD PTR SS:[EBP-10] |                  |
| 00407044 | . 50             | PUSH EBX                      |                  |
| 00407045 | . E8 01FFFFFF    | <b>CALL MrBills.00406F48</b>  |                  |
| 00407048 | . 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10] |                  |
| 0040704D | . 83C4 0C        | ADD ESP,0C                    |                  |
| 00407050 | . 83C1 F0        | ADD ECX,-10                   |                  |
| 00407053 | . 8AD8           | MOV BL,AL                     |                  |
| 00407055 | . E8 EEA0FFFF    | <b>CALL MrBills.00401148</b>  |                  |
| 00407058 | . 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |                  |

Here, the value for AL is set back

이곳, AL value 가 set 되고 돌아온다.

After it was first set in BL

먼저 BL 이 set 된 후에

Do you understand that this means that this call most probably has no influence on BL (and AL).

이 뜻은 이 call 은 아마 BL 에 영향이 없다. 이해했어?(and AL)

But AL is decided here in this call

그러나 AL 은 이 call 에서 결정된다.

Right, AL is set in the call just above, so put a BP

맞아, AL 은 이 call 의 위에서 set 된다. 그래서 BP 를 넣어라.

Remember that we are a couple of calls deep in the code yet.

기억해. 우리는 이 code 에서 call 의 couple 이 깊어진다. 아직

Also remember that we pressed <enter> to come see the code in this call.

또한 기억해. 우리가 이 call 에서 code 를 보기 위해 enter 를 넣었다.

To verify if AL is really set here, we will run till breaking in this BP. Press F9

검증하자. 만약에 AL 이 정말로 set 됐다면, 우리는 BP 가 걸린 곳까지 run 할 수 있다. F9 눌러.

C CPU - main thread, module MrBills

| Address                 | Hex dump        | Disassembly                    | Comment |
|-------------------------|-----------------|--------------------------------|---------|
| 00400FF9                | E8 40FFFFFF     | CALL MrBills.00406F48          |         |
| 00400FFF                | . C840 F0       | MOU ECX, DWORD PTR SS:[EBP-10] |         |
| Bam, we break in the BP |                 |                                |         |
| 0040700E                | E8 30FFFFFF     | CALL MrBills.00401148          |         |
| 00407011                | . C840 F4       | MOU ECX, DWORD PTR SS:[EBP-C]  |         |
| 00407013                | 8AC3            | MUL DL, AL                     |         |
| 00407014                | 5B              |                                |         |
| 0040701B                | 64:89           |                                |         |
| 0040701C                | C9              |                                |         |
| 0040701D                | C3              |                                |         |
| 00407022                | B8 AB           |                                |         |
| 00407027                | E8 A1           |                                |         |
| 00407028                | S1              |                                |         |
| 00407029                | S3              |                                |         |
| 0040702F                | FF35            |                                |         |
| 00407032                | 8040            |                                |         |
| 00407037                | E8 38           |                                |         |
| 00407039                | FF75 00         |                                |         |
| 0040703E                | 8365            |                                |         |
| 00407041                | 8045 F0         | LEH EAX, DWORD PTR SS:[EBP-10] |         |
| 00407044                | 5A              | PUSH EAX                       |         |
| 00407045                | E8 01FFFFFF     | CALL MrBills.00406F48          |         |
| 00407049                | . C840 F0       | MOU ECX, DWORD PTR SS:[EBP-10] |         |
| 0040704D                | 83C4 0C         | ADD ESP, 0C                    |         |
| 00407050                | 83C1 F0         | ADD ECX, -10                   |         |
| 00407053                | 8AD8            | MOU BL, AL                     |         |
| 00407055                | E8 EEA0FFFF     | CALL MrBills.00401148          |         |
| 00407059                | . C840 F4       | MOU ECX, DWORD PTR SS:[EBP-C]  |         |
| 0040705D                | 8AC3            | MUL AL, BL                     |         |
| 0040705F                | 5B              | POP EBX                        |         |
| 00407060                | 64:8900 000000  | MOU DWORD PTR FS:[0], ECX      |         |
| 00407067                | C9              | LEAVE                          |         |
| 00407068                | C3              | RETN                           |         |
| 00407069                | B8 03384B00     | MOU EAX, MrBills.004B3803      |         |
| 0040706E                | E8 5F000700     | CALL MrBills.004860C8          |         |
| 00407073                | 83EC 0C         | SUB ESP, 0C                    |         |
| 00407076                | 89D0 A1765000   | CMP BYTE PTR DS:[5076A1], 0    |         |
| 0040707D                | . 0F85 9F000000 | JNZ MrBills.00407122           |         |
| 00407083                | C605 A1765000   | MOU BYTE PTR DS:[5076A1], 1    |         |
| 00407090                | E8 4B050000     | CALL MrBills.00492508          |         |

Bam, we break in the BP

우리는 BP 에서 멈출 수 있다.

Next step is crucial for you to understand.

다음 step 은 너에게 이해하는데 있어 중요하다.

1. Note the value for AL

1.AL 을 적어라.

2.We are about to execute the call we suspect to set AL

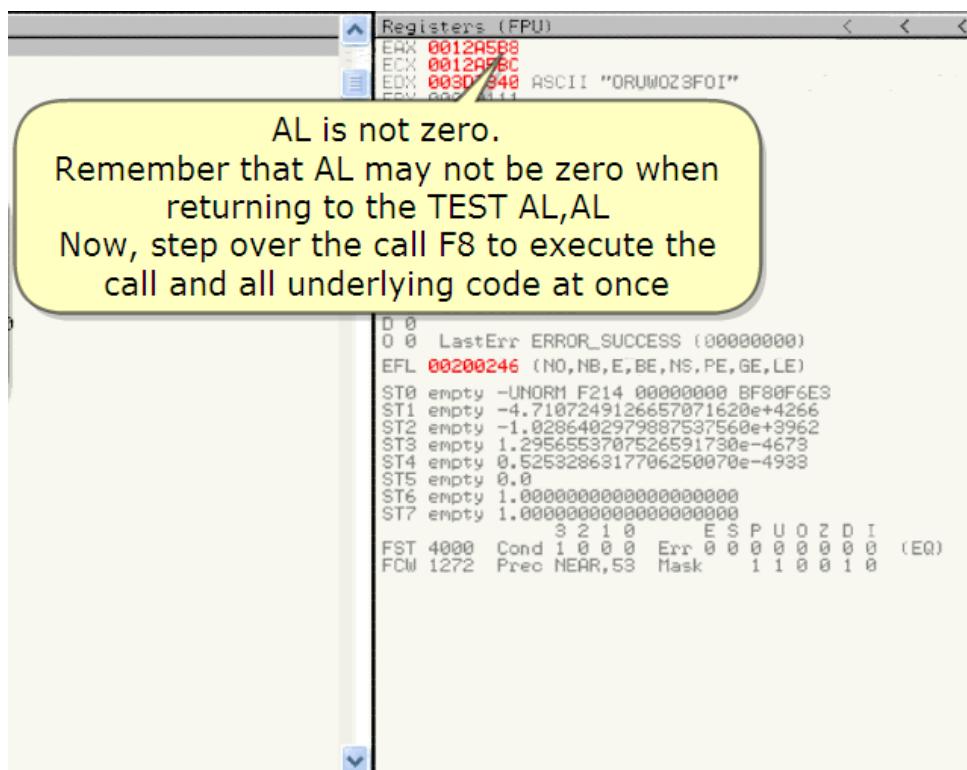
2.우리는 call 을 실행하기 위한 것이 있다. AL 을 set 하기 위해 의심한다.

3.Step over this call(F8)

3.Step 을 넘기기 위해 F8 을 눌러.

4.Seek confirmation looking at AL again

4.AL 을 보고 다시 확인하고자 합니다.



AL is not zero.

AL 은 zero 가 아니다.

Remember that AL may not be zero when returning to the TEST AL, AL

기억해. TEST AL, AL 을 하고 난 후에 AL 은 zero 가 되지 않을 것이다.

Now, step over the call F8 to execute the call underlying code at once

이제, F8 을 눌러 한 번에 근본적인 call 을 실행 시켜보자.

**C CPU - main thread, module MrBills**

| Address  | Hex dump       | Disassembly                   | Comment  | Registers (FP) |
|--|----------------|-------------------------------|--|----------------|
| 00406FF9   | E8 40FFFFFF    | CALL MrBills.00406F4B         |  |                |
| 00406FFE   | 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407001   | 83C4 0C        | ADD ESP,0C                    |  |                |
| 00407004   | 88C1 F0        | ADD ECX,-10                   |  |                |
| 00407007   | 88D8           | MOV BL,AL                     |  |                |
| 00407009   | E8 38A1FFFF    | CALL MrBills.00401148         | because after the call :<br>AL == 0                                    |                |
| 0040700E   | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 00407011   | 88C3           | MOV AL,0                      | Yep ! So, in this call, AL is set to 0<br>(not registered)             |                |
| 00407014   | 58             | POP EBX                       |  |                |
| 00407016   | 64:8900 000000 | MOV DI,0                      |  |                |
| 00407018   | C9             | LEAVE                         |  |                |
| 0040701A   | C3             | RETN                          |  |                |
| 00407020   | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 00407022   | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 00407025   | S1             | PUSH ECX                      |  |                |
| 00407028   | S2             | PUSH EBX                      |  |                |
| 00407029   | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 0040702E   | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 00407031   | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407034   | 88C1 F0        | ADD ECX,-10                   |  |                |
| 00407037   | 58             | POP EBX                       |  |                |
| 00407039   | 64:8900 000000 | MOV DI,0                      |  |                |
| 0040703B   | C9             | LEAVE                         |  |                |
| 0040703D   | C3             | RETN                          |  |                |
| 00407040   | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 00407042   | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 00407045   | S1             | PUSH ECX                      |  |                |
| 00407048   | S2             | PUSH EBX                      |  |                |
| 00407049   | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 00407052   | E8 38A1FFFF    | CALL MrBills.00401148         | And also take note of<br>the AL and BL values<br>in the next steps !!! |                |
| 00407055   | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407058   | 88C1 F0        | ADD ECX,-10                   |  |                |
| 0040705B   | 58             | POP EBX                       |  |                |
| 0040705D   | 64:8900 000000 | MOV DI,0                      |  |                |
| 0040705F   | C9             | LEAVE                         |  |                |
| 00407061   | C3             | RETN                          |  |                |
| 00407068   | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 00407070   | E8 A1F00700    | CALL MrBills.00496008         | Setting BL to zero<br>in this step because<br>AL == 0                  |                |
| 00407073   | S1             | PUSH ECX                      |  |                |
| 00407076   | S2             | PUSH EBX                      |  |                |
| 00407077   | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 00407080   | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 00407083   | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407086   | 88C1 F0        | ADD ECX,-10                   |  |                |
| 00407089   | 58             | POP EBX                       |  |                |
| 0040708B   | 64:8900 000000 | MOV DI,0                      |  |                |
| 0040708D   | C9             | LEAVE                         |  |                |
| 0040708F   | C3             | RETN                          |  |                |
| 00407096   | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 00407098   | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 0040709B   | S1             | PUSH ECX                      |  |                |
| 0040709E   | S2             | PUSH EBX                      |  |                |
| 0040709F   | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 004070A2   | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 004070A5   | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 004070A8   | 88C1 F0        | ADD ECX,-10                   |  |                |
| 004070AB   | 58             | POP EBX                       |  |                |
| 004070AD   | 64:8900 000000 | MOV DI,0                      |  |                |
| 004070AF   | C9             | LEAVE                         |  |                |
| 004070B1   | C3             | RETN                          |  |                |
| 004070B8   | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 004070BA   | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 004070BD   | S1             | PUSH ECX                      |  |                |
| 004070CE   | S2             | PUSH EBX                      |  |                |
| 004070CF   | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 004070D2   | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 004070D5   | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 004070D8   | 88C1 F0        | ADD ECX,-10                   |  |                |
| 004070DB   | 58             | POP EBX                       |  |                |
| 004070DD   | 64:8900 000000 | MOV DI,0                      |  |                |
| 004070DF   | C9             | LEAVE                         |  |                |
| 004070E1   | C3             | RETN                          |  |                |
| 004070E8   | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 004070EA   | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 004070EB   | S1             | PUSH ECX                      |  |                |
| 004070ED   | S2             | PUSH EBX                      |  |                |
| 004070EF   | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 004070F2   | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 004070F5   | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 004070F8   | 88C1 F0        | ADD ECX,-10                   |  |                |
| 004070FB   | 58             | POP EBX                       |  |                |
| 004070FD   | 64:8900 000000 | MOV DI,0                      |  |                |
| 004070FF   | C9             | LEAVE                         |  |                |
| 00407101   | C3             | RETN                          |  |                |
| Stack SS:[0012A5B8]=00307340, (ASCII "ORUM023FOI") |                |                               |  |                |
| ECX=0012A5BC                                       |                |                               |  |                |

Yup! So, in this call, AL is set to 0 (not registered)

Because after the call : AL == 0

예! 그래서 이 call에서 al은 0으로 set 된다.(미등록)

왜냐하면 call 후에 : AL == 0이기 때문이다.

F8 to see what happens further

무슨 일이 생기는지 F8을 눌러서 보자.

