11.Intermediate patching using Olly's "pane window"

2012년 1월 29일 일요일

오후 7:47

Hello everybody.

모두들 안녕.

Welcome to this Part 11 in my series about reversing for newbies/beginners.

나의 초보자 reversing series Part 11에 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.

Lena151 (2006)

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\*864로 설정해 그리고 full screen으로 movie를 보기 위해 F11를 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 screen을 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.

Movie는 text와 다음 screen을 skip할 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 button과 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 text와 다음 screen을 보기 위해 hotspot을 click해.

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

이 movie 어디에서나 즉시 떠나기 위해 이 spot을 click 할 수 있다.

1. **Abstract**

In this part 11, we will reverse a "real" application to learn something about the use of the "Pane window" in Olly.

이번 part 11에서는, 우리는 Olly에서 "Pane window"를 어떻게 사용하는지 배우기 위해 "real" application을 reverse 할 것이다.

Whilst finding the path to the patches, we will be looking into another reversing in intermediate patching level.

경로에서 patch를 찾는 동안, 우리는 intermediate patching level에서 다른 reversing을 볼 것이다.

This is 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.

좀 더 이해력을 높이고 네가 초보자라면, 너는 이 movie를 보기 전에 이 series의 이전 part를 먼저 보라고 권유한다.

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

이 tutorial의 목표는 너에게 program's behaviour에 대하여 가르치기 위한 것이다.

In my search not to harm authors, I found an old version of Flash Jigsaw producer (version 2.0.0.22) which is no longer available for download.

나의 연구는 제작자에게 해가 되지 않는다. 나는 Flash Jigsaw producer의 old version을 찾았다. 그것은 더 이상 download 되지 않는다.

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

특화된 media를 봐. 나는 이미 "cracked" 된 application을 찾았다.

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

여기, 이 applications은 오직 선택됐다. 왜냐하면 이것은 reversing tutorial에 이상적이다. 그리고 이 target된 것은 오직 교육적인 목적이다.

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

네가 얻은 새로운 지식을 긍정적인 방향으로 이용하길 바란다.

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

문제가 있으면, Part 1를 참조하기 바란다.

1. **Tools and Target**

**이것도 똑같음**

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

오늘의 tools은 : Ollydebug와 너의 두뇌다.

The first can be obtained for free at

먼저 무료로 여기에서 얻을 수 있다.

<http://www.ollydbg.de>

Again, the brain is your responsibility ;)

다시, 두뇌는 너의 책임이다 ;)

Todays target is a program called Flash Jigsaw Producer 2.0.0.22

오늘 target program은 Flash Jigsaw Producer 2.0.0.22로 불린다.

Because it can no longer be downloaded, I have included it in this package for research.

왜냐하면 이것은 더 이상 download 되지 않는다, 나는 이 package에 연구용으로 첨부했다.

1. **Behaviour of the program**

Because you know meanwhile about the importance of decent study of your target and because you've seen how to do it in previous Parts in this series.

그 동안 너의 target에 대한 적절한 공부는 중요했다. 그리고 너는 이 series의 이전 parts에서 어떻게 하는지 봤다.

I will only show you the things we will need to take care of.

오직 너에게 things를 보여줄 것이다. 우리는 조심할 필요가 있다.

As you can see, I have already opened the target program in Olly and in PEiD

네가 볼 때, 나는 Olly나 PEiD에서 이미 target program을 열었다.

REMARK :

This program uses a trick to detect the debugger when run without protection and will exit.

실행할 때는 보호되지 않고 종료될 수도 있다. 이 program은 debugger를 찾는 trick을 사용한다.

It's not the goal of this Part to explain this feature now.

이제 이 Part의 목표는 특징을 설명하는 것이 아니다.

Hence, download the HideDebug or similar plugin for now and extract into Olly's plugin directory.

그리하여, 지금 HideDebug나 비슷한 plugin을 download 받는다. 그리고 Olly's plugin directory에 압축을 푼다.

I'll come back to this extensively in later Parts.

나는 광범위하게 다음 part에서 돌아올 것이다.

<http://www.tuts4you.com/download.php?view.57>

시스템 생성 대체 텍스트: 『｀L, 「In
며．이큼D
爵샅麗雯7鰕컨r르무뿟
驟［층囊紀奪PbljvU·，」
□니니티
RDS:t43드
:X.2
Fi논：C：판ro莩amF'es「廊hJD'aWPro山cer\6producer.exe
PTOR汗PT
RD걘．7FRO
띠劇刃UU乙一
RT「jprodu。．0e42
8000
R【）PTR05:[4353
.8
EntrYP（노nt: ()()()2()38B
EPS손d刃n:
土띠仇拐
Theappha5beenopenedinPeidand
ShOWSUSthls...
tBytes:
辰价n勵劈慤r蠶
펭ORT「Jprㅇd니c.004
:X,뎨를아귑DPTRDS:[
IX.ERX
]ORDPTRDS:tECX】
IORT「Jpr。duc.e04
EqX.니OROPTRDS'
松《．leB
FTf.jDroduㅇ．0e42
ystem:
.teXt
6A,60,68,CS
W納32GLJI
b'cr。＇》什비
C++7.0
MU出
E)dt
l:.20B
因그
므」
...theprogramwas
comPiledinMSVC++7.0

The app has been opened in PEiD and shows us this …

… the program was compiled in MS VC++ 7.0

이 app은 PEiD에서 열었다. 그리고 우리에게 이것을 보여준다.