**C CPU - main thread, module MrBills**

| Address  | Hex dump       | Disassembly                   | Comment  | Registers (FP) |
|----------|----------------|-------------------------------|--|----------------|
| 00406FF9 | E8 40FFFFFF    | CALL MrBills.00406F4B         |  |                |
| 00406FFE | 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407001 | 83C4 0C        | ADD ESP,0C                    |  |                |
| 00407004 | 88C1 F0        | ADD ECX,-10                   |  |                |
| 00407007 | 88D8           | MOV BL,AL                     |  |                |
| 00407009 | E8 38A1FFFF    | CALL MrBills.00401148         | And also take note of<br>the AL and BL values<br>in the next steps !!! |                |
| 0040700E | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 00407011 | 88C3           | MOV AL,0                      |  |                |
| 00407014 | 58             | POP EBX                       | Setting BL to zero<br>in this step because<br>AL == 0                  |                |
| 00407016 | 64:8900 000000 | MOV DI,0                      |  |                |
| 00407018 | C9             | LEAVE                         |  |                |
| 0040701A | C3             | RETN                          |  |                |
| 0040701D | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 00407022 | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 00407025 | S1             | PUSH ECX                      |  |                |
| 00407028 | S2             | PUSH EBX                      |  |                |
| 00407029 | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 0040702E | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 00407031 | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407034 | 88C1 F0        | ADD ECX,-10                   |  |                |
| 00407037 | 58             | POP EBX                       |  |                |
| 00407039 | 64:8900 000000 | MOV DI,0                      |  |                |
| 0040703B | C9             | LEAVE                         |  |                |
| 0040703D | C3             | RETN                          |  |                |
| 00407040 | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 00407042 | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 00407045 | S1             | PUSH ECX                      |  |                |
| 00407048 | S2             | PUSH EBX                      |  |                |
| 00407049 | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 00407052 | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 00407055 | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407058 | 88C1 F0        | ADD ECX,-10                   |  |                |
| 0040705B | 58             | POP EBX                       |  |                |
| 0040705D | 64:8900 000000 | MOV DI,0                      |  |                |
| 0040705F | C9             | LEAVE                         |  |                |
| 00407061 | C3             | RETN                          |  |                |
| 00407068 | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 00407070 | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 00407073 | S1             | PUSH ECX                      |  |                |
| 00407076 | S2             | PUSH EBX                      |  |                |
| 00407077 | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 00407080 | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 00407083 | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407086 | 88C1 F0        | ADD ECX,-10                   |  |                |
| 00407089 | 58             | POP EBX                       |  |                |
| 0040708B | 64:8900 000000 | MOV DI,0                      |  |                |
| 0040708D | C9             | LEAVE                         |  |                |
| 0040708F | C3             | RETN                          |  |                |
| 00407096 | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 00407098 | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 0040709B | S1             | PUSH ECX                      |  |                |
| 0040709E | S2             | PUSH EBX                      |  |                |
| 0040709F | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 004070D2 | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 004070D5 | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 004070D8 | 88C1 F0        | ADD ECX,-10                   |  |                |
| 004070DB | 58             | POP EBX                       |  |                |
| 004070DD | 64:8900 000000 | MOV DI,0                      |  |                |
| 004070DF | C9             | LEAVE                         |  |                |
| 004070E1 | C3             | RETN                          |  |                |
| 004070E8 | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 004070EA | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 004070EB | S1             | PUSH ECX                      |  |                |
| 004070ED | S2             | PUSH EBX                      |  |                |
| 004070EF | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 004070F2 | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 004070F5 | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 004070F8 | 88C1 F0        | ADD ECX,-10                   |  |                |
| 004070FB | 58             | POP EBX                       |  |                |
| 004070FD | 64:8900 000000 | MOV DI,0                      |  |                |
| 004070FF | C9             | LEAVE                         |  |                |
| 00407101 | C3             | RETN                          |  |                |
| 00407108 | \$ E8 AB374B00 | MOU ERX,MrBills.004B37AB      |  |                |
| 0040710A | E8 A1F00700    | CALL MrBills.00496008         |  |                |
| 0040710D | S1             | PUSH ECX                      |  |                |
| 0040710E | S2             | PUSH EBX                      |  |                |
| 0040710F | F0             | LEA ECX,DWORD PTR SS:[EBP-C]  |  |                |
| 00407112 | E8 38A1FFFF    | CALL MrBills.00401148         |  |                |
| 00407115 | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-10] |  |                |
| 00407118 | 88C1 F0        | ADD ECX,-10                   |  |                |
| 0040711B | 58             | POP EBX                       |  |                |
| 0040711D | 64:8900 000000 | MOV DI,0                      |  |                |
| 0040711F | C9             | LEAVE                         |  |                |
| 00407121 | C3             | RETN                          |  |                |

And also take note of the AL and BL values in the next steps !!!

AL과 BL 값을 적어놓자.

Setting BL to zero in this step because AL == 00

이 step에서 BL 값을 zero로 setting 한다. 왜냐하면 AL == 00이기 때문이다.

Registers (FPU)

```

ERX 00000000
ECX 003D7330
EDX 003D0608
EBX 00000100
ESP 0012A5B4
EBP 0012A5C8
ESI 0012AD6C
EDI 0012AE88
EIP 00407009 MrBills.00407009
C 1 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit ?FFDE000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00200207 (NO,B,NE,BE,NS,PE,GE,G)
ST0 empty -UNORM F214 00000000 BF80F6E3
ST1 empty -4.7107249126657071620e+4266
ST2 empty -1.0286402979887537560e+3962
ST3 empty 1.2956553707526591730e-4673
ST4 empty 0.5253286317706250070e-4933
ST5 empty 0.0
ST6 empty 1.000000000000000000000000000000
ST7 empty 1.000000000000000000000000000000
          3 2 1 0   E S P U O Z
FST 4000 Cond 1 0 0 0 Err 0 0 0 0 0 0
FCW 1272 Prec NEAR,53 Mask 1 1 0 0

```

AL and BL  
are zero

AL and BL are zero

AL and BL 은 zero 이다.

Registers (FPU)

```

ERX 00000001
ECX 003D7330
EDX 003D0608
EBX 00000100
ESP 0012A5B4
EBP 0012A5C8
ESI 0012AD6C
EDI 0012AE88
EIP 0040700E MrBills.0040700E
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 1 FS 003B 32bit ?FFDE000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00200296 (NO,NB,NE,A,S,PE,L,LE)
ST0 empty -UNORM F214 00000000 BF80F6E3
ST1 empty -4.7107249126657071620e+4266
ST2 empty -1.0286402979887537560e+3962
ST3 empty 1.2956553707526591730e-4673
ST4 empty 0.5253286317706250070e-4933
ST5 empty 0.0
ST6 empty 1.000000000000000000000000000000
ST7 empty 1.000000000000000000000000000000
          3 2 1 0   E S P U O Z
FST 4000 Cond 1 0 0 0 Err 0 0 0 0 0 0
FCW 1272 Prec NEAR,53 Mask 1 1 0 0

```

Oops  
AL == 1

Oops AL == 1

웁스 AL == 1 이다.

## C CPU - main thread, module MrBills

| Address  | Hex dump       | Disassembly                    | Comment                                   |
|----------|----------------|--------------------------------|---|
| 00406FF9 | E8 40FFFFFF    | CALL MrBills.00406F48          |   |
| 00406FFE | 884D F0        | MOV ECX, DWORD PTR SS:[EBP-10] |   |
| 00407001 | 83C4 0C        | ADD ESP, 0C                    |   |
| 00407004 | 83C1 F0        | ADD ECX, -10                   |   |
| 00407007 | 8AD8           | MOV BL, AL                     |   |
| 00407009 | E8 3A81FFFF    | CALL MrBills.00401148          |   |
| 0040700E | 884D F4        | MOV ECX, DWORD PTR SS:[EBP-C]  |   |
| 00407011 | SAC3           | MOV AL, BL                     |   |
| 00407013 | 5B             | POP EBX                        |   |
| 00407014 | 64:8900 000000 | MOV DWORD PTR FS:[0], ECX      |   |
| 0040701B | C9             | LEAVE                          |   |
| 0040701C | C3             |                                |   |
| 0040701D | \$ B8          |                                | Aha, see why AL was put in BL ?           |
| 00407022 | E8             |                                | Yes, now it can be zeroed again by BL     |
| 00407027 | S1             |                                | INFO : if a program needs to work with    |
| 00407028 | S3             |                                | the EAX register, it will temporarily put |
| 00407029 | FF3            |                                | its value in another register             |
| 0040702F | 8D4            |                                | 04BA710                                   |
| 00407032 | E8             |                                |   |
| 00407037 | FF7            |                                |   |
| 0040703A | 83C6           |                                |   |
| 0040703E | FF7            |                                |   |
| 00407041 | 8D45           |                                |   |
| 00407044 | 50             | PUSH ECX                       |   |
| 00407045 | E8 01FFFFFF    | CALL MrBills.00406F48          |   |
| 0040704A | 884D F0        | MOV ECX, DWORD PTR SS:[EBP-10] |   |
| 0040704D | 83C4 0C        | ADD ESP, 0C                    |   |
| 00407050 | 83C1 F0        | ADD ECX, -10                   |   |
| 00407053 | 8AD8           | MOV BL, AL                     |   |

Aha, see why AL was put in BL?

아하, 왜 BL 이 AL 에 넣어졌나?

Yes, now it can be zeroed again by BL

예, 다시 BL 에 의해 zero 가 될 것이다.

INFO : if a program needs to work with the EAX register, it will temporarily put its value in another register

정보 : 만약에 program 이 EAX register 와 함께 일하는 게 필요하다면, 그것은 임시적으로 그것의 값이 다른 register 에 넣어질 것이다.

I'll explain you once again, so you get the feeling of how a program works

다시 한 번 너에게 설명하겠다. 그래서 너는 program 이 어떻게 일하는지 느낌을 얻을 수 있다.

| Address  | Hex dump    | Disassembly                    | Comment  | Registers (CPU)  |
|----------|-------------|--------------------------------|--|--|
| 00406FF9 | E8 40FFFFFF | CALL MrBills.00406F48          |  | ECX 00000000<br>ECX 00124600<br>ESP 00000000<br>ESP 00000000<br>EBP 1245B4<br>EBP 1245C8<br>EBP 124600<br>EBP 124600 |
| 00406FFE | 884D F0     | MOV ECX, DWORD PTR SS:[EBP-10] |  |  |
| 00407001 | 83C4 0C     | ADD ESP, 0C                    |  |  |
| 00407004 | 83C1 F0     | ADD ECX, -10                   |  |  |
| 00407007 | 8AD8        | MOV BL, AL                     |  |  |
| 00407009 | E8 3A81FFFF | CALL MrBills.00401148          | Did you remark that AL is only temporarily "moved" in BL (during the call) ... |  |
| 0040700E | 884D F4     | MOV ECX, DWORD PTR SS:[EBP-C]  |  |  |
| 00407011 | SAC3        | MOV AL, BL                     |  |  |
| 00407013 | \$ B8       | RET                            |  |  |
| 00407014 | E8 406FF9   | CALL MrBills.00406F48          | And that AL is again equal to zero after it is reset by BL                     |  |
| 0040701C | C9          | LEAVE                          |  |  |
| 0040701D | E8 0B374B00 | MOV ERX, MrBills.004B37AB      |  |  |
| 00407022 | E8 A1F08700 | CALL MrBills.004A8700          |  |  |
| 00407027 | S3          | PUSH ECX                       |  |  |
| 00407028 | FF75 0C     | PUSH ECX                       |  |  |
| 00407029 | 8955 FC 00  | PUSH DWORD PTR DS:[0041A0]     |  |  |
| 0040702A | 8955 00 00  | PUSH DWORD PTR DS:[0041A1]     |  |  |
| 0040702B | 8945 F8     | PUSH ECX                       |  |  |
| 0040702C | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 0040702D | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040702E | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040702F | 8945 F8     | PUSH ECX                       |  |  |
| 00407031 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407034 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407035 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407036 | 8945 F8     | PUSH ECX                       |  |  |
| 00407037 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407039 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040703A | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040703B | 8945 F8     | PUSH ECX                       |  |  |
| 0040703C | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 0040703D | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040703E | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040703F | 8945 F8     | PUSH ECX                       |  |  |
| 00407040 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407041 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407042 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407043 | 8945 F8     | PUSH ECX                       |  |  |
| 00407044 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407045 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407046 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407047 | 8945 F8     | PUSH ECX                       |  |  |
| 00407048 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407049 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040704A | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040704B | 8945 F8     | PUSH ECX                       |  |  |
| 0040704C | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 0040704D | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040704E | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040704F | 8945 F8     | PUSH ECX                       |  |  |
| 00407050 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407051 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407052 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407053 | 8945 F8     | PUSH ECX                       |  |  |
| 00407054 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407055 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407056 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407057 | 8945 F8     | PUSH ECX                       |  |  |
| 00407058 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407059 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040705A | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040705B | 8945 F8     | PUSH ECX                       |  |  |
| 0040705C | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 0040705D | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040705E | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040705F | 8945 F8     | PUSH ECX                       |  |  |
| 00407060 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407061 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407062 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407063 | 8945 F8     | PUSH ECX                       |  |  |
| 00407064 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407065 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407066 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407067 | 8945 F8     | PUSH ECX                       |  |  |
| 00407068 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407069 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040706A | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040706B | 8945 F8     | PUSH ECX                       |  |  |
| 0040706C | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 0040706D | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040706E | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040706F | 8945 F8     | PUSH ECX                       |  |  |
| 00407070 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407071 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407072 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407073 | 8945 F8     | PUSH ECX                       |  |  |
| 00407074 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407075 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407076 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407077 | 8945 F8     | PUSH ECX                       |  |  |
| 00407078 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407079 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040707A | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040707B | 8945 F8     | PUSH ECX                       |  |  |
| 0040707C | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 0040707D | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040707E | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040707F | 8945 F8     | PUSH ECX                       |  |  |
| 00407080 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407081 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407082 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407083 | 8945 F8     | PUSH ECX                       |  |  |
| 00407084 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407085 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407086 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407087 | 8945 F8     | PUSH ECX                       |  |  |
| 00407088 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407089 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040708A | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040708B | 8945 F8     | PUSH ECX                       |  |  |
| 0040708C | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 0040708D | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040708E | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040708F | 8945 F8     | PUSH ECX                       |  |  |
| 00407090 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407091 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407092 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407093 | 8945 F8     | PUSH ECX                       |  |  |
| 00407094 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407095 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 00407096 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 00407097 | 8945 F8     | PUSH ECX                       |  |  |
| 00407098 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 00407099 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040709A | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040709B | 8945 F8     | PUSH ECX                       |  |  |
| 0040709C | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 0040709D | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 0040709E | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 0040709F | 8945 F8     | PUSH ECX                       |  |  |
| 004070A0 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070A1 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070A2 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070A3 | 8945 F8     | PUSH ECX                       |  |  |
| 004070A4 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070A5 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070A6 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070A7 | 8945 F8     | PUSH ECX                       |  |  |
| 004070A8 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070A9 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070AA | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070AB | 8945 F8     | PUSH ECX                       |  |  |
| 004070AC | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070AD | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070AE | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070AF | 8945 F8     | PUSH ECX                       |  |  |
| 004070B0 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070B1 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070B2 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070B3 | 8945 F8     | PUSH ECX                       |  |  |
| 004070B4 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070B5 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070B6 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070B7 | 8945 F8     | PUSH ECX                       |  |  |
| 004070B8 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070B9 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070BA | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070BB | 8945 F8     | PUSH ECX                       |  |  |
| 004070BC | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070BD | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070BE | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070BF | 8945 F8     | PUSH ECX                       |  |  |
| 004070C0 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070C1 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070C2 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070C3 | 8945 F8     | PUSH ECX                       |  |  |
| 004070C4 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070C5 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070C6 | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070C7 | 8945 F8     | PUSH ECX                       |  |  |
| 004070C8 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070C9 | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070CA | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070CB | 8945 F8     | PUSH ECX                       |  |  |
| 004070CC | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  |  |
| 004070CD | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]      |  |  |
| 004070CE | 8955 FC 00  | PUSH DWORD PTR SS:[EBP+4], 0   |  |  |
| 004070CF | 8945 F8     | PUSH ECX                       |  |  |
| 004070D0 | S3          | LEA ERX, DWORD PTR SS:[EBP-10] |  | </   |

**C CPU - main thread, module MrBills**

| Address  | Hex dump       | Disassembly                   | Comment |
|----------|----------------|-------------------------------|---------|
| 00406FF9 | E8 4DFFFFFF    | CALL MrBills.00406F48         |         |
| 00406FFE | E8 4D F0       | MOU ECX,DWORD PTR SS:[EBP-10] |         |
| 00407001 | 89C4 0C        | ADD ESP,0C                    |         |
| 00407004 | 89C1 F0        | ADD ECX,-10                   |         |
| 00407007 | 89D8           | MOU BL,AL                     |         |
| 00407009 | E8 3FA1FFFF    | CALL MrBills.00401148         |         |
| 0040700E | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |         |
| 00407011 | 89C3           | MOU AL,BL                     |         |
| 00407013 | 58             | POP EBX                       |         |
| 00407014 | 64:8900 00000  | MOU DWORD PTR FS:[0],ECK      |         |
| 00407018 | C9             | LEAVE                         |         |
| 0040701B | C3             | RETN                          |         |
| 0040701C | \$ E8 AB374B00 | MOU EAX,MrBills.004B37AB      |         |
| 00407022 | E8 A1F00700    | CALL MrBills.004860C8         |         |
| 00407027 | 51             | PUSH ECK                      |         |

...and put back here after the call.  
So this call has no influence on AL

So, my conclusion that this call has no influence on AL (and BL) is correct

...and put back here after the call.

Call 후에 여기에 돌려준다.

So this call has no influence on AL

이 call 은 AL 에 영향을 주지 않는다.

So, my conclusion that this call has no influence on AL (and BL) is correct

그래서, 나의 결론 : 이 call 은 AL 에 정확히 영향을 주지 않는다.

**C CPU - main thread, module MrBills**

| Address  | Hex dump       | Disassembly                   | Comment |
|----------|----------------|-------------------------------|---------|
| 00406FF9 | E8 4DFFFFFF    | CALL MrBills.00406F48         |         |
| 00406FFE | E8 4D F0       | MOU ECX,DWORD PTR SS:[EBP-10] |         |
| 00407001 | 89C4 0C        | ADD ESP,0C                    |         |
| 00407004 | 89C1 F0        | ADD ECX,-10                   |         |
| 00407007 | 89D8           | MOU BL,AL                     |         |
| 00407009 | E8 3FA1FFFF    | CALL MrBills.00401148         |         |
| 0040700E | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |         |
| 00407011 | 89C3           | MOU AL,BL                     |         |
| 00407013 | 58             | POP EBX                       |         |
| 00407014 | 64:8900 00000  | MOU DWORD PTR FS:[0],ECK      |         |
| 00407018 | C9             | LEAVE                         |         |
| 0040701B | C3             | RETN                          |         |
| 0040701C | \$ E8 AB374B00 | MOU EAX,MrBills.004B37AB      |         |
| 00407022 | E8 A1F00700    | CALL MrBills.004860C8         |         |
| 00407027 | 51             | PUSH ECK                      |         |

Thus stating the setting of AL in here

Thus starting the setting of AL in here

처음 AL 값은 여기에서 setting 된다.

**C CPU - main thread, module MrBills**

| Address  | Hex dump       | Disassembly                   | Comment |
|----------|----------------|-------------------------------|---------|
| 00406FF9 | E8 4DFFFFFF    | CALL MrBills.00406F48         |         |
| 00406FFE | E8 4D F0       | MOU ECX,DWORD PTR SS:[EBP-10] |         |
| 00407001 | 89C4 0C        | ADD ESP,0C                    |         |
| 00407004 | 89C1 F0        | ADD ECX,-10                   |         |
| 00407007 | 89D8           | MOU BL,AL                     |         |
| 00407009 | E8 3FA1FFFF    | CALL MrBills.00401148         |         |
| 0040700E | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |         |
| 00407011 | 89C3           | MOU AL,BL                     |         |
| 00407013 | 58             | POP EBX                       |         |
| 00407014 | 64:8900 00000  | MOU DWORD PTR FS:[0],ECK      |         |
| 00407018 | C9             | LEAVE                         |         |
| 0040701C | C3             | RETN                          |         |
| 0040701D | \$ E8 AB374B00 | MOU EAX,MrBills.004B37AB      |         |
| 00407022 | E8 A1F00700    | CALL MrBills.004860C8         |         |
| 00407027 | 51             | PUSH ECK                      |         |
| 00407029 | F4             |                               |         |
| 0040702F | 89C6           |                               |         |
| 00407032 | FF75 08        | PUSH DWORD PTR SS:[EBP+8]     |         |
| 00407035 | 89C5 F0        | LEA EAX,DWORD PTR SS:[EBP-10] |         |
| 00407038 | 58             | POP EBX                       |         |
| 0040703E | E8 01FFFFFF    | CALL MrBills.00406F48         |         |

Finally, we land on the return to go back to the previous call. Step it F8 or F7.

Finally, we land on the return to go back to the previous call.

마지막으로, 우리는 이전의 call 로 돌아가기 위한 return 값에 도착한다.

Step it F8 or F7.

F8이나 F7을 눌러.

Ok. And so we are back in this call.

Ok. 우리는 call에서 돌아왔다.

Remember that AL may not be equal to zero when we return to the TEST AL, AL (JNZ to registered or not)

기억해. 우리가 돌아와서 TEST AL, AL을 할 때(JNZ 등록됐는지 아닌지) AL은 zero와 같아지지 않는다.

Now, study hits code here.

What happens with AL here?

이제, 여기 code를 공부하자.

이 AL에 무슨 일이 일어났나?

Mmmm, this here is all obvious : AL is never changed, but quite some stuff is carried out according to AL being 1 or 0 (=registered or not)

음, 이것은 명확하다 : AL은 절대 바뀌지 않았다, 그러나 꽤 많은 재료들은 AL이 1이나 0에 따라 움직였다. (=등록되거나 아니거나)

C CPU - main thread, module MrBills

| Address  | Hex dump    | Disassembly          | Comment                      | Registers (ESP)   |
|----------|-------------|----------------------|------------------------------|---|
| 0040715A | . 84C0      | TEST AL, AL          |                              | ERX 00000000<br>ECX 0012AE8C<br>EDX 0012AE88<br>ESP 0000001111<br>BP 0012AE88<br>0012AE88 |
| 0040715C | : 59        | POP ECX              | 0012AE8C                     | 0012AE88  |
| 0040715D |             |                      |                              | 0012AE88  |
| 0040715E |             |                      |                              | 0012AE88  |
| 0040715F |             |                      |                              | 0012AE88  |
| 00407160 |             |                      |                              | 0012AE88  |
| 00407161 |             |                      |                              | 0012AE88  |
| 00407162 |             |                      |                              | 0012AE88  |
| 00407163 |             |                      |                              | 0012AE88  |
| 00407164 |             |                      |                              | 0012AE88  |
| 00407165 |             |                      |                              | 0012AE88  |
| 00407166 |             |                      |                              | 0012AE88  |
| 00407167 |             |                      |                              | 0012AE88  |
| 00407168 |             |                      |                              | 0012AE88  |
| 00407169 |             |                      |                              | 0012AE88  |
| 00407170 | .           | 84C0                 | TEST AL, AL                  | 0012AE88  |
| 00407171 | .           | 59                   | POP ECX                      | 0012AE88  |
| 00407172 | .           | 59                   | POP ECX                      | 0012AE88  |
| 00407173 | .           | 59                   | POP ECX                      | 0012AE88  |
| 00407174 | .           | A2 A0765000          | MOU BYTE PTR DS:[S07600], AL | 0012AE88  |
| 00407175 | .           | A2 A2765000          | MOU BYTE PTR DS:[S07642], AL | 0012AE88  |
| 00407176 | .           | v74 00               | JNE SHORT MrBills.00407180   | 0012AE88  |
| 00407177 | > FF75 0C   |                      |                              | 0012AE88  |
| 00407178 | > FF75 08   |                      |                              | 0012AE88  |
| 00407179 |             |                      |                              | 0012AE88  |
| 00407180 |             |                      |                              | 0012AE88  |
| 00407181 |             |                      |                              | 0012AE88  |
| 00407182 |             |                      |                              | 0012AE88  |
| 00407183 |             |                      |                              | 0012AE88  |
| 00407184 |             |                      |                              | 0012AE88  |
| 00407185 |             |                      |                              | 0012AE88  |
| 00407186 |             |                      |                              | 0012AE88  |
| 00407187 |             |                      |                              | 0012AE88  |
| 00407188 |             |                      |                              | 0012AE88  |
| 00407189 |             |                      |                              | 0012AE88  |
| 0040718A |             |                      |                              | 0012AE88  |
| 0040718B |             |                      |                              | 0012AE88  |
| 0040718C |             |                      |                              | 0012AE88  |
| 0040718D | > 50        |                      |                              | 0012AE88  |
| 0040718E | ,^E9 D6FFFF | JMP MrBills.00407069 |                              | 0012AE88  |

Step the code F8 to seek confirmation for that

And notice that AL is still zero

F8을 눌러 좀 더 확인하자.

AL은 여전히 zero다.

**C CPU - main thread, module MrBills**

| Address  | Hex dump      | Disassembly                  | Comment |
|----------|---------------|------------------------------|---------|
| 0040715A | 84C0          | TEST AL,AL                   |         |
| 0040715C | · 59          | POP ECX                      |         |
| 0040715D | · 59          | POP ECX                      |         |
| 0040715E | · R2 A0765000 | MOV BYTE PTR DS:[5076A01],AL |         |
| 00407163 | · v75 1B      | JNZ SHORT MrBills.00407180   |         |
| 00407165 | · FF75 0C     | PUSH DWORD PTR SS:[EBP+C]    |         |
| 00407168 | · FF75 08     | PUSH DWORD PTR SS:[EBP+8]    |         |
| 0040716B | · E8 ADFFFFFF | CALL MrBills.00407010        |         |
| 00407170 | · 84C0        | TEST AL,AL                   |         |
| 00407172 | · 59          | POP ECX                      |         |
| 00407173 | · 59          | POP ECX                      |         |
| 00407174 | · R2 A0765000 | MOV BYTE PTR DS:[5076A01],AL |         |
| 00407176 | · R2 A2765000 | MOV BYTE PTR DS:[5076A21],AL |         |
| 0040717E | > v74 0D      | JE SHORT MrBills.00407180    |         |
| 00407180 | > FF75 0C     | PUSH DWORD PTR SS:[EBP+C]    |         |
| 00407183 | > FF75 08     | PUSH DWORD PTR SS:[EBP+8]    |         |
| 00407186 | > E8 45F8FFFF | CALL MrBills.00406900        |         |
| 00407188 | > 59          | POP ECX                      |         |
| 0040718C | > 59          | POP ECX                      |         |
| 0040718D | > 5D          | POP EBP                      |         |
| 0040718E | > E9 D6FEFFFF | JMP MrBills.00407069         |         |

Copying AL  
in a pointer

Copying AL in a pointer

AL 를 pointer 에 복사했다.

**C CPU - main thread, module MrBills**

| Address  | Hex dump                  | Disassembly                                    | Comment |
|----------|---------------------------|--|---------|
| 0040715A | 84C0                      | TEST AL,AL                                     |         |
| 0040715C | · 59                      | POP ECX  |         |
| 0040715D | · 59                      | POP ECX  |         |
| 0040715E | · R2 A0765000             | MOV BYTE PTR DS:[5076A01],AL                   |         |
| 00407163 | · v75 1B                  | JNZ SHORT MrBills.00407180                     |         |
| 00407165 | · FF75 0C                 | PUSH DWORD PTR SS:[EBP+C]                      |         |
| 00407168 | · FF75 08                 | PUSH DWORD PTR SS:[EBP+8]                      |         |
| 0040716B | · E8 ADFFFFFF             | CALL MrBills.00407010                          |         |
| 00407170 | · 84C0                    | TEST AL,AL                                     |         |
| 00407172 | · 59                      | POP ECX  |         |
| 00407173 | · 59                      | POP ECX  |         |
| 00407174 | · R2 A0765000             | MOV BYTE PTR DS:[5076A01],AL                   |         |
| 00407176 | · R2 A2765000             | MOV BYTE PTR DS:[5076A21],AL                   |         |
| 0040717E | > v74 0D                  | JE SHORT MrBills.00407180                      |         |
| 00407180 | > FF75 0C                 | PUSH DWORD PTR SS:[EBP+C]                      |         |
| 00407183 | > FF75 08                 | PUSH DWORD PTR SS:[EBP+8]                      |         |
| 00407186 | > E8 45F8FFFF             | CALL MrBills.00406900                          |         |
| 00407188 | > 59                      | POP ECX  |         |
| 0040718C | > 59                      | POP ECX  |         |
| 0040718D | > 5D                      | POP EBP  |         |
| 0040718E | > E9 D6FEFFFF             | JMP MrBills.00407069                           |         |
| 00407193 | & 56                      | PUSH ESI                                       |         |
| 00407194 | FF7424 08                 | PUSH DWORD PTR SS:[ESP+8]                      |         |
| 00407198 | · 8BF1                    | MOU ESI,ECX                                    |         |
| 00407199 | · 8366 04 00              | AND DWORD PTR DS:[ESI+4],0                     |         |
| 0040719E | · C746 08 010000          | MOU DWORD PTR DS:[ESI+8],1                     |         |
| 004071A5 | · E8 B6E30800             | CALL MrBills.00495560                          |         |
| 004071A9 | · 8966                    | MOU DWORD PTR DS:[ESI],ERX                     |         |
| 004071AC | · 8BC6                    | MOU EAX,ESI                                    |         |
| 004071AE | · 5E                      | POP ESI  |         |
| 004071AF | · C3 0400                 | RETN 4   |         |
| 004071B2 | & 56                      | PUSH ESI                                       |         |
| 004071B3 | FF7424 08                 | PUSH DWORD PTR SS:[ESP+8]                      |         |
| 004071B7 | · 8BF1                    | MOU ESI,ECX                                    |         |
| 004071B9 | · 8366 04 00              | AND DWORD PTR DS:[ESI+4],0                     |         |
| 004071B9 | · C746 08 010000          | MOU DWORD PTR DS:[ESI+8],1                     |         |
| 004071C4 | · FF15 40944B00           | CALL DWORD PTR DS:[<&OLEAUT32.SysAllocString>] |         |
| 004071C8 | · 8C90                    | TEST EAX,EAX                                   |         |
| 004071CC | · 8966                    | MOU DWORD PTR DS:[ESI],EAX                     |         |
| 004071CE | · 8240                    | JZ SHORT MrBills.004071E0                      |         |
| 004071D0 | · 8D4D PTR SS:[ESP+8],EAX |  |         |
| 004071D4 | · 8940                    | SHORT MrBills.004071E0                         |         |
| 004071D6 | · 8F 00                   | JSH 0002000E                                   |         |

OLEAUT32.SysAllocString

AL=00  
DS:[005076A0]=00

The pointer  
will stay zero

Mmmm

The pointer will stay zero

음

Pointer 는 zero 를 유지할 것이다.

| Address  | Hex dump  | ASCII           |
|----------|---|-----------------|
| 00504000 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ...BSI.1EJ.BEJ. |

0012A5D8  
0012H5D0  
0A12Q5F0

C CPU - main thread, module MrBills

| Address                   | Hex dump         | Disassembly                      | Comment |
|---------------------------|------------------|----------------------------------|---------|
| 0040715A                  | • 84C0           | TEST AL,AL                       |         |
| 0040715C                  | • 59             | POP ECX                          |         |
| 0040715D                  | • 59             | POP ECX                          |         |
| 0040715E                  | • 75 1B          | JNZ SHORT MrBills.00407180       |         |
| 00407163                  | • FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |         |
| 00407165                  | • FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |         |
| 00407168                  | • E8 ADFFEFFF    | CALL MrBills.00407010            |         |
| 0040716B                  | • 84C0           | TEST AL,AL                       |         |
| 00407172                  | • 59             | POP ECX                          |         |
| 00407173                  | • 59             | POP ECX                          |         |
| 00407174                  | • A2 A0765000    | MOU BYTE PTR DS:[5076A0],AL      |         |
| 00407179                  | • A2 A2765000    | MOU BYTE PTR DS:[5076A2],AL      |         |
| 0040717E                  | ✓ 74 00          | JE SHORT MrBills.00407180        |         |
| 00407180                  | > FF75 0C        | PUSH DWORD PTR SS:[EBP+C]        |         |
| 00407183                  | • FF75 08        | PUSH DWORD PTR SS:[EBP+8]        |         |
| 00407186                  | • E8 45F8FFFF    | CALL MrBills.00406900            |         |
| 0040718B                  | • 59             | POP ECX                          |         |
| 0040718C                  | • 59             | POP ECX                          |         |
| 0040718D                  | > 50             | POP EBP                          |         |
| 0040718E                  | ^ E9 D6FEFFFF    | JMP MrBills.00407069             |         |
| 00407193                  | ‡ 56             | PUSH ESI                         |         |
| 00407194                  | • FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |         |
| 00407198                  | • 8BF1           | MOU ESI,ECX                      |         |
| 00407199                  | • 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |         |
| 0040719E                  | • C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1       |         |
| 004071A5                  | • E8 B6E30800    | CALL MrBills.00495560            |         |
| 004071A8                  | • 8906           | MOU DWORD PTR DS:[ESI],EAX       |         |
| 004071AC                  | • 8BC6           | MOU EAX,ESI                      |         |
| 004071B0                  | • 5E             | POP ESI                          |         |
| 004071B1                  | • C2 0400        | RETN 4                           |         |
| 004071B2                  | ‡ 56             | PUSH ESI                         |         |
| 004071B3                  | • FF7424 08      | PUSH DWORD PTR SS:[ESP+8]        |         |
| 004071B7                  | • 8BF1           | MOU ESI,ECX                      |         |
| 004071B9                  | • 8366 04 00     | AND DWORD PTR DS:[ESI+4],0       |         |
| 004071BD                  | • C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1       |         |
| 004071C4                  | • FF15 40944B00  | CALL DWORD PTR DS:[%OLEAUT32,#2] |         |
| 004071CA                  | • 85C0           | TEST EAX,EAX                     |         |
| 004071CE                  | • 75 06          | MOU DWORD PTR DS:[ESI],EAX       |         |
| 004071D0                  | ✓ 3944           | JNZ SHORT MrBills.00407180       |         |
| 004071D4                  | ✓ 74 00          | MOU PTR SS:[ESP+8],EAX           |         |
| 004071D6                  | 68 000000        | JMP MrBills.004071E0             |         |
| Jump is NOT taken         |                  | 0002000E                         |         |
| 00407190-MrBills.00407180 |                  |                                  |         |

mmmm

Jump NOT taken when unregistered

Mmmm

Jump NOT taken when unregistered

음

미등록 되었을 때 jump 하지 않는다.