Program은 MS VC++ 7.0으로 compile 됐다.

시스템 생성 대체 텍스트: ROS:
:t435
【ESI+4」
3「요1-「含
뱉괴凶니囚
ROS:[
:【4352
RDS:【
DS:[435
넌uO.eO4
DS:r435
螺祇霧
File: C
노KAN^LvZ.82
曰二미，겯－
FIle c:'Pr四ramFIles『Ias륭IJi이awPraducer山Produ
王CkC32::0002吟3ㅌO::0042ㅌ3ㅌO
一TSTST
닐POPDP
DS.t435
PrP＇一
EnhPOe
H논Of仕
,,,andthis
(Thㅇughthisis『lot50importantforus『low.I
wi∥alsocomebacktothisirllaterParts...)
DS:【ECX】
'OdUC.e04
》PTRDS'
About
MUltiS
巨Stay
K」니0.0042
닐」UC.0042
슨슨·『「DO-
se.rching...
曰

...and this

(Though this is not so important for us now. I will also come back to this in later Parts …)

We can close PEiD now.

그리고 이거.

현재 이것은 우리에게 중요하지 않다. 나는 나중 part에서 이것을 위해 돌아올 것이다.

우리는 이제 PEiD를 닫을 수 있다.

Ok, always study the soft thoroughly first

I've done that already and will show you the limitation for non-registered

Ok, 항상 철저하고 가볍게 공부해 보자.

나는 이미 해냈다. 너에게 미등록을 위하여 제한을 보여주겠다.

So, run the soft

그래서, 가볍게 실행하자.

시스템 생성 대체 텍스트: .J.먀苞上주dwproduCer《u『뻑沙red)
해ㅃnt-1決。니―靭e陋必·終－디紬，：·
彌驢"心氓헨논
Notethis…갸en띠니R柚－∼er
山）ns
出me。倂
軌얘．야
畛衲a.JPg
…Q圄凶凶
Be戚andsnaam:
Be戚andst蹙en IH戚ureReg
巨Erlab隱Rotation
因eeonty
rRelnofeCon眈혀
佇ㅐelpinPage
一맡巫極丕
Heiq贓 1 1
oUS飇附OU
hnHCJh
nn4夕自44R
66:81384D驪궉
.v75IF
8D48gC
e3cs
81395e45e00e
.v7512
eFB74118
贄nnR슭1슭自n더
ChP盼ORDrTnDC'：ㄷ슴섰：.
JlㅓZ크HOF7「jprㅇduc.oe4
ECX.D이
ECX,ER
미DRD
SH()RT
아砲PTRDS:[E自X＋玖그】
X
PTRDS:【ECX]
fjpr。duc.e04
쏘、勵reg비eredUSerS
-a<-
XE댜＜,뺘ORDPTRDS'IEQ<+18]
FO닛＿InR

시스템 생성 대체 텍스트: 嶼心繃蠟｀tefed．■．,'
肥陸汗뵨醜‘’紆디洙‘'.:－飾rlAr기釉中晄
2
Ad＂솨-,
■■■■■■■■■■■■■■■■■■■■■■■■
-
紀
-'＇무＇「
功eken戚IL」Rash勿SaW飾蠟蹈er
日勿ns-
燿】出me·gif
희勅ow．샷
r】硼ba.JPg
\
Bestandsnaam:lh아ne．夕
B械andst,en l더ctureRes
- 勵＊e-
－一E」 Can헤-
뉵―---!-
- - … I · · 솥
巨EnableRotalion nRem야eCOntr히
佇HeIPinPage
喇h 「푸커－=
－긔NOKe瘢｀tr戡lon
0042043e
0042043드
3e420437
0042e43R
0042043C
ee420442
00420444
白슭4夕슭44只
66:81384D驪궉…ChP
·v75IF IJ뺨42
8B483C n以』
e3CS …RDD
8139드04SeO0e…C"P
.v7512 …JNZ
eFB74118 r1）』Z
숙nnp슭1九녹n더 …「HP
냈戚DPTn以즐：：ㄷ슴샀：.騙
하刃RTrjprㅇd니ㅇ．0042
...andthis
Rrregbteredu，甥sonly
ECX.며柏RDPTRDS'[ERX+3C]
ECX,ERX
PTRDS:【ECX】
fjprㅇduc.
XE댜＜,닌ORDPTR
FQ닛＿1슭P
【EQ샨18]

Note this …

...and this

이것과 이것

Which tells us that the program is crippled

Program은 훼손됐다고 말한다.

INFO :

I'm using "crippled" in the sense of "not all features available while unregistered".

"미등록 되었을 때 사용할 수 없는 모든 기능"에서 "제한" 되어 있다.

It is clear that there are also crippled programs that are never meant to be fully working.

이것은 그곳은 훼손된 program이 있다는 것이 명확하다. 결코 충분히 일하는 것을 뜻하지 않는다.

These are also often called "demo" because this soft can only "show" some of the features whilst some of the (other) features are then simply not coded/implemented.