Right ;)

Do you understand that the program will keep "Am I registered or not" in this pointer?

맞아 ;)

Program 은 "등록됐는지 아닌지" 이 pointer 에서 유지할 수 있다는 것을 이해했어?

C CPU - main thread, module MrBills

| Address  | Hex dump         | Disassembly                 | Comment |
|----------|------------------|-----------------------------|---------|
| 0040715A | • 84C0           | TEST AL,AL                  |         |
| 0040715C | • 59             | POP ECX                     |         |
| 0040715D | • 59             | POP ECX                     |         |
| 0040715E | • A2 A0765000    | MOU BYTE PTR DS:[5076A0],AL |         |
| 00407163 | ✓ 75 1B          | JNZ SHORT MrBills.00407180  |         |
| 00407165 | • FF75 0C        | PUSH DWORD PTR SS:[EBP+C]   |         |
| 00407168 | • FF75 08        | PUSH DWORD PTR SS:[EBP+8]   |         |
| 0040716B | • E8 ADFFEFFF    | CALL MrBills.00407010       |         |
| 00407170 | • 84C0           | TEST AL,AL                  |         |
| 00407172 | • 59             | POP ECX                     |         |
| 00407173 | • 59             | POP ECX                     |         |
| 00407174 | • A2 A0765000    | MOU BYTE PTR DS:[5076A0],AL |         |
| 00407179 | • A2 A2765000    | MOU BYTE PTR DS:[5076A2],AL |         |
| 0040717E | ✓ 74 00          | JE SHORT MrBills.00407180   |         |
| 00407180 | > FF75 0C        | PUSH DWORD PTR SS:[EBP+C]   |         |
| 00407183 | • FF75 08        | PUSH DWORD PTR SS:[EBP+8]   |         |
| 00407186 | • E8 45F8FFFF    | CALL MrBills.00406900       |         |
| 0040718B | • 59             | POP ECX                     |         |
| 0040718C | • 59             | POP ECX                     |         |
| 0040718D | > 50             | POP EBP                     |         |
| 0040718E | ^ E9 D6FEFFFF    | JMP MrBills.00407069        |         |
| 00407193 | ‡ 56             | PUSH ESI                    |         |
| 00407194 | • FF7424 08      | PUSH DWORD PTR SS:[ESP+8]   |         |
| 00407198 | • 8BF1           | MOU ESI,ECX                 |         |
| 00407199 | • 8366 04 00     | AND DWORD PTR DS:[ESI+4],0  |         |
| 0040719E | • C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1  |         |
| 004071A5 | • E8 B6E30800    | CALL MrBills.00495560       |         |
| 004071AC | • 8906           | MOU DWORD PTR DS:[ESI],EAX  |         |
| 004071B0 | • 8BCA           | MOU EAX,ESI                 |         |

Right ;)

Do you understand that the program will keep "Am I registered or not" in this pointer ?

and in these pointers too ?

And in these pointers too?

그리고 이것들도 마찬가지지?

C CPU - main thread, module MrBills

| Address  | Hex dump         | Disassembly                 | Comment | Registers                                    |
|----------|------------------|-----------------------------|---------|--|
| 0040715A | • 84C0           | TEST AL,AL                  |         | ERX 0001<br>ECX 0011<br>EDX 0011<br>EBX 0011 |
| 0040715C | • 59             | POP ECX                     |         |  |
| 0040715D | • 59             | POP ECX                     |         |  |
| 0040715E | • A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL |         |  |
| 0040715F | • ~75 1B         | JNZ SHORT MrBills.00407180  |         |  |
| 00407165 | • FF75 0C        | PUSH DWORD PTR SS:[EBP+C]   |         |  |
| 00407168 | • FF75 08        | PUSH DWORD PTR DS:[ESP+8]   |         |  |
| 0040716B | • E8 A0FFFF      | CALL MrBills.00407010       |         |  |
| 00407170 | • 84C0           | TEST AL,AL                  |         |  |
| 00407172 | • 59             | POP ECX                     |         |  |
| 00407173 | • 59             | POP ECX                     |         |  |
| 00407174 | • A2 A0765000    | MOV BYTE PTR DS:[5076A0],AL |         |  |
| 00407179 | • ~75 0D         | JNZ SHORT MrBills.00407180  |         |  |
| 0040717E | • >FF75 0C       | PUSH DWORD PTR SS:[EBP+C]   |         |  |
| 00407180 | • FF75 08        | PUSH DWORD PTR SS:[EBP+8]   |         |  |
| 00407183 | • E8 45F8FFFF    | CALL MrBills.00406900       |         |  |
| 00407186 | • E9 45F8FFFF    | JMP MrBills.00407069        |         |  |
| 00407188 | • 56             | PUSH ESI                    |         |  |
| 0040718C | • 59             | POP ECX                     |         |  |
| 0040718D | • > 50           | POP EBP                     |         |  |
| 0040718E | • E9 D6FFFFFF    | JMP MrBills.00407069        |         |  |
| 00407193 | • 56             | PUSH ESI                    |         |  |
| 00407194 | • FF7424 08      | PUSH DWORD PTR SS:[ESP+8]   |         |  |
| 00407198 | • 8BF1           | MOV ESI,ECX                 |         |  |
| 0040719A | • 8366 04 00     | RND DWORD PTR DS:[ESI+4],1  |         |  |
| 0040719E | • C746 08 010000 | MOV DWORD PTR DS:[ESI+8],1  |         |  |
| 004071A5 | • E8 B6E30000    | CALL MrBills.00495560       |         |  |
| 004071A8 | • 8906           | MOV DWORD PTR DS:[ESI],EAX  |         |  |
| 004071AC | • 8BC6           | MOV EAX,ESI                 |         |  |
| 004071AE | • SE             | POP ESI                     |         |  |

Note that this call is only executed if we are NOT registered  
It could i.e. put the "Unregistered" string

Note that this call is only executed if we are NOT registered

It could i.e. put the "Unregistered" string

등록되지 않았을 때 이 call 은 오직 실행됐다.

"Unregistered" string 을 넣을 것이다.

Now, let's step the code F8

F8 을 눌러서 계속 해보자.

C CPU - main thread, module MrBills

| Address  | Hex dump      | Disassembly                 | Comment | Registers   |
|----------|---------------|-----------------------------|---------|---|
| 0040715A | • 84C0        | TEST AL,AL                  |         | EAX 0<br>ECX 0<br>EDX 0<br>EBX 0<br>ESP 0<br>EBP 0<br>ESI 0<br>EDI 0<br>EIP 0 |
| 0040715C | • 59          | POP ECX                     |         |   |
| 0040715D | • 59          | POP ECX                     |         |   |
| 0040715E | • A2 A0765000 | MOV BYTE PTR DS:[5076A0],AL |         |   |
| 00407163 | • ~75 1B      | JNZ SHORT MrBills.00407180  |         |   |
| 00407165 | • FF75 0C     | PUSH DWORD PTR SS:[EBP+C]   |         |   |
| 00407168 | • FF75 08     | PUSH DWORD PTR SS:[EBP+8]   |         |   |
| 0040716B | • E8 A0FFFF   | CALL MrBills.00407010       |         |   |
| 00407170 | • 84C0        | TEST AL,AL                  |         |   |
| 00407172 | • 59          | POP ECX                     |         |   |
| 00407173 | • 59          | POP ECX                     |         |   |
| 00407174 | • A2 A0765000 | MOV BYTE PTR DS:[5076A0],AL |         |   |
| 00407179 | • A2 A2765000 | MOV BYTE PTR DS:[5076A2],AL |         |   |
| 0040717E | • >74 0D      | JNZ SHORT MrBills.00407180  |         |   |
| 00407180 | • >FF75 0C    | PUSH DWORD PTR SS:[EBP+C]   |         |   |
| 00407183 | • FF75 08     | PUSH DWORD PTR SS:[EBP+8]   |         |   |
| 00407186 | • E8 45F8FFFF | CALL MrBills.00406900       |         |   |
| 00407188 | • E9 D6FFFFFF | JMP MrBills.00407069        |         |   |
| 00407193 | • 56          | PUSH ESI                    |         |   |
| 00407194 | • FF7424 08   | PUSH DWORD PTR SS:[ESP+8]   |         |   |
| 00407198 | • 8BF1        | MOV ESI,ECX                 |         |   |

These will take over AL's job later on

These will take over AL's job later on

이것들은 AL job 을 물려받는 것이다.

C CPU - main thread, module MrBills

| Address  | Hex dump         | Disassembly   | Comment |
|----------|------------------|---|---------|
| 0040715A | • 84C0           | TEST AL,AL  |         |
| 0040715C | • 59             | POP ECX   |         |
| 0040715D | • 59             | POP ECX   |         |
| 0040715E | • A2 A0765000    | MOU BYTE PTR DS:<br>JNZ SHORT MrBills.0040716B      |         |
| 00407163 | ✓ 75 1B          | PUSH DWORD PTR SS:<br>CALL MrBills.0040716B         |         |
| 00407165 | • FF75 0C        | PUSH DWORD PTR SS:<br>CALL MrBills.0040716B         |         |
| 00407168 | • FF75 08        | PUSH DWORD PTR SS:<br>CALL MrBills.0040716B         |         |
| 0040716B | • E8 40FEFFFF    | CALL MrBills.0040716B                               |         |
| 00407170 | • 84C0           | TEST AL,AL  |         |
| 00407172 | • 59             | POP ECX   |         |
| 00407173 | • 59             | POP ECX   |         |
| 00407174 | • A2 A0765000    | MOU BYTE PTR DS:<br>JNZ SHORT MrBills.0040716B      |         |
| 00407179 | • A2 A2765000    | MOU BYTE PTR DS:<br>JNZ SHORT MrBills.0040716B      |         |
| 0040717E | ✓ 74 00          | JNZ SHORT MrBills.0040716B                          |         |
| 00407180 | > FF75 0C        | PUSH DWORD PTR SS:<br>CALL MrBills.0040716B         |         |
| 00407183 | • FF75 08        | PUSH DWORD PTR SS:[TEBP+8]<br>CALL MrBills.00407069 |         |
| 00407186 | • E8 45F8FFFF    | CALL MrBills.00407069                               |         |
| 00407188 | • 59             | POP ECX   |         |
| 0040718C | • 59             | POP ECX   |         |
| 0040718D | > SD             | POP EBP   |         |
| 0040718E | • E9 D6FFFFFF    | JMP MrBills.00407069                                |         |
| 00407193 | ‡ 56             | PUSH ESI  |         |
| 00407194 | • FF7424 08      | PUSH DWORD PTR SS:[ESP+8]                           |         |
| 00407198 | • 8BF1           | MOU ESI,ECX   |         |
| 00407199 | • 8366 04 00     | AND DWORD PTR DS:[ESI+4],0                          |         |
| 0040719E | • C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1                          |         |
| 004071A5 | • E8 B6E30000    | CALL MrBills.004095560                              |         |
| 004071A9 | • 8906           | MOU DWORD PTR DS:[ESI],EAX                          |         |
| 004071AC | • 89C6           | MOU EAX,ESI   |         |
| 004071AE | • SE             | POP ESI   |         |
| 004071AF | • C2 0400        | RETN 4  |         |
| 004071B2 | ‡ 56             | PUSH ESI  |         |
| 004071B3 | • FF7424 08      | PUSH DWORD PTR SS:[ESP+8]                           |         |
| 004071B7 | • 8BF1           | MOU ESI,ECX   |         |
| 004071B9 | • 8366 04 00     | AND DWORD PTR DS:[ESI+4],0                          |         |
| 004071BD | • C746 08 010000 | MOU DWORD PTR DS:[ESI+8],1                          |         |
| 004071C4 | • FF15 40944B00  | CALL DWORD PTR DS:[<OLEAUT32.#2>]                   |         |
| 004071CA | • 85C0           | TEST EAX,EAX  |         |
| 004071CE | • 8906           | MOU DWORD PTR DS:[ESI],EAX                          |         |
| 004071D0 | ✓ 75 10          | JNZ SHORT MrBills.004071E0                          |         |
| 004071D4 | • 394424 08      | CMP DWORD PTR SS:[ESP+8],EAX                        |         |
| 004071D8 | ✓ 74 0A          | JE SHORT MrBills.004071E0                           |         |
| 004071D9 | • 68 0F000020    | PUSH AAA000020                                      |         |

Sorry if all this goes too slow for you. But I imagine this is all somewhat confusing for a starter in reversing. So, I'm trying to explain this all indepth but I promise to go faster in next Parts in this series, assuming you understand all this ....

But it's all clear now  
(I hope)  
Step F8 to continue

But it's all clear now(I hope) Step F8 to continue

이것은 모두 명확하다. 이제 F8 을 눌러 계속하자.

Sorry if all this goes too slow for you. But I imagine this is all somewhat confusing for a starter in reversing.

미안. 모든 것이 너에게 매우 느려졌다. 이것은 reversing 초보자에게 혼란을 준다고 생각한다.

So, I'm trying to explain this all indepth but I promise to go faster in next Parts in this series, assuming you understand all this ....

그래서, 나는 너에게 이것의 상세히 설명하려고 한다. 나는 이 series 의 다음 Part 에서 너는 빠르게 이해할 것이라고 약속한다. 네가 모든 것을 이해한다고 생각한다.