그것들은 자주 "demo"로 불린다. 왜냐하면 다른 특징들이 간단히 암호화/실행 될 때 이 soft는 오직 약간의 특징들을 보여준다.

Ok. We have all the information we need. So, off to …

Ok. 그래서 우리가 필요로 하는 정보를 모든 정보를 가지고 있다.

1. **Finding the patches**

Now let's return to Olly (click in Olly)

이제 Olly로 돌아가자 (Olly에서 click 해)

I'm sure you already know what I'll be looking for …

내가 찾고자 하는 것을 네가 이미 알고 있다.

시스템 생성 대체 텍스트: L닙＾ 따Ul《Ur쟈b
EDX7C98EB94n鷺d∥.KiFa$ts,'
EBXS000e鱗n
ESP001旣）8F4
EBP0012D9드8
ES!eeeeeZDe
EDI0000000e
SP'e
EIP7C90E894n탭dlLK송F.'tSV뱀
ES0e2332bito(FF「FF「F
CSoelB32b(to(「FFFFFF
SS002332b乙te(FFFFFFF
DS0e2332b(to(FFFFFFF
FSO03B32bLt7FFDF00O(
GS0000「ILjLL
L*'tErrERRI꽈L驢꿸CcESS(
000002461NO.HB.ㅌ，BE.NS,
0·‘e·‘·dpsn긷
CPR헷LSTDO
fO
E님
Lr kF
C아mneflt
Brea跡。「t
텨4trac·
RLIntraC욘
EFL
New驪聊nhere
GOto
Ctrl숴갈ay*
꺼田ad
FOIbw.【）내np
NL
샅t「
굼nC
STOenot딪*77?「FFFeeoeeoeE
STlef뼁）t부-???FFFF000O0Oe〔
STZenpty-？후？FFFF00OeO08E
ST3ehpt,'2？수FFFFDe000000〔
ST4e∥pty..e'＇계쎄ㅑ 〃＊
ST드e叩t,e.0마구환‘- ｀。．
ST6순hpty驪．27478500067:289茫
ST7·＂pt,0.1350997947lC642드
q p ' 山
Sear出拓r
Findre노renC손Sto
V맡W
C아珊toexecU勿바e
At'ajys.
SOOh戚盤
山叫’debuggedPrOCeSS
一 Ma눈山때’ofPrㄸ翩S
Nam톄ab톄「currentf閃山눈Ctd뀨』
Namein체紬山‘e5즌
COfnmand
S旣칟enceofcommands
COnsbnt
B.arystr.g
Ct∥뀨＝
Ctd수S
Ctd용B
이胞
:)
A미＇arance
비탭■［三시■
0012FFC8
OOiZFFCC
OOiZFFDO
O이ZFFD4
e이2F「D8
OO12FFoc
a012FFEO
O012FFE4
OO12FFEB
OO12FFEC
괩九a꿸솝鷺7「「白
7C910738
FFFFFF「F
7「FDB0eo
00000640
00!ZFFCS
8609F780
FFFFFFFF
7C8399F3
7C816［石8
Ooa000eo
枕날노쵸a걀｀날노‘'a
R트쩽캑
n'al'-
…
…
AII「terlnl》蘆」ar
새以rr녑nds
Allseq내軾（es
AllconS勿rlts
수
^j돠威댜난S
스날-
…
EndO
SEha
k.rh·
(
strin댜s
USer뉩e륩nedlab이
USer뉩e륩ned以m「넌nt

:)

The "newbie way" to find what we want. Better and more advanced ways will be explained later.

Stay turned….

"초보자 방법" 우리가 원하는 것을 찾으려고 한다. 좋고 좀 더 진화된 방법은 나중에 설명하겠다.

켜져 있어요….