C CPU - main thread, module MrBills

| Address  | Hex dump        | Disassembly                   | Comment |
|----------|-----------------|-------------------------------|---------|
| 00407069 | ‡ B8 03384B00   | MOU EAX,MrBills.004083003     |         |
| 0040706B | • E8 55F00700   | CALL MrBills.0040860C8        |         |
| 00407073 | • 83EC 0C       | SUB EBP,0C                    |         |
| 00407076 | • 883D R1765000 | CHP BYTE PTR DS:[S076A11],0   |         |
| 0040707D | ✓ 0F85 9F000000 | JNZ MrBills.00407122          |         |
| 00407083 | • C605 R1765000 | MOU BYTE PTR DS:[S076A11],0   |         |
| 0040708A | • E8 4B050000   | CALL MrBills.0040750D4        |         |
| 0040709F | • 8810          | MOV EDX,DWORD PTR DS:[EAX]    |         |
| 0040709A | • 88C8          | MOV ECX,EAX                   |         |
| 0040709C | • FF52 0C       | CALL DWORD PTR DS:[EDX+C]     |         |
| 00407096 | • 88C0 10       | ADD EAX,10                    |         |
| 00407099 | • 8945 EC       | MOV DWORD PTR SS:[EBP-14],EAX |         |
| 0040709C | • 8865 FC 00    | AND DWORD PTR SS:[EBP-41],0   |         |
| 004070A0 | • E8 35050000   | CALL MrBills.0040750D4        |         |
| 004070A5 | • 8810          | MOV EDX,DWORD PTR DS:[EAX]    |         |
| 004070A7 | • 88C8          | MOV ECX,EAX                   |         |
| 004070A9 | • FF52 0C       | CALL DWORD PTR DS:[EDX+C]     |         |
| 004070AC | • 88C0 10       | ADD EAX,10                    |         |
| 004070AF | • 8945 F0       | MOV DWORD PTR SS:[EBP-10],EAX |         |
| 004070E2 | • 8045 F0       | LEA EAX,DWORD PTR SS:[EBP-10] |         |
| 004070E5 | • 50            | PUSH EAX                      |         |
| 004070E6 | • 8045 EC       | LEA EAX,DWORD PTR SS:[EBP-14] |         |
| 004070E9 | • 59            | PUSH EAX                      |         |
| 004070E8 | • C645 FC 01    | MOU BYTE PTR SS:[EBP-4],1     |         |
| 004070E0 | EO 1CCCCCCC     | CALL MrBills.0040860C8        |         |

Indeed

Another pointer :)

다른 pointer 다.

indeed

Another pointer :)

C CPU - main thread, module MrBills

| Address  | Hex dump        | Disassembly                   | Comment |
|----------|-----------------|-------------------------------|---------|
| 00407069 | \$ B8 03384B00  | MOV EAX,MrBills.004B3880      |         |
| 0040706E | . E8 55F00700   | CALL MrBills.004B50C8         |         |
| 00407073 | . 83EC 0C       | SUB ESP,0C                    |         |
| 00407076 | . 83D0 A1765A00 | CMP BYTE PTR DS:[5076A11],0   |         |
| 0040707D | ✓ 0F85 9F000000 | JNZ MrBills.00407122          |         |
| 00407083 | ✓ C605 A1765A00 | MOU BYTE PTR DS:[5076A11],1   |         |
| 0040708A | . E8 4B050A00   | CALL MrBills.00407500         |         |
| 0040708F | . 8B10          | MOU EDX,DWORD PTR SS:[EBP-10] |         |
| 00407091 | . 8BC8          | MOU ECX,EAX                   |         |
| 00407093 | . FFS2 0C       | CALL DWORD PTR                |         |
| 00407096 | . 83C0 10       | ADD EAX,10                    |         |
| 00407099 | . 8945 EC       | MOU DWORD PTR SS:[EBP-14],EAX |         |
| 0040709C | . 8365 FC 00    | PNU DWORD PTR SS:[EBP-4],0    |         |
| 004070A0 | . E8 35050A00   | CALL MrBills.00407500         |         |
| 004070A5 | . 8B10          | MOU EDX,DWORD PTR DS:[EAX]    |         |
| 004070A7 | . 8BC8          | MOU ECX,EAX                   |         |
| 004070A9 | . FFS2 0C       | CALL DWORD PTR DS:[EDCX+C]    |         |
| 004070AC | . 83C0 10       | ADD EAX,10                    |         |
| 004070AF | . 8945 F0       | MOU DWORD PTR SS:[EBP-10],EAX |         |
| 004070B2 | . 8045 F0       | LEA EAX,DWORD PTR SS:[EBP-10] |         |
| 004070B5 | . 59            | PUSH EAX                      |         |
| 004070B6 | . 8045 EC       | LEA ECX,DWORD PTR SS:[EBP-14] |         |
| 004070B9 | . 59            | PUSH ECX                      |         |
| 004070BA | . C645 FC 01    | MOU BYTE PTR SS:[EBP-4],1     |         |
| 004070BE | . E8 15FDFFFF   | CALL MrBills.00406D00         |         |
| 004070C3 | . 8045 F0       | LEA EAX,DWORD PTR SS:[EBP-10] |         |
| 004070C6 | . 59            | PUSH EAX                      |         |
| 004070C7 | . 8045 EC       | LEA EAX,DWORD PTR SS:[EBP-14] |         |
| 004070CA | . 59            | PUSH ECX                      |         |
| 004070CB | . E8 01FFFFFF   | CALL MrBills.00406FD01        |         |
| 004070D0 | . 8045 F0       | ADD ESP,10                    |         |
| 004070D3 | . 84C0          | TEST AL,AL                    |         |
| 004070D5 | . H2 A0765000   | MOU BYTE PTR DS:[5076A0],AL   |         |

Oh, not registered, we will jump here

mmmm, so it's all clear for you too ????

Mmmm, so it's all clear for you too ????

음, 너에게 모든 것이 명확해졌어?

Oh, not registered, we will jump here

오, 미등록, 우리는 jump 할거야.

And so finally, we return back to successfully register or not.

Continue stepping

마지막으로, 우리는 성공적으로 등록했든지 아니든지 원래 자리로 돌아왔다.

계속해보자.

C CPU - main thread, module MrBills

| Address  | Hex dump        | Disassembly                    | Comment |
|----------|-----------------|--------------------------------|---------|
| 00429982 | . 59            | POP ECX                        |         |
| 00429983 | . 33DB          | XOR EBX,EBX                    |         |
| 00429985 | . 84C0          | TEST AL,AL                     |         |
| 00429987 | . 59            | POP ECX                        |         |
| 00429988 | . 59            | PUSH EBX                       |         |
| 00429989 | ✓ 75 36         | JNZ SHORT MrBills.004299F1     |         |
| 0042998B | . 59            | PUSH 30                        |         |
| 0042998D | . 6A 30         | PUSH MrBills.004C1370          |         |
| 004299BD | . E8 74270800   | CALL MrBills.004AC138          |         |
| 004299C2 | . 8D8E 20010000 | LEA ECX,DWORD PTR DS:[ESI+120] |         |
| 004299CD | . E8 567CFDFE   | CALL MrBills.00401628          |         |
| 004299D2 | . 8BCF          | MOV ECX,EDI                    |         |
| 004299D4 | . E8 4F7CFDFE   | CALL MrBills.00401628          |         |
| 004299D9 | . 59            | PUSH EBX                       |         |
| 004299DA | . 8BCE          | MOV ECX,ESI                    |         |
| 004299DC | . E8 D5A60700   | CALL MrBills.004A40B6          |         |
| 004299E1 | . 8D8E 7C010000 | LEA ECX,DWORD PTR DS:[ESI+17C] |         |
| 004299E7 | . E8 83D00700   | CALL MrBills.004A6A6F          |         |
| 004299EC | ✓ E9 29010000   | JMP MrBills.0042981A           |         |
| 004299F1 | > E9 40         | PUSH 40                        |         |
| 004299F3 | . 68 50134C00   | PUSH MrBills.004C1350          |         |
| 004299F8 | . E8 3E270800   | CALL MrBills.004AC138          |         |
| 004299FD | . 6A 01         | PUSH 1                         |         |
| 004299F9 | . 8BCE          | MOU ECX,ESI                    |         |
| 00429A01 | . E8 2F8E0700   | CALL MrBills.004A2835          |         |
| 00429A06 | . E8 C1E9FDFF   | CALL MrBills.00408300          |         |
| 00429A0B | . 8BF0          | MOU ESI,EAX                    |         |
| 00429A0D | . E8 C8D00700   | CALL MrBills.004A7500          |         |
| 00429A12 | . 8B10          | MOU EDX,DWORD PTR DS:[EAX]     |         |
| 00429A14 | . 8BC8          | MOU ECX,EAX                    |         |
| 00429A16 | . FFS2 0C       | CALL DWORD PTR DS:[EDCX+C]     |         |
| 00429A19 | . 83C0 10       | ADD EAX,10                     |         |
| 00429A1C | . 8945 F0       | MOU DWORD PTR SS:[EBP-10],EAX  |         |
| 00429A1F | . 8045 F0       | LEA ECX,DWORD PTR SS:[EBP-10]  |         |
| 00429A22 | . 59            | PUSH EAX                       |         |
| 00429A23 | . 8BCF          | MOU ECX,ESI                    |         |
| 00429A25 | . 89            | DWORD PTR SS:[EBP-4],EBX       |         |
| 00429A28 | . E8 3887FDFF   | MrBills.004A5388               |         |
| 00429A2D | . 6A 7E         | PUSH 7E                        |         |
| 00429A2F | . 8045 EC       | LEA ECX,DWORD PTR SS:[EBP-14]  |         |
| 00429A32 | . E8 3887FDFF   | CALL MrBills.0040216F          |         |
| 00429A37 | . 59            | PUSH EAX                       |         |
| 00429A38 | . 8045 F8       | LEA EBX,DWORD PTR SS:[EBP-18]  |         |

Indeed.

And so we know why we will continue to the Badboy!

왜 우리가 계속하면 Badboy 로 가는지 안다.

**C CPU - main thread, module MrBills**

| Address         | Hex dump        | Disassembly                       | Comment |
|-----------------|-----------------|-----------------------------------|---------|
| 004299E2        | • 59            | POP ECX                           |         |
| 004299E3        | • 38DB          | XOR EBX, EBX                      |         |
| 004299E5        | • 84C0          | TEST AL, AL                       |         |
| 004299E7        | • 59            | POP ECX                           |         |
| 004299E8        | • 53            | PUSH EBX                          |         |
| <b>004299E9</b> | ✓ 75 36         | <b>JNZ SHORT MrBills.004299F1</b> |         |
| 004299E9        | • 6A 30         | PUSH 30                           |         |
| 004299E9        | • E8 70134C00   | PUSH MrBills.004AC138             |         |
| 004299E9        | • E8 74270800   | <b>CALL MrBills.004AC138</b>      |         |
| 004299C7        | • 8D8E 20010000 | LEA ECX, DWORD PTR DS:[ESI+120]   |         |
| 004299CD        | • E8 567CFDFF   | <b>CALL MrBills.00401628</b>      |         |
| 004299D2        | • 8BCF          | MOV ECX, EDI                      |         |
| 004299D4        | • E8 4F7CFDFF   | <b>CALL MrBills.00401628</b>      |         |
| 004299D9        | • 53            | PUSH EBX                          |         |
| 004299DA        | • 8BCE          | MOU ECX, ESI                      |         |
| 004299DC        | • E8 D5A60700   | <b>CALL MrBills.004A40B8</b>      |         |
| 004299E1        | • 8D8E 7C010000 | LEA ECX, DWORD PTR DS:[ESI+17C]   |         |
| 004299E7        | • E8 83D00700   | <b>CALL MrBills.004A6A6F</b>      |         |
| 004299EC        | > E9 29810000   | <b>JMP MrBills.0042981A</b>       |         |
| 004299F1        | > 6A 40         | PUSH 40                           |         |
| 004299F3        | • 68 50134C00   | PUSH MrBills.004C1350             |         |
| 004299F8        | • E8 3E270800   | <b>CALL MrBills.004AC138</b>      |         |
| 004299FD        | • 6A 01         | PUSH 1                            |         |
| 004299FF        | • 8BCE          | MOU ECX, ESI                      |         |
| 00429A01        | • E8 2F8E0700   | <b>CALL MrBills.004A2835</b>      |         |
| 00429A06        | • E8 C1E9FDFF   | <b>CALL MrBills.00408300</b>      |         |
| 00429A0B        | • 8BF0          | MOU ESI, EAX                      |         |
| 00429A0D        | • E8 C8D00700   | <b>CALL MrBills.004A75D8</b>      |         |
| 00429A12        | • 8B10          | MOU EDX, DWORD PTR DS:[EAX]       |         |
| 00429A14        | • 8B08          | MOU ECX, ESI                      |         |
| 00429A16        | • FFS2 0C       | <b>CALL QWORD PTR DS:[EDX+C]</b>  |         |
| 00429A19        | • 83C0 10       | ADD EDX, 10                       |         |
| 00429A1C        | • 8945 F8       | MOU QWORD PTR SS:[EBP-10], ERX    |         |
| 00429A1F        | • 8D45 F0       | LEA ERX, DWORD PTR SS:[EBP-10]    |         |
| 00429A22        | • 50            | PUSH ERX                          |         |
| 00429A23        | • 8BCE          | MOU ECX, ESI                      |         |
| 00429A25        | • 895D FC       | MOU DWORD PTR SS:[EBP-4], EBX     |         |
| 00429A28        | • E8 5BB90700   | <b>CALL MrBills.004A5388</b>      |         |
| 00429A2D        | • 6A 7E         | PUSH 7E                           |         |
| 00429A2F        | • 8D4D EC       | LEA ECX, DWORD PTR SS:[EBP-14]    |         |
| 00429A32        | • E8 3887FDFF   | <b>CALL MrBills.0040216F</b>      |         |
| 00429A37        | • 50            | PUSH EAX                          |         |
| 00429A3B        | • 8045 F8       | LEA EBX, DWORD PTR SS:[EBP-18]    |         |

Jump is NOT taken  
004299F1=MrBills.004299F1

:)