시스템 생성 대체 텍스트: 더T'extstri雎SrefereγㅉIinfjproduc:.text
口回可
^·ㅁ르
drets
DL$a$$e낟“, Iㅜcㅐ零
尸＿'니FJpro山흩c,004헷‘'O nXll
PUSHfJpr。duc.ee429aFe R이〕11
PU·긺쵱「jpr。d"c.ee4292E쿠 RSCll
PUSH「Jpr。d녀c.ee430360 RSCll
PUSHfJprㅇduc.ee4292DC R竄그I
P냐SH시pr。d니c.0e4292E8 RSCll
PUSHfjOr。duc.0e4292D8 nSCll
PUSH시pr。duc.00430360 nSCll
PUSHfJpr。d니c.ee4292C8 n히〕11
PUSHfJprㅇduc.004292E8 pS（그I
PUSH「jpr。du。，00429804 p戚그I
PUSHfJpr。duc.00429300 RSCll
＂醜〕미刃RDPTRSS:[E얏나ie],「jproduc·OO42nSCll
H以졀며勵戚）PTR55.【ESP+C】.「Jpr。嫩‘C.Oe42엇n허Dll
PUSH「jpr。duc.e0429380 n앗그I
PUSH시pr。duc.004293OC RSC!I
PUSH「jpr。duc.0e429SD4 RSCll
PUSHfjpr。d니c.ee4309ee RSCll
PUSHrjpr。duc.ee4293D0 n5Cll
PUSH「jpr。duc.004293CS nSCll
PUSH「JprㅇduC.0e4293C4 nSCll
PUSHfjpr。duC.ee429388 nSCll
PUSH勺prㅇduC.00429驪（ nSCll
PUSH조Jpr。duc.ee429鮮놈4 R잇Dll
P나SHf,jpr。duc.06429394 R戚그I
P냐SHfjorod니C.0e4292D8 R히〕11
PUSHfJpr。duc.00429388 n5（』1
PUSH「Jpr。d니c.ee4294R4 nSCll
PUSH시pr。duc.0042949e pSCll
PUSH「jpr。d녀c.0042938e p戚그I
PUSH「jpr。duc.e04294R4 pSCll
PUSH「jpr。d니0.0e42947C n竄그I
PUSHfJpr。duc·00429驪긔4 pSCll
PUSH「jpr。du。．ee42946C R히〕11
String
..C:'DㅇC..h'nt술."써
r*''
;)
二츨，'i"d료｀t「、.＇닐β令I
FO馳win蔯955테楓er
'^hn''슬、’>’副，9:．「f＼「jpl'.0d∥ce‘、'$')r’휘Ip
"F。nl"'9ㅎPatr
＂야4ionS"
"C·＼【）OCUn슨nt룔름
"F예lh솥9'''
"Opt．ㅇn''
"Zd"
"C.＼【）卯UnentS릍
"Tran'쵸ti。nㅜL'
"OPttonV'
"S●le。tReuer’뱀
·＇여（'.
"P'OtUreF솥1.'''
"Pl순슬5.in룔ta【I
..1.0.4"
"ZZd各ZZd缶Z4d各Z궉
..datah"
＂낚닐낚．,au＇。「t.c'
.'Z룔＂
"na衲eURㄴ＂
"Z3d"
..TrantTLn."
"COIOrF쵱【【＂
＂汝恪Zd"
"C괵》＄'zestrLng*
.'Z《1"
ter
a\YaVSO*t｀「Jproducer\startup
Se枇小n은xt
Ctrt귀．
E804E34
78899nHB
·■춈뱁■욥.．춈뱁드·■욥뱁프뀀흩
'．츨．■홑．■솥뱀‘.．솝뱀홑.．욥
.'YaVS。ft'f,jpr。ducet\start니p
TOg塋ebr轍po.t
Condbon님brea驕여nt
Con山bon혀bgbrea聯恥t
F2
Shi什수FZ
Sh'ft퓨＝4
Setbrea財納tonev.yα밝r、md
SetbQbre써nnt。neverycommand
COPyto呻board
APpearance
ZCIF7EeFDSF8nOS84Da깊gCE3E<OB
IclclD拓47騁花C8印EZEZ臼E4E6E7톄ECEEEF印8889예8E麗
.'11뱁‘11111111111술‘1''1.'22쵸乙Za乙
292D
2932
"StartLink"
"C。衲pre''Error..
"DataRead'ngErrㅇr"
"1.e.4"
＂歇∥pre$$Err。낟’
"De「【atein'terr。r"
"Co衲pre''Errar"
"D·fLateerror"
締牝柏牝牝牝牝柏牝柏鞠柏牝舵牝貂貂貂4040牝牝牝柏牝柏物4e柏柏柏牝舵牝
쁘盼的盼騁冊애騁騁eeee에oo卵ee的OOee애Oe騁ee에eeeeeeee開ee騁舵eeee韶開

;)

시스템 생성 대체 텍스트: F罕
'．口닙닐'
』■·=‘∼ ＇탭
ter沈XttosearChfof
」口쿄跡驢撤玉
「C邵e功n繃盼e
stringontopof
theWindow
FEnblesc아裙
敞ldr랖별！
- 먀q l cance"-

Remember the string on top of the window

Window의 top에 있던 string을 기억해.