**C CPU - main thread, module MrBills**

| Address         | Hex dump        | Disassembly                       | Comment |
|-----------------|-----------------|-----------------------------------|---------|
| 004299E2        | • 59            | POP ECX                           |         |
| 004299E3        | • 38DB          | XOR EBX, EBX                      |         |
| 004299E5        | • 84C0          | TEST AL, AL                       |         |
| 004299E7        | • 59            | POP ECX                           |         |
| 004299E8        | • 53            | PUSH EBX                          |         |
| <b>004299E9</b> | ✓ 75 36         | <b>JNZ SHORT MrBills.004299F1</b> |         |
| 004299E9        | • 6A 30         | PUSH 30                           |         |
| 004299E9        | • E8 70134C00   | PUSH MrBills.004AC138             |         |
| 004299E9        | • E8 74270800   | <b>CALL MrBills.004AC138</b>      |         |
| 004299C7        | • 8D8E 20010000 | LEA ECX, DWORD PTR DS:[ESI+120]   |         |
| 004299CD        | • E8 567CFDFF   | <b>CALL MrBills.00401628</b>      |         |
| 004299D2        | • 8BCF          | MOV ECX, EDI                      |         |
| 004299D4        | • E8 4F7CFDFF   | <b>CALL MrBills.00401628</b>      |         |
| 004299D9        | • 53            | PUSH EBX                          |         |
| 004299DA        | • 8BCE          | MOU ECX, ESI                      |         |
| 004299DC        | • E8 D5A60700   | <b>CALL MrBills.004A40B8</b>      |         |
| 004299E1        | • 8D8E 7C010000 | LEA ECX, DWORD PTR DS:[ESI+17C]   |         |
| 004299E7        | • E8 83D00700   | <b>CALL MrBills.004A6A6F</b>      |         |
| 004299EC        | > E9 29810000   | <b>JMP MrBills.0042981A</b>       |         |
| 004299F1        | > 6A 40         | PUSH 40                           |         |
| 004299F3        | • 68 50134C00   | PUSH MrBills.004C1350             |         |
| 004299F8        | • E8 3E270800   | <b>CALL MrBills.004AC138</b>      |         |
| 004299FD        | • 6A 01         | PUSH 1                            |         |
| 004299FF        | • 8BCE          | MOU ECX, ESI                      |         |
| 00429A01        | • E8 2F8E0700   | <b>CALL MrBills.004A2835</b>      |         |
| 00429A06        | • E8 C1E9FDFF   | <b>CALL MrBills.00408300</b>      |         |
| 00429A0B        | • 8BF0          | MOU ESI, EAX                      |         |
| 00429A0D        | • E8 C8D00700   | <b>CALL MrBills.004A75D8</b>      |         |
| 00429A12        | • 8B10          | MOU EDX, DWORD PTR DS:[EAX]       |         |
| 00429A14        | • 8B08          | MOU ECX, ESI                      |         |
| 00429A16        | • FFS2 0C       | <b>CALL QWORD PTR DS:[EDX+C]</b>  |         |
| 00429A19        | • 83C0 10       | ADD EDX, 10                       |         |
| 00429A1C        | • 8945 F8       | MOU QWORD PTR SS:[EBP-10], ERX    |         |
| 00429A1F        | • 8D45 F0       | LEA ERX, DWORD PTR SS:[EBP-10]    |         |
| 00429A22        | • 50            | PUSH ERX                          |         |
| 00429A23        | • 8BCE          | MOU ECX, ESI                      |         |
| 00429A25        | • 895D FC       | MOU DWORD PTR SS:[EBP-4], EBX     |         |
| 00429A28        | • E8 5BB90700   | <b>CALL MrBills.004A5388</b>      |         |
| 00429A2D        | • 6A 7E         | PUSH 7E                           |         |
| 00429A2F        | • 8D4D EC       | LEA ECX, DWORD PTR SS:[EBP-14]    |         |
| 00429A32        | • E8 3887FDFF   | <b>CALL MrBills.0040216F</b>      |         |
| 00429A37        | • 50            | PUSH EAX                          |         |
| 00429A3B        | • 8045 F8       | LEA EBX, DWORD PTR SS:[EBP-18]    |         |

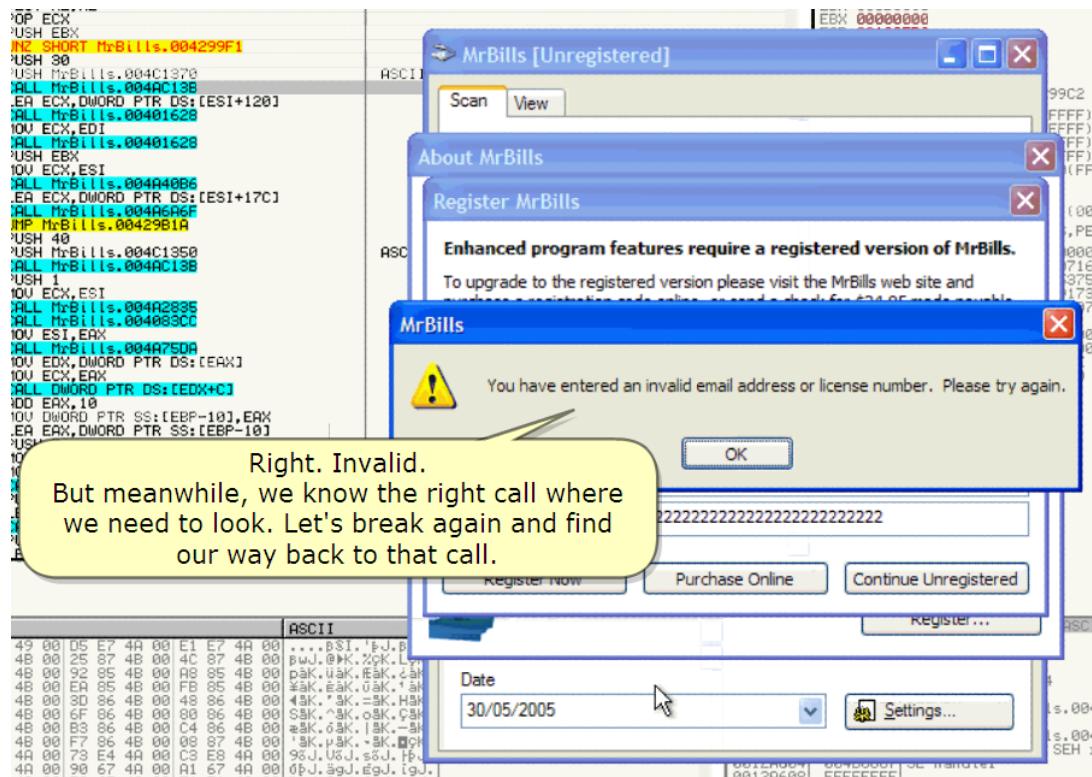
--> not registered.  
Press run to see the result ...

--> not registered.

Press run to see the result ...

--> 미등록

결과를 보기 위해 Run 을 눌러



Right. Invalid.

But meanwhile, we know the right call where we need to look.

Let's break again and find our way back to that call.

정확히. 일치하지 않아.

그러나 그 동안, 우리는 우리가 보기 위해 필요한 정확한 call 을 알았다.

다시 멈추자. 그리고 찾았던 방법으로 call로 가자.

## 5. Patching the program

| Address  | Hex dump    | Disassembly                | Comment                                       |
|----------|-------------|----------------------------|---|
| 00429980 | E8 9AD7FDDF | CALL MrBills.0040714C      |   |
| 00429982 | 59          | POP ECX                    |   |
| 00429983 | 33D8        | WOR EFX EFX                |   |
| 00429985 | 8B          |                            |   |
| 00429987 | 5F          |                            |   |
| 00429988 | 55          |                            |   |
| 00429989 | 75 36       | JNZ SHORT MrBills.004299F1 |   |
| 0042998B | 6A 30       | PUSH 30                    |   |
| 0042998D | 68 70134C00 | PUSH MrBills.004C1370      |   |
| 0042998F | E9 74270800 | CALL MrBills.004AC12B      |   |
| 00429990 | 8D          |                            | ASCII "You have entered an invalid email add: |
| 004299CD |             |                            |   |
| 004299D2 |             |                            |   |
| 004299D4 |             |                            |   |
| 004299D9 |             |                            |   |
| 004299DA |             |                            |   |
| 004299DC |             |                            |   |
| 004299E1 |             |                            |   |
| 004299E7 |             |                            |   |
| 004299EC |             |                            |   |
| 004299F1 |             |                            |   |
| 004299F3 |             |                            |   |
| 004299F8 | E8 9E270800 | CALL MrBills.004C12D0      |   |
| 004299FD | 6A 01       | PUSH 1                     |   |
| 004299FF | 8BCE        | MOV ECX,ESI                |   |

Ok, step in the call (F7)

... to find the right call down in the code.

Ok, F7 로 call 안으로 들어가자.

Code 의 Call 에서 바로 찾을 수 있다.

BTW, I could also press "RUN" because I set a BP there, remember? But I want to show you once more where we found the "guilty" once :))

By the way, "RUN'을 누른다. 왜냐하면 나는 BP 를 set 했다. 기억해? 그러나 나는 너에게 우리가 찾았던 의심스러운 곳을 한 번 더 보여주겠다.

Remember the call we entered before

기억해. 우리는 전에 왔던 call 에 들어왔다.

| CPU - main thread, module MrBills |             |                              |         |
|-----------------------------------|-------------|------------------------------|---------|
| Address                           | Hex dump    | Disassembly                  | Comment |
| 0040714C                          | 55          | PUSH EBP                     |         |
| 0040714D                          | 8BEC        | MOV EBP, ESP                 |         |
| 0040714F                          | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]    |         |
| 00407152                          | FF75 08     | PUSH DWORD PTR SS:[EBP+8]    |         |
| 00407155                          | E8 77FFFF   | CALL MrBills.00406FD1        |         |
| 00407159                          | 84C0        | TEST AL, AL                  |         |
| 0040715D                          | 59          | POP ECX                      |         |
| 0040715E                          | 59          | POP ECX                      |         |
| 00407163                          | H2 A0765000 | MOU BYTE PTR DS:[5076A0], AL |         |
| 00407165                          | 75 1B       | JNZ SHORT MrBills.00407180   |         |
| 00407168                          | FF75 0C     | PUSH DWORD PTR SS:[EBP+C]    |         |
| 0040716B                          | FF75 08     | PUSH DWORD PTR SS:[EBP+8]    |         |
| 0040716B                          | E8 ADFFFFFF | CALL MrBills.00407010        |         |
| 00407170                          | 84C0        | TEST AL, AL                  |         |
| 00407172                          | 59          | POP ECX                      |         |
| 00407173                          | 59          | POP ECX                      |         |
| 00407174                          | A2 A0765000 | MOU BYTE PTR DS:[5076A0], AL |         |
| 00407179                          | A2 A2765000 | MOU BYTE PTR DS:[5076A2], AL |         |
| 0040717E                          | 74 0D       | JE SHORT MrBills.00407160    |         |
| 00407180                          | > FF75 0C   | PUSH DWORD PTR SS:[EBP+C]    |         |
| 00407183                          | FF75 08     | PUSH DWORD PTR SS:[EBP+8]    |         |
| 00407186                          | E8 45F8FFFF | CALL MrBills.004069D0        |         |
| 00407188                          | 59          | POP ECX                      |         |
| 0040718C                          | 59          | POP ECX                      |         |

F7

So, here we are back.

우리는 여기로 돌아왔다.

Continue stepping F8 till the call or press run

F8 을 눌러 call 까지 계속 해.

| CPU - main thread, module MrBills |                |                               |                  |
|-----------------------------------|----------------|-------------------------------|------------------|
| Address                           | Hex dump       | Disassembly                   | Comment          |
| 00406FD1                          | B8 AB374B00    | MOV EAX,MrBills.004B37AB      |                  |
| 00406FD6                          | E8 E0F00700    | CALL MrBills.004860C8         |                  |
| 00406FDB                          | 51             | PUSH ECX                      |                  |
| 00406FDC                          | 53             | PUSH EBX                      |                  |
| 00406FD0                          | FF35 A4415000  | FUSH QWORD PTR DS:[5041A4]    |                  |
| 00406FE3                          | 804D F0        | LEA ECX,DWORD PTR SS:[EBP-10] | MrBills.004BA704 |
| 00406FE6                          | E8 84B1FFFF    | CALL MrBills.0040216F         |                  |
| 00406FEB                          | FF75 0C        | PUSH DWORD PTR SS:[EBP+C]     |                  |
| 00406FEE                          | 8365 FC 00     | AND DWORD PTR SS:[EBP-4],0    |                  |
| 00406FEC                          | FF75 08        | PUSH DWORD PTR SS:[EBP+8]     |                  |
| 00406FF5                          | 8045 F0        | LEA EAX,DWORD PTR SS:[EBP-10] |                  |
| 00406FF8                          | 50             | PUSH EAX                      |                  |
| 00406FE9                          | E8 40FFFFFF    | CALL MrBills.00406F48         |                  |
| 00406FFE                          | 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10] |                  |
| 00407001                          | 88C4 0C        | ADD ESP,8C                    |                  |
| 00407004                          | 83C1 F8        | ADD ECX,-10                   |                  |
| 00407007                          | 8AD8           | MOU BL,AL                     |                  |
| 00407009                          | E8 3AA1FFFF    | CALL MrBills.00401148         | remember this    |
| 0040700E                          | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |                  |
| 00407011                          | 8AC3           | MOU AL,BL                     |                  |
| 00407013                          | 5B             | POP EBX                       |                  |
| 00407014                          | C4:890D 000000 | MOU DWORD PTR FS:[0],ECX      |                  |
| 0040701B                          | C9             | LEAVE                         |                  |
| 0040701C                          | C3             | RETN                          |                  |
| 0040701D                          | B8 AB374B00    | MOV EAX,MrBills.004B37AB      |                  |
| 00407022                          | E8 A1F00700    | CALL MrBills.004860C8         |                  |

Remember this

기억해 이곳?

| Address  | Hex dump        | Disassembly                   | Comment                                  |
|----------|-----------------|-------------------------------|--|
| 00406F01 | \$ B8 AB374B00  | MOV EAX,MrBills.004B37AB      |  |
| 00406F06 | . E8 EC00700    | CALL MrBills.004B60C8         |  |
| 00406F0B | . 51            | PUSH ECX                      |  |
| 00406F0D | . FF35 04415000 | PUSH QWORD PTR DS:[E041104]   |  |
| 00406FE3 | . 8040 F0       | LEA ECX,DWORD PTR SS:[EBP-10] |  |
| 00406FE6 | . E8 941FFFF    | CALL MrBills.0040216F         | MrBills.004BA704                         |
| 00406FED | . FF75 0C       | PUSH DWORD PTR SS:[EBP+C]     |  |
| 00406FEC | . 8365 FC 00    | AND DWORD PTR SS:[EBP-4],0    |  |
| 00406FED | . FF75 08       | PUSH DWORD PTR SS:[EBP+8]     |  |
| 00406FED | . 8045 F0       | LEA EAX,DWORD PTR SS:[EBP-10] |  |
| 00406FF8 | . 50            | PUSH EBX                      |  |
| 00406FF7 | \$ E8 40FFFFFF  | CALL MrBills.00406F4B         | So we decided this is<br>the place to go |
| 00406FFE | . 8840 F0       | MOV ECX,DWORD PTR SS:[EBP-10] |  |
| 00407001 | . 89C4 0C       | ADD ESP,0C                    |  |
| 00407004 | . 89C1 F0       | ADD ECX,-10                   |  |
| 00407007 | . 8AD8          | MOU BL,AL                     |  |
| 00407009 | . E8 9AA1FFFF   | CALL MrBills.00401148         |  |
| 0040700E | . 8840 F4       | MOV ECX,DWORD PTR SS:[EBP-C]  |  |
| 00407011 | . 8AC3          | MOU AL,BL                     |  |
| 00407013 | . 5B            | POP EBX                       |  |
| 00407014 | . 64:8900 00000 | MOU DWORD PTR FS:[0],ECX      |  |
| 00407018 | . C9            | LEAVE                         |  |
| 0040701C | . C3            | RET                           |  |
| 00407022 | \$ B8 AB374B00  | MOV EAX,MrBills.004B37AB      |  |
| 00407027 | . E8 A1F00700   | CALL MrBills.004B60C8         |  |
| 00407028 | . 51            | PUSH ECX                      |  |
| 0040702C | . FF35 A0415000 | PUSH QWORD PTR DS:[5041100]   |  |
| 0040702F | . 8040 F0       | LEA ECX,DWORD PTR SS:[EBP-10] |  |
| 00407032 | . E8 38B1FFFF   | CALL MrBills.0040216F         | MrBills.004BA710                         |
| 00407037 | . FF75 0C       | PUSH DWORD PTR SS:[EBP+C]     |  |
| 00407039 | . 8365 FC 00    | AND DWORD PTR SS:[EBP-4],0    |  |
| 0040703E | . FF75 08       | PUSH DWORD PTR SS:[EBP+8]     |  |
| 00407041 | . 8045 F0       | LEA EAX,DWORD PTR SS:[EBP-10] |  |
| 00407044 | . 50            | PUSH EBX                      |  |
| 00407045 | . E8 01FFFFFF   | CALL MrBills.00406F4B         |  |
| 00407049 | . 8840 F0       | MOV ECX,DWORD PTR SS:[EBP-10] |  |
| 0040704D | . 89C4 0C       | ADD ESP,0C                    |  |
| 00407050 | . 89C1 F0       | ADD ECX,-10                   |  |
| 00407053 | . 8AD8          | MOU BL,AL                     |  |
| 00407055 | . E8 E000FFFF   | CALL MrBills.00401148         |  |
| 00407059 | . 8840 F4       | MOV ECX,DWORD PTR SS:[EBP-C]  |  |

So we decided this is the place to go

이곳에서 결정한다. 들어가 보자.