시스템 생성 대체 텍스트: n
T功仗Strin鱗referen騁dinfjprolj
.teXt
톄녜더
nddr슨흖륭
00409999
0040프：'9D7
0040궁qD:
004e3R3e
00403슴4R
004e3R61
00403自72
D요＄a''ehb【y
勵＿ISH'j。1'oc巨石』驪룔30증청4
ㅜC胛t
''＇■솔뿅횹짱홉빻■솝'．춈＇춈＇흩＇쵸＇흩＇홉．■홑맣홑'．홑''＇흩랗욥무．솥맣■솝＇쵸맣‘뿅쵸뺨．춈뺨■솥뺨．춈빻■룝쨍홑＇쵸＇■홑''＇■홑맣｀
Fㅣ＿！〔．H
Fㅣ』l딩H
『IOt』
N以졀
P냐SH
PUSH
anVastst.:.b
C\\\ZCC
＇■욥＇■슴찡홉썅홉'''．솥''＇·욥쟁｀쨍홉쟁홉＇■욥쨍홉＇·욥썅홉＇■욥쨍욥떻·욥＇■솥'It홉썅‘'．욥맬■솥'．욥뺨‘썅i＇■욥멩■욥
SCScSCscScSCScSCScSCSCscSCscSCSCSCSCSCSCSCScSCscSCSCSCSCsc
nnHnHnnppnnnHnHnHCHCHCHnHnHnHnCHCHCLRnHCHppppp
00403n7BPUSH
004e3습98PUSH
00403nR2PUSH
90403自ColPUSH
Oe4O3nC드PUSH
OO403DBS.＂醜룔
00403타궈4"J」
00403F37"OU
00403F87PUSH
Oe403FSCPUSH
00403FDEPUSH
00403「「히래SH
00404384PUSH
00404583!PUSH
0e4043E9PUSH
004e4441
e04e44DC
00404드23
tjpr。duC.ee429Bn4
fjDr。d녀c.ee429B71:
E냐＜.fjpr。duc.0043야石8
ERX,f、jpr。duc.e043驪石8
시pr。d니c.0e430p드8
fjor。duc.0e430R58
시pr。duc.00429B64
fjpr。d니c.e0429B58
fjprㅇduc.00430q58
「jpr。du。·00429B88
fjpr。duc.OO429BIC
E勵＜,「Jpr。d니c.OO42Eige
티枕．fjprodU。．0e42E2n0
E勵＜.「Jpr。d녀c·0042E198
시pr。duc.00429RF8
「jpr。duc.oe429RE4
fjpr。d니c.ee429ROC
rjpr。duc.oe429自CS
「jpr。duc.oe429C드4
「JprㅇduC.0e429C28
fjpr。duC.ee429C00
勺produC.004302E4
티枕．fjpr。duc.oe430lBS
RSC
RSC
nSC
RSC
$tring
"＜∥。Pa$＄낫’
"Err。r"
"InageFLlef。rR*'er＄샅S'den。零Eㅐi$tV'
"C·＼【）醜un슨nt$andSettLng'\Ik\"니ndocunenten"
"c:'Doc니n'nt'andSett'ngt'Ik\"ijn毓》cu飇nt'n"
"c:＼【）。cunent$andSett'ng'\Ik'H너ndocu杓enten"
"c:＼耿）cunentsandSett孔ng''Ik\"ijnd。cu騁nten"
'.CreateDLrect。r,Z'샌
"Dlre。t。r,n。teㅐ''t"
"C:\Docunent$ands순tt딩ng$\Ik\"'Jndocu吟enten"
"CreateDire。t。ryE,r。군’
"Cann。tcreated뜁t·ct。ry"
..OUt"
＂「LhLta"
＇·。Ut"
"Fll놈Lsh.d후＂
"Ready'Sh여‘re'u't수＂
"ooe。＂
n。tcreate「ile
rFL쵸elnfo\Tt슬n룔·
r내驢L〔‘In「。＼204
tingFi!.In「。＼204
0,0,22"
D。cuhent$andSe
DOCunent룔andSe
Sㅇ「첩＼fjDr。d니oer\
Docuheht$ands솥
''
술ti
HZO
HZg
On"
4H\FII슨OescrLpt（。n"
4糾＼ProduCtUet별10。＂
I,시pr。d녀c.0043036e
1.「Jprㅇd니C.ee429Cn4
I,fjpt。d니c.00430lB8
1.fjpr。duc.00429C98
ttin
ttLn
O'
95
'Ik、ㄴ。cal
\Ik\L。cal
부슬V
C:\
棚엶엶
PHll"HH"N
e04e4S3O
004a4또F.
00404572ㅣ
흡零ar零”p.in요＂
tting'\Ik\L。cal
V.vsoft'f,jpr。dla。’r\''
랗‘랗■홑V'＇흩
00404577PUSH
OO4e4667PUSH
004e4679PUSH
OO4O469DPUSH
004046EDPUSH
004047901PU므H
jpr。du
jpr。du
jpr。du
jpr。du
Jpr。du
jp,O蠟·
C.00430350
C.00429여〕4
C.O042EeBS
0.0e4308OC
C.00429CF0
O.Oa42멧re
- r놈r노』,.『노콘닐r노r'
"C:\Docunent$ands숟tti
"fjr"
"0123456789．嫩。de「ghijkL
"-!329144668"
;)
S。ttingt\Rpplic.ti。nD.t.\V.VS。Ft'fjpr。duc.r\.'
SettLng$'ROptL。ati。noata새닐VS。予t'f,jpr。ducer'$tartup
SettLng‘노RpptLcat山nData던7.VS。「t\f,jpr。dUcer\"
驢etting‘노RpPLLcationDat샅｀Va'6。「t＼「，jprodu。er'$tartup
ngCY
"Fla드h
'.FIa딧놀
익9'a니
J”콜맬a닐
ProdUCer"
ProdUOer
轍무슨9용＄ter.dP'
DSDSrTLTfLTf굿f·
EㅌEE

;)

Scroll up to see better

좀 더 좋게 보기 위해 scroll 올려.

Yes! This is what's on the window top

예! 이것은 window top이다.

Doubleclick to go there

Doubleclick 해서 가자.

Now let's see

이제 살펴보자.

And scroll down

그리고 scroll 내려.

시스템 생성 대체 텍스트: 더cPu,耐inthread,mollulefjProduc
슴ddre''
Up,U녹、 γ
004046DE
004046DF
HeHduhD
D쵭sa$$enb료，
r1OP
더OP
Ah히nowstudythlswel-...
Doyouseewhat1see구끄
T·kt="F【a$hJLgs슬낚Pr여汕。슬r"
汕hd=>e82FeZ鮮놈('F【a'hJt''a닐Produc·r1unreg'...',0【a
Set닒tndo닐TeㅐtR
Te닙L＝츠FI솥轍JI''‘·Pr여눕。＊rlu。r·9료＇t。，軟D"
버―긔꺼버
戚 戚 璧
do' 軟 N배
a。 r1OF
8R4424e4 n아」RL,B무TEPTR55:【ESP+4〕
84C8 TESTRL,RL.
7412 JESHORT予jproduc.OO4046FR
R1440R43ee h0U탸楙，며J야큅DPTRDS:t43야놈44]
68FOgC42eo PUSH「Jpr。duc.ee429CFe
드O PUSHEnX
FF!5SC924200CnLL며．하DPTROS.[＜各USER32.S.tULn
C3 RETH
SBOD
44야놀4300畛니ECX,미＇ORDPTRDS:〔43야놀44]
탸멧갸ZO0 lPUSHfJPt여눕c.OO42몃刀8
PUSHECX
55C92420e.
鹹翩톄ECfJ
4730
4736
473R
RTSSL
E무뱀‘ER
L.SPSI亂
REE
588EC28
S6
680CO3438e
68309D420e
ES3DFDFFFF
8B8088E14200
'non
8D442424
드0
5l
ESRO39OZee
8D5424ZC
52
ES6eE2e000
33co
noeCO343eo
83C418
33F6
84Ce
.v7418
》50
ESnnE200ee
83C404
CRLL
RE채
HOP
HOP
더OP
SUB
PUSH
PUSㅐ
PUSH
CrLL
"OV
PUSH
LEn
PUSH
PUSㅐ
CRLL
LER
PUSH
CnLL
XOR
"OU
RDD
XOR
TEST
JES
미J아궉DPTROSt［《各USER32.S.tUIh
hllnd=>OeZF02鮮놈('F【a$hJ(9$a닐Pr。ducer〔unregi...',cla
Set닒LndO니Te써tR
81F3a긷OpO딩
'r큐FC999
ESP.28
ESI
「Jprㅇd니c.ee43030C
칫쁘삑蟾，맸빵貶므챘
'JprO。너O·Up륵덕夔뺙륵b.
습SC!I"-!329144668'.
RSC11"C:'"
ECX.며졀ORDPTRDS:[42E188】
FaU그샅4q샅E따－q·
花기71기71기72題
44444444
,미결ORDPTR55:【ESP+24】
X
X
Drod.C.ee428OD6
ED:<.DU아국DPTR55:〔ESP+ZC]
EDX
「jorod.O.ee4129n6
X
EPTRDS볍【4383eC]
bpa삡컥‘히 1
5구444·一
白→仕p凸U00np仕p仕p쵸p仕p00nUapap白긴ap仕poapoapnUO
444444444444444444444444
n·edp麴pdO0eo仕0000000000쇼Od킵edpd뱁on-
凸UOap00白깊odU쵸p繭p白po色긴eaU00aUeO0aUUn너－
테）RTfjDr。duc.Oe4O4768
PUSHE아엡
驛孔．L「jprㅇdu。．80412n00
RDDESP,4
脈며29CC8=fjpr。duc.eO4ZgCCS(RSCI】"F【a읗h
hLLLbr1Lt쐼Ll의닙L‘님Lesesesesesesesesesse-esesesse---
Jig룔슬닐Pr어緻O슬r〔unregi$tered)")
… 白길눼그ㅡ
一U'-一
「 一I→
-'1"·
。·너－-
ㅓ나ㅎ가1--
－너··、=
→니너一

Aha, now study this well …

Do you see what I see ???

아하, 이제 이것을 공부하자.

내가 보는 것을 너도 보고 있어 ???

In short : ESP + 4 will decide whether jump is taken to …

요약 : ESP + 4는 jump할 것인지 말 것인지 결정할 수 있다.