So step with F7 in the call

F7 을 눌러 들어가자.

| Address  | Hex dump       | Disassembly                   | Comment                         |
|----------|----------------|-------------------------------|---------------------------------|
| 00406F4B | \$ B8 E9374B00 | MOV EAX,MrBills.004B37E9      |                                 |
| 00406F50 | . E8 73F10700  | CALL MrBills.004B60C8         |                                 |
| 00406F55 | . 51           | PUSH ECX                      |                                 |
| 00406F56 | . 8845 08      | MOU EAX,DWORD PTR SS:[EBP+8]  |                                 |
| 00406F59 | . 53           | PUSH EBX                      |                                 |
| 00406F5A | . 56           | PUSH ESI                      |                                 |
| 00406F5B | . FF30         | PUSH DWORD PTR DS:[EAX]       |                                 |
| 00406F5D | . 8045 08      | LEA EAX,DWORD PTR SS:[EBP+8]  |                                 |
| 00406F60 | . 50           | PUSH EBX                      |                                 |
| 00406F61 | . E8 38FBFFFF  | CALL MrBills.00406F9E         |                                 |
| 00406F66 | . 8845 0C      | MOU EAX,DWORD PTR SS:[EBP+C]  |                                 |
| 00406F69 | . FF30         | PUSH DWORD PTR DS:[EAX]       |                                 |
| 00406F6B | . 8365 FC 00   | AND DWORD PTR SS:[EBP-4],0    |                                 |
| 00406F6F | . 8045 F0      | LEA EAX,DWORD PTR SS:[EBP-10] |                                 |
| 00406F72 | . 50           | PUSH EBX                      |                                 |
| 00406F73 | . E8 26FBFFFF  | CALL MrBills.00406F9E         |                                 |
| 00406F78 | . FF75 10      | PUSH DWORD PTR SS:[EBP+10]    |                                 |
| 00406F7B | . C645 FC 01   | MOU BYTE PTR SS:[EBP-4],1     |                                 |
| 00406F7F | . 50           | PUSH EBX                      |                                 |
| 00406F80 | . 8045 08      | LEA EAX,DWORD PTR SS:[EBP+8]  |                                 |
| 00406F83 | . 50           | PUSH EBX                      |                                 |
| 00406F84 | . 8045 0C      | LEA EAX,DWORD PTR SS:[EBP+C]  |                                 |
| 00406F87 | . 50           | PUSH EBX                      |                                 |
| 00406F88 | . E8 89FDFFFF  | CALL MrBills.00406D16         | Aha, this is quite some routine |
| 00406F8D | . FF30         | PUSH DWORD PTR DS:[EAX]       |                                 |
| 00406F8F | . 8875 08      | MOU ESI,DWORD PTR SS:[EBP+8]  |                                 |
| 00406F92 | . 56           | PUSH ESI                      |                                 |
| 00406F93 | . E8 4FF10700  | CALL MrBills.004B60E7         |                                 |
| 00406F98 | . 884D 0C      | MOU ECX,DWORD PTR SS:[EBP+C]  |                                 |
| 00406F9B | . 88C4 28      | ADD ESP,28                    |                                 |
| 00406F9E | . 86D8         | MOU EBX,EAX                   |                                 |
| 00406FA0 | . F7DB         | NEG EBX                       |                                 |
| 00406FA2 | . 1AD8         | SBB BL,BL                     |                                 |
| 00406FA4 | . 89C1 F0      | ADD ECX,-10                   |                                 |
| 00406FA7 | . FEC3         | INC BL                        |                                 |
| 00406FA9 | . E8 9AA1FFFF  | CALL MrBills.00401148         |                                 |
| 00406FAE | . 884D F0      | MOU ECX,DWORD PTR SS:[EBP-10] |                                 |
| 00406FB1 | . 89C1 F0      | ADD ECX,-10                   |                                 |
| 00406FB4 | . E8 8FA1FFFF  | CALL MrBills.00401148         |                                 |
| 00406FB9 | . 804E F0      | LEA ECX,DWORD PTR DS:[ESI-10] |                                 |
| 00406FC1 | . E8 8791FFFF  | CALL MrBills.00401148         |                                 |
| 00406FC4 | . 884D F4      | MOU ECX,DWORD PTR SS:[EBP-C]  |                                 |
|          | . 5F           | POP ESI                       |                                 |

Aha, this is quite some routine

아하, 이것은 꽤 약간 되는 routine 이다.

Let's look down, before the return, where AL is set

Scroll down

밑을 보자. 돌아가기 전의 AL 이 어디에서 set 되는지

Scroll 내려

Mmmm, quite a lot of code.

Code 가 꽤 많다.

For this first time, let's not dig too deep in right away.

첫번째, 정상적인 방법으로 더 이상 깊이 들어가지 않는다.

I suspect somewhere in one of these calls is the verification of the serial.

나는 여러 call 들 중에서 serial 을 검증하는 call 하나를 의심한다.

But that is for other Parts, today, let's patch AL here

다른 part 에서 하기로, 오늘은 AL 을 여기에서 patch 하겠다.

Which explains also the difference with "Advanced level patching" where we would dig deeper till the end :) (See in a later Part in this series)

"진보된 level patching"은 다르다고 설명했다. 우리는 끝날 때까지 깊게 들어갈 수 있다.(이 series 의 다음 Part 에서 보기로 하자)

| Address  | Hex dump       | Disassembly                    | Comment                           |
|----------|----------------|--------------------------------|-----------------------------------|
| 00406F66 | • 8845 0C      | MOV ECX, DWORD PTR SS:[EBP+C]  |                                   |
| 00406F68 | FF30           | PUSH DWORD PTR DS:[ECX]        |                                   |
| 00406F6B | 83E5 FC 00     | AND DWORD PTR SS:[EBP-4], 0    |                                   |
| 00406F6C | 8045 F0        | LEA EAX, DWORD PTR SS:[EBP-10] |                                   |
| 00406F72 | 50             | PUSH EAX                       |                                   |
| 00406F73 | E8 26FBFFFF    | CALL MrBills.00406A9E          |                                   |
| 00406F78 | FF75 10        | PUSH DWORD PTR SS:[EBP+10]     |                                   |
| 00406F7B | C645 FC 01     | MOU BYTE PTR SS:[EBP-4], 1     |                                   |
| 00406F7F | 50             | PUSH EAX                       |                                   |
| 00406F80 | 8045 08        | LEA EAX, DWORD PTR SS:[EBP+8]  |                                   |
| 00406F83 | 50             | PUSH EAX                       |                                   |
| 00406F84 | 8045 0C        | LEA EAX, DWORD PTR SS:[EBP+C]  |                                   |
| 00406F87 | 50             | PUSH EAX                       |                                   |
| 00406F88 | E8 89FDFFFF    | CALL MrBills.00406D15          |                                   |
| 00406F8D | FF30           | PUSH DWORD PTR DS:[ECX]        |                                   |
| 00406F8F | 8875 08        | MOU EST,DWORD PTR SS:[EBP+8]   |                                   |
| 00406F92 | 50             | PUSH EST                       |                                   |
| 00406F93 | E8 4FF10700    | CALL MrBills.0040680E7         |                                   |
| 00406F98 | 884D 0C        | MOU ECX,DWORD PTR SS:[EBP+C]   |                                   |
| 00406F9B | 89C4 28        | ADD ESP, 28                    |                                   |
| 00406F9E | 8608           | MOU EBX,EAX                    |                                   |
| 00406FA0 | F7DB           | NEG EBX                        |                                   |
| 00406FA2 | 1ADB           | SBB BL,BL                      |                                   |
| 00406FA4 | 89C1 F0        | ADD ECX,-10                    |                                   |
| 00406FA7 | FE03           | INC BL                         |                                   |
| 00406FA9 | E8 9AA1FFFF    | CALL MrBills.004081148         |                                   |
| 00406F9E | 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10]  |                                   |
| 00406FB1 | 89C1 F0        | ADD ECX,-10                    |                                   |
| 00406FB4 | E8 8FA1FFFF    | CALL MrBills.004081148         |                                   |
| 00406FB9 | 804E F0        | LEA ECX,DWORD PTR DS:[ESI-10]  |                                   |
| 00406FBC | E8 87A1FFFF    | CALL MrBills.004081148         |                                   |
| 00406FC1 | 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C1]  |                                   |
| 00406FC4 | 5E             | POP ESI                        |                                   |
| 00406FC5 | 89C3           | MOU AL,BL                      | and make BL go dance the samba :) |
| 00406FC7 | 5B             | POPEBX                         |                                   |
| 00406FC8 | 64:890D 000000 | MOADWORD PTR FS:[0],ELX        |                                   |
| 00406FDD | C9             | LEAVE                          |                                   |
| 00406FD0 | C3             | RETN                           |                                   |
| 00406FD1 | \$ B8 AB374B00 | MOU EAX,MrBills.004B37AB       |                                   |
| 00406FD6 | E8 EDF00700    | CALL MrBills.004080C8          |                                   |
| 00406FDB | 51             | PUSH ECX                       |                                   |
| 00406FDC | 53             | PUSH EBX                       |                                   |
| 00406FDD | FE35 04415000  | PUSH DWORD PTR DS:[5041504]    | MrBills.004080704                 |

And make BL go dance the samba :)

BL 을 samba 춤 추게 만들자.

**CPU - main thread, module MrBills**

| Address  | Hex dump       | Disassembly                      | Comment          |
|----------|----------------|----------------------------------|------------------|
| 00406F59 | FF30           | MOV ECX, DWORD PTR SS:[EBP+C]    |                  |
| 00406F5B | 8365 FC 00     | PUSH DWORD PTR DS:[EBP-10]       |                  |
| 00406F5C | 8345 F0        | AND DWORD PTR SS:[EBP-4], 0      |                  |
| 00406F5D | E8 00          | LEA ECX, DWORD PTR SS:[EBP-10]   |                  |
| 00406F5E | 50             | PUSH ECX                         |                  |
| 00406F5F | E8 26FBFFF     | CALL MrBills.0040650E            |                  |
| 00406F60 | FF75 10 FF     | MOV BYTE PTR SS:[EBP+10]         |                  |
| 00406F61 | S8             | PUSH EBX                         |                  |
| 00406F62 | 8045 00        | LEA EBX, DWORD PTR SS:[EBP-41,1] |                  |
| 00406F63 | 83C4 28        | PUSH ECX                         |                  |
| 00406F64 | 8045 00        | LEA EBX, DWORD PTR SS:[EBP+C]    |                  |
| 00406F65 | 8045 F0        | PUSH EBX                         |                  |
| 00406F66 | 8045 F0FFFF    | CALL MrBills.0040650E            |                  |
| 00406F67 | FF30           | PUSH DI                          |                  |
| 00406F68 | 8875 00        | MOV ES:[0], 0                    |                  |
| 00406F69 | 50             | PUSH ES                          |                  |
| 00406F6A | 8840 00        | CALL MrBills.0040650E            |                  |
| 00406F6B | 8840 0C        | MOU ECX, DWORD PTR SS:[EBP+C]    |                  |
| 00406F6C | 8840 28        | ADD ESP, 28                      |                  |
| 00406F6D | 8840 00        | POP ECX                          |                  |
| 00406F6E | F706           | NEG EBX                          |                  |
| 00406F6F | 1AD8           | SBB BL,BL                        |                  |
| 00406F70 | 8840 C1 F0     | ADD ECX,-18                      |                  |
| 00406F71 | FF30           | INC ECX                          |                  |
| 00406F72 | E8 9A91FFFF    | CALL MrBills.00401148            |                  |
| 00406F73 | 8840 F0        | MOU ECX, DWORD PTR DS:[ESI-10]   |                  |
| 00406F74 | 8840 F0        | ADD ECX, 0                       |                  |
| 00406F75 | E8 8F51FFFF    | CALL MrBills.00401148            |                  |
| 00406F76 | 8840 F0        | MOU ECX, DWORD PTR SS:[EBP-C]    |                  |
| 00406F77 | 8840 F4        | POP ECX                          |                  |
| 00406F78 | 50             | PUSH BL                          |                  |
| 00406F79 | 8840 00        | POP EBX                          |                  |
| 00406F7A | 64:8900 000000 | MOH DWORD PTR FS:[0], 0          |                  |
| 00406F7B | C9             | LEAVE                            |                  |
| 00406F7C | 58             | RETN                             |                  |
| 00406F7D | E8 A874E800    | MOU ECX,MrBills.004083           |                  |
| 00406F7E | E8 EDF00700    | CALL MrBills.0040860C            |                  |
| 00406F7F | 50             | PUSH ECX                         |                  |
| 00406F80 | FF35 04415000  | PUSH DWORD PTR DS:[5041041]      | MrBills.00408704 |

I hope you expected something else ???

Assemble at 00406FC5  
MOV BL,1  
will with NOPs

I hope you thought I was going to assemble MOV AL,1 or INC AL ?

I've done this to make you think.  
Let me explain : also at each startup, the code here is executed. But the program starts with AL == 1 (registered !!!)

Exactly here, the program unregisters when not really registered. Try it out for yourself :

```
MOV AL,1
or
MOV BL,1
or
NOP
NOP
```

will all register this program.  
However, if you don't understand all this, never mind, we will see more of this in later parts in this series and eventually, it will all become clear. In that case, just assume I assembled MOV AL,1

I hope you expected something else ???

다른 걸 예상했어?

I hope you thought I was going to assemble MOV AL,1 or INC AL?

네 생각에 MOV AL, 1 이거나 INC AL 로 assemble 할 거라 생각했겠지?

I've done this to make you think.

네가 그런 생각을 하게 만들었어.

Let me explain : also at each startup, the code here is executed. But the program starts with AL == 1 (registered !!!)

설명 해줄께 : 각 startup 은, code 가 이곳에서 실행됐다. 그러나 program 은 AL == 1 일 때 실행된다.  
(등록 !!!)

Exactly here, the program unregisters when not really registered. Try it out for yourself :

정확히 이곳이다. 정말 등록되지 않았을 때 program 은 미등록 됐다. 너는 이렇게 할 수 있다.

MOV AL, 1

Or

MOV BL,1

Or

NOP

NOP

Will all register this program.

이 program 에 등록할 수 있다.

However, if you don't understand all this, never mind, we will see more of this in later parts in this series and eventually, it will all become clear.

그러나, 네가 이것에 대해서 이해가 안됐다면, 걱정하지 마. 우리는 이 series 의 뒤 part 에서 좀 더 볼 거야. 결국 그것은 명확해질 거야.

If that case, just assume I assembled MOV AL, 1

이번 경우는, MOV AL, 1 로 assemble 했을 거라 추정했다.

C CPU - main thread, module MrBills

| Address  | Hex dump         | Disassembly                   | Comment |
|----------|------------------|-------------------------------|---------|
| 00406F66 | • 8845 0C        | MOU ECX,DWORD PTR SS:[EBP+C]  |         |
| 00406F69 | • FF30           | PUSH DWORD PTR DS:[ECX]       |         |
| 00406F6E | • 8365 FC 00     | AND DWORD PTR SS:[EBP-4],0    |         |
| 00406F6F | • 8045 F0        | LEA EAX,DWORD PTR SS:[EBP-10] |         |
| 00406F72 | • 50             | PUSH EAX                      |         |
| 00406F73 | • E8 26FBFFFF    | CALL MrBills.00406A9E         |         |
| 00406F78 | • FF75 10        | PUSH DWORD PTR SS:[EBP+10]    |         |
| 00406F7B | • C645 FC 01     | MOV BYTE PTR SS:[EBP-4],1     |         |
| 00406F7F | • 50             | PUSH EAX                      |         |
| 00406F80 | • 8045 08        | LEA EAX,DWORD PTR SS:[EBP+8]  |         |
| 00406F83 | • 50             | PUSH EAX                      |         |
| 00406F84 | • 8045 0C        | LEA EAX,DWORD PTR SS:[EBP+C]  |         |
| 00406F87 | • 50             | PUSH EAX                      |         |
| 00406F88 | • E8 89FDFFFF    | CALL MrBills.00406D16         |         |
| 00406F8D | • FF30           | PUSH DWORD PTR DS:[ECX]       |         |
| 00406F8F | • 8875 08        | MOV ESI,DWORD PTR SS:[EBP+8]  |         |
| 00406F92 | • 55             | PUSH ESI                      |         |
| 00406F93 | • E8 4FF10700    | CALL MrBills.004860E7         |         |
| 00406F98 | • 884D 0C        | MOU ECX,DWORD PTR SS:[EBP+C]  |         |
| 00406F9B | • 83C4 28        | ADD ESP,28                    |         |
| 00406F9E | • 88D8           | MOU EBX,ECX                   |         |
| 00406FA0 | • F7DB           | NEG EBX                       |         |
| 00406FA2 | • 1AD8           | SBB BL,BL                     |         |
| 00406FA4 | • 83C1 F0        | ADD ECX,-10                   |         |
| 00406FA7 | • FEC3           | INC BL                        |         |
| 00406FA9 | • E8 9001FFFF    | CALL MrBills.00401148         |         |
| 00406FAE | • 884D F0        | MOU ECX,DWORD PTR SS:[EBP-10] |         |
| 00406FB1 | • 83C1 F0        | ADD ECX,-10                   |         |
| 00406FB4 | • E8 8FA1FFFF    | CALL MrBills.00401148         |         |
| 00406FB9 | • 804E F0        | LEA ECX,DWORD PTR DS:[ESI-10] |         |
| 00406FDC | • E8 87A1FFFF    | CALL MrBills.00401148         |         |
| 00406FC1 | • 884D F4        | MOU ECX,DWORD PTR SS:[EBP-C]  |         |
| 00406FC2 | • 55             | POP ESI                       |         |
| 00406FC5 | • B3 01          | MOU BL,1                      |         |
| 00406FC7 | • 50             | POP EBX                       |         |
| 00406FC8 | • 64:8900 000001 | MOU DWORD PTR FS:[0],ECX      |         |
| 00406FCF | • C9             | LEAVE                         |         |
| 00406FD0 | • RETN           |                               |         |
| 00406FD1 | • B8 AB374B00    | MOV EAX,MrBills.004B37AB      |         |
| 00406FD6 | • E8 EDF00700    | CALL MrBills.004860C8         |         |
| 00406FDB | • S1             | PUSH ECX                      |         |
| 00406FDC | • 53             | PUSH EBX                      |         |
| 00406FDD | • FF35 B4415000  | PUSH DWORD PTR DS:[5041B4]    |         |
|          |                  | MrBills.004B37AB              |         |

Of course, we could dig deeper to find where BL is set

but let's try these changes out.

Of course, we could dig deeper to find where BL is set

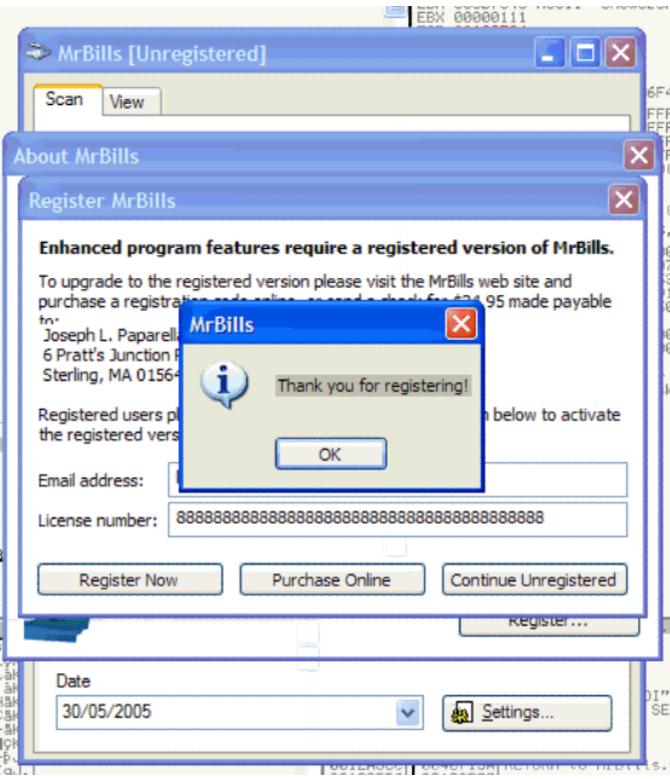
But let's try these changes out.

물론, 우리는 BL 이 어디에서 set 되는지 좀 더 깊게 찾을 수 있다.

그러나 여기에서 바꾼 것으로 끝내자.

For now, give it a go (or F9)

이제, 실행해 보자.(F9)

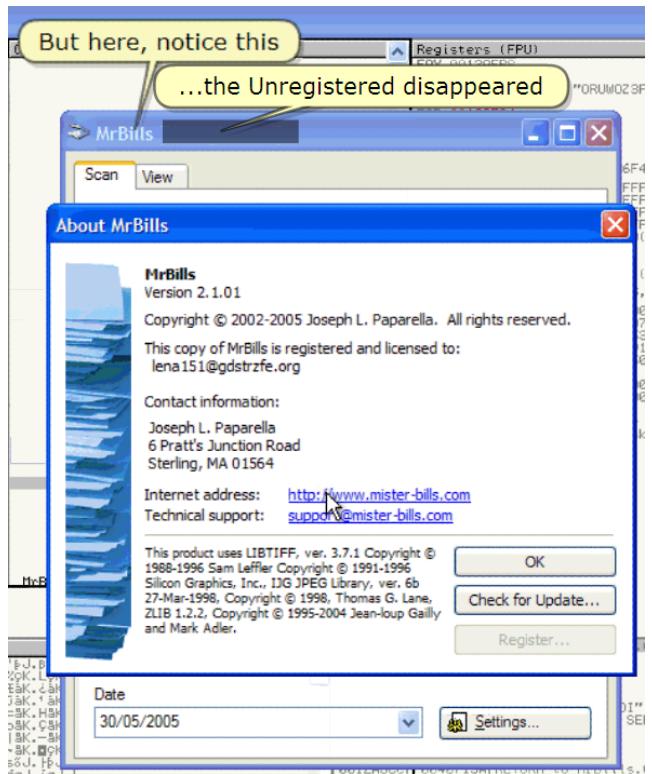


Hehe, how about that ???

헤헤, 어때 ???

Now notice this

이것을 알려준다.



But here, notice this

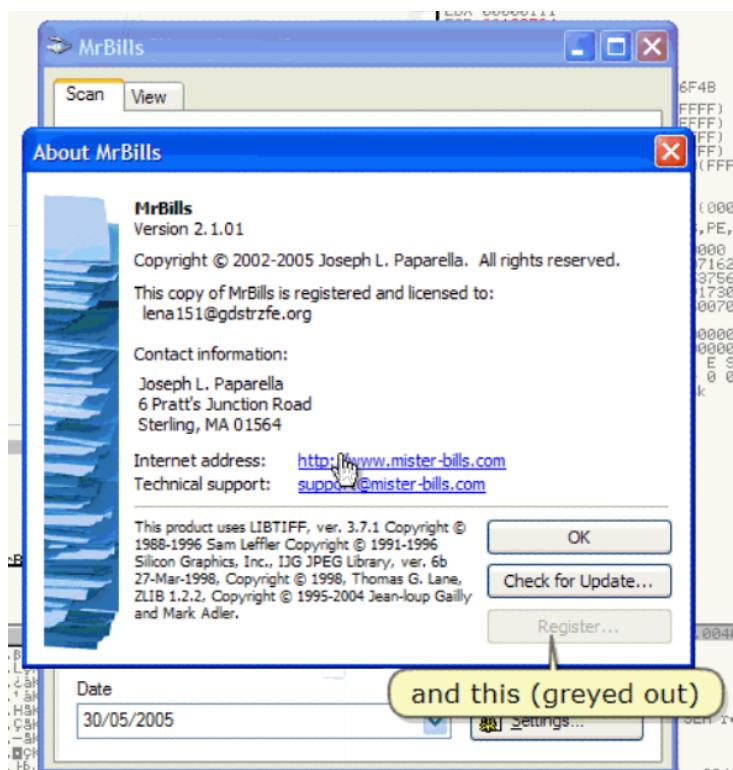
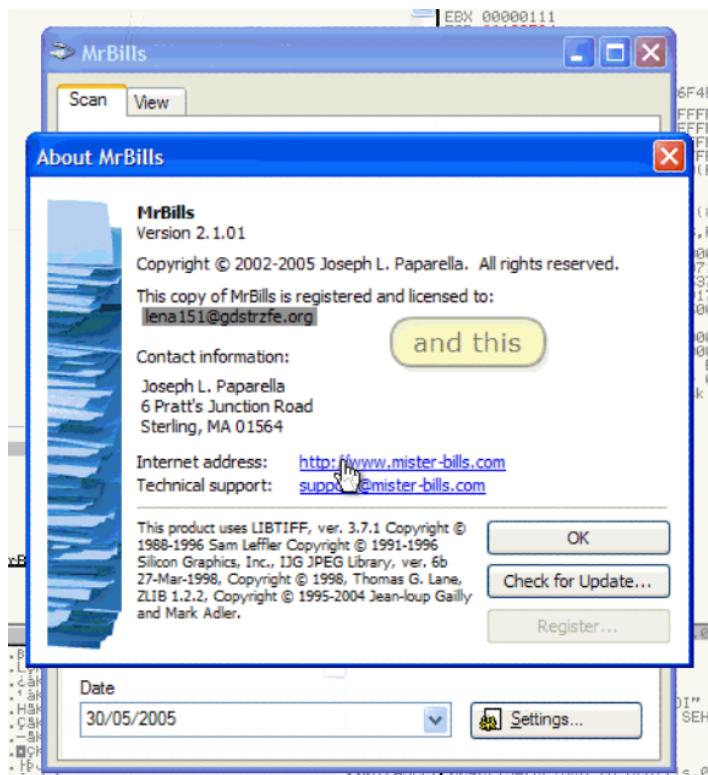
... the Unregistered disappeared

여기도, 알린다.

미등록 되어서 사라졌다.

And this

이것도



And this(greyed out)

이것도(회색으로 바꿔었다)

So, save the changes

그래서, 바뀐 것들을 저장하자.

... under a new name

다른 이름으로 저장해

And try it out

Test 해보자.

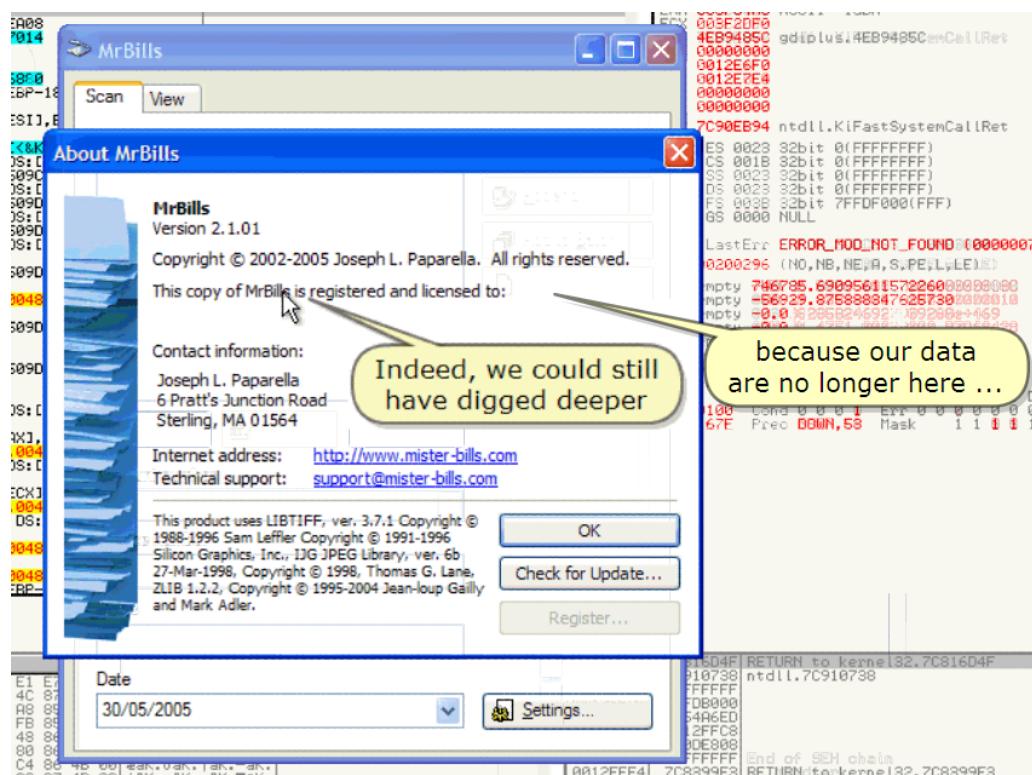
## 6. Testing the patched program

And run the soft

Let's verify the program

부드럽게 실행하자.

Program 을 검증하자.



Indeed, we could still have dugged deeper

정말, 우리는 깊게 팔 수 있었다.

Because our data are no long here ...

왜냐하면 우리의 data 는 이곳에 더 이상 없다.

But see this

이곳을 봐

And this !!!

그리고 여기도

The "Unregistered" has gone !!!

미등록이 없어졌다 !!!

## 7. Conclusion

In this part 7, the primary goal was to study the behaviour of a program's registration scheme and patching it at intermediate level.

이번 part 7에서, 가장 중요한 목표는 program 을 등록하기 위한 행동과 중간 level 로 patch 를 배우는 것이다.

I hope you understood everything fine and I also hope someone somewhere learned something from this. See me back in part 08 ;)

모든 것을 잘 이해했기를 바란다. 그리고 나는 누구든지 어느 곳에서든지 이것에서 무엇이든지 배웠기를 바란다. Part 08 에서 돌아올 것이다

The other parts are available at

다른 parts 는 사용 가능하다.

<http://tinyurl.com/27dzdn> (tuts4you)

<http://tinyurl.com/r89zq> (SnD Filez)

<http://tinyurl.com/l6srv> (fixdown)

Regards to all and especially to you for taking the time to look at this tutorial.

Lena151 (2006, updated 2007)

모두에게 안부를 전하고 특별히 이 tutorial 에 시간을 투자해준 너에게 감사한다.