시스템 생성 대체 텍스트: 더cPLj,m茁社hread,m이lulefjproduc
土ㅐdu叩
90
n흽sa'senb〔，
HOP
NOF'
COn轍ent
0404
qL.타’IEPTR58:〔E斗나ㅓ〕
Rㄴ·RL
SHORTFJprㅇduc.004046Fn
브
타盼、．tlU야괵DPTRDS
H「〕「r。duc.00429C
:[43야겹44]
Fe
태
뎨·
X ㅣ
며出PTRDS볍r（各USER32.S.ttjindOUT순흩
rT탠트＝、＂팃桑L스9동캤．Pr엔힌야r'''
l엥’'P므＝굿u擊＝'’드。ㅒ(-「La'n。I95a닐rr。OUc·r【unregl●··-,cl.
'b슬tUtnCO닐IeHtH
〕D《，D이ORDPTP05:[43OR44]
t구produc.0盼추29CC8
ECX
4험며DPTROS·[<‘냐SER32.S.tU죠ndo닐T
· ■
。r:r한-,「'．뜨饅L스9枓느·Pt으du．헷r(“뜨엣l't'r르dj"
1깻n으므2．므‘'U드硼'-「｀。＄n。Lg＇뭡＂。。니Cer'unreg"··'.cla
솥톄'bet뻐【noㅇ닐1eHtH
TS ㅐㅐL써∥
n닢·나h匕EOUUO삽Ln·
서"TJhPPCRll
9e
9e
흥8R44a404
84CO
.、，74L크
SFR
六〕以
440n43e0
F09C42e0
5C924200…
44翩4沁이
CegC4〔00
thisplace
뱁｀SaDF3BOO닿ㅕ‘rrgyg1UO킬
pZOrOFC·－蠱'OrpFC999
零83EC28
.SUBE
PUSH
PUSH
PUSH
CrLL
엣
ES
0Ce34380
309D4200
3【）FDFFFF
.28
I
pr。d"c.e843030C
pr。duc.oe429D3e
따여눕。．0040446e
.［靭ORDPTRDS:〔42Ei88】
pSC11"-1329144668"
RSC11"C.'"
｀낟·｀닉JX
OD88E14200r1OUEC
6ROR
8D442424
PUSHep
LEnEpX.며J여귑DPTR55:[ESP+24]
PUSHE습X
PUSHECX
CnLL루JPr여눕c.OO428eD'
LEpEDX,DUORDPTR55:[ESP+ZC]
PUSHEDX
CnLLfjpr。l눌。．e64129R6
XORE댜＜.E自X
"OUnL,B무TEPTRDS:[43e3eC]
RD【）ESP.18
X아극ESI,ESI
TESTRL.RL
JES벼꼬Tfjproduc.OO4O4768
rPUSHE댜《
6898BCH
rp6ZOE86
댜LLfJOr여눕。．ea41즈놈oe
RDDESP.4
e a긷 a긴 e
s e e e
e22Cee盼 ee
9 2 38 2
盼24eE凶1 8麗
R4 60046el n
e18脯28沈。3C3F4C4ee
rDr댜EsrpE3ns슴구8찧rSE
·····……갼＞·
EF仕p468D츱‘3^nHapLpb큰훵nLEFn긴349E39BFe뱀‘6nHBa밍27RCEO쨈‘
6D6D6E6E柾6E6E邰6F/r-6F沁柏’P0泌沁泌泌7171기717172譴727273柏祗柏7374稗74겨겨겨花花
444444444계444444444444444444444444444444
柏40柏柏柏犯4e柏牝柏柏柏柏柏牝404040柏盼柏盼柏柏舵柏40柏柏盼柏40404040盼柏40柏柏
0e卵e8卵卵盼恥에觸헨ee帥騁Oe騁애卵盼冊애的觸卵朋舵恥卵觸盼朋卵騁애騁0e卵oeee朋e8
00404756
Ll l 쌩7「q
83c404
DS:[0049On44)=002F023R
Ju"pfro"e04046E6
■自탭닙닙탭■r
■■r 계■·

This place

이곳에 위치해.

시스템 생성 대체 텍스트: 더cpLj-颱inthread,驟업ulefjProd
암넙畛솥·blH촹H
d니枋D
90
1:0「I「．Ent
^IR
ister'IFP
9O
9e
inthe、：
eR44Z4O새
84CO
D룁‘羈senbI,
HOP
N’〕P
더0F'
"l:.IJgL.E''TE
TESTF4ㄴ.nL
:〔E드P+4〕
withthe"unregisterel
WindOWtitle
.·7ㅓ
12
440n43e0
FOgC420e
JESHORT
h0U탸仇．tl
「Jptod
U야국DP
uC.鱗I4O48Fn
TRDS:[49야놀44〕
55C924200
「J'r。d니c.e0429CFe
EnX
며．ORDPTRDS볍[＜各USER32.S슬tULn改》·T버
「e닝t="F【a$hJLgs술．Pr어珊uc슬r"
nlllrld＝》082Fe28R('Fla$hJ'9’、Prγ知cer
S슬t나tnd。“Teㅐtq /
珏nreg'...',O【a
ㅐHL써r
SSLT"
UUO얇Ln
PPCRn
EF仕p468D23n·
印6D柾6E柾枉6E邰6F邙
4444444444
000仕UdpapaUa빕a긴仕p
4444444444
00ap0000O0O
0000hUe凸긴白p轟pe
0040
·탬·嵋뺘송
0044어괘
C89C42
l드5C92
4맣O
現
4a〕U
FC닉，마110RD
」＇
JPUSH
[PUSH
ICr뵙L
RETH
HOP
H아》
"gF
…룝U8
…PUSㅐ
:PUSH
'P냐Sㅐ
Cf(L
:"OV
…PUSH
LEn
PUSH
PUSH
CRLL
LEp
PUSH
CnLL
XOR
:"qp
RDD
…X아극
TEST
JES
rodUㄷ
PTPD읽[4크OR44]
.OO429CCS
PTR05·L＜驢냐SE穴32.S.tUtf놀嫩날T버
ECX
며．며出
[
Teγt="F!a드hJ'9:a니Pto（勿ccr
「．띠n．」=、OeZFOZ鮮경(-Fla$hJ19'
Set닒나뉼do낚T솥ㅐtR
豕而i
玩gted콘
cern'nregi...'.cta
冬88EC28
56
68SCO343ee
68309D42e0
ES3DFDFFFF
SBOD88E14200
'non
8D442424
드0
51
ESRe39e28e
SD드424ZC
52
ES60EZOOee
33C0
noeCO343ee
83C418
33F6
84Ce
.v7418
》Se
ESnnEZO0ee
83C404
ESP.28
ESI
fjprㅇduc.ee43830C
「jorㅇduC.O0429［》3e
fjprt뵤눕。．0040446e
ECX.며JORDPTRDS:〔42Ei88]
On
EpX.며J이귑DPTR55:tESP+24]
EnX
ECX
시Pr여눕c.OO428eD'
EDX,DUORDPTR55:〔ESP+ZC]
EDX
fj마여눌o.ee4129ne
E아《．E自X
nL,B무TEPTRDS:[43O3eC〕
ESP.18
ES】,ESI
RL.RL
테）RTfjoroduc.OO4e4768
댜SC11"-!329l44668''
RSC11''C:\"
EgT嶼D嶼〕244
ED!00000O0e
E!P7CgeEB94r
CO ESOOa큐:
P! CSOolBㅌ
Re SSOe23드
Z! DS0e23뜨
Se FSOe38E
TO GS0e00「
De
oe ㄴa별tErrE
EFL0000024'(
STOeh。t,－수수별
STlef')t,-?？별
STZenpt,－수？설
ST3'npty一？？별
ST4enpt,e.0
ST드이뺑，t,e.0
ST6ehpty7.6'
ST7e叩t,e.i'
ㅓ‘saOFSOBdO쨍‘F乙Jon밍O킹
p'rDFC·－습乙Or댜FC999
· · …、／ · …
「STe120 CㅇnC
FCI·1272 Pr휴C
PUSHE댜《
여LLfJOr여스lo.e0412nse
nDDESP,4
r■■■．■■■■■■■■■■■ r■■■■■■■■■■·■■■■
→너ILp·ㅡr 一EFn깊349E39BFa디ㅓㅗ'nHBn밍27nHCE凸U뱀ㅗ6
沁柏겨泌村쟈仍기71기71717272727273柏松柏花747474겨겨겨花花花忙
444444444444444444444444444444)
仕p什pap仕po仕pape色U仕p0O00apdp00Oapeapdp00ap쇼pOO0a
4444444444444444444444444444444
'[0043eR44】＝002F029n
hpfr。n004046E6
恥開開開開開開oeoe開舵卵朋朋朋腑開觸馝oeoeoe騁0e盼開岬開盼朋얩DS洲

시스템 생성 대체 텍스트: 더cPU-mdin
thread,moduleflproduc
습ddre｀일1HeH
004046E0
004046E4
OO4O46E6
004046E8
004e46ED
004046F2
004046F3
004046「9
·．8·暢＂송
0e40이｀00
l:IO4t:14-0듀
oe‘홍0470b
1:10404-0-
00404‘刀D
0e40470E
0e40470F
ee4e471e
Oe404713
e04047!4
Oe404719
O04O47lE
00404723
00404729
Oe4O472B
0e40472F
00404730
00404731
00404736
0e4()473R
OO4O473B
00404740
00404742
0e404747
0040474R
ee40474C
0040474E
0e4047드0
00404751
004047드6
dunp
90
90
aO
8R44a4
84CO
DLsassenb요，
"OP
텨OP
∥OP
RL,
F4ㄴ
B''TEPTF:58:〔E아＞＋ㅓ」
.R_
1a
440n43ee
Fe9C4200 …
55C92420뻐
HOPT「Jproduc.004O46Fn
탸盼．.tlU야국DPTRDS:[43야겹44]
H「JLr。duc.00429CF0
Te:It
hI〕「．：」
긔
"Fla$hJig＄슬닒Pr여노O슬r"
USHE自X
盼헤團
e82FeZ鮮놈('F【a'hJLg'a닐Produc·r〔ㅗnregi...'.ola
r■■L
PTR
DS볍【＜各USER32.SetUindOUTe얍
SetULndO닐TeHtn
t:.lj까에獄盼
"TJhPPCR
D44硼쎄굶
「89c4「뼉눕
Sscga4ㅀ”-
c28 -
0뎨34880 -
309D4208 -
크旺DEFFF__-
O88E14ZO01
덛멨＇、』 I
"011
F'USH
PUSH
Cr뵙L
REYH
HUP
H아》
＂습「
FC굿，Di,.ORDPTR05:[4沁R441 ·
蠟r乫竺쁜：르＿_____...._.f
U.［차뱁U「IHUblLi毓UbbK珊굡．돕et.LnOO닐I려'
■ ■ - →
兀祗콰’'；橓釜多’衿答。戮d凋쵱넓“麗識
Set뻐LndO"TeㅐtR
즈t른red)"
cㅎr(unregㄴ..'.cla
1멩뱁‘seF3BdO괌‘F乙Oon킬a킹
l(p6rOFCS'Or댜FC999
、
SUBESP.28
PUSㅐESI
PUSH「Jpr。duc.e843830C
PUSHf
‘빽’ · · … O ·하、 · … 令궂 …
r．■■■■■■■■■■■·■■ r■■■■■
．【Lf
觸出
C.00429D3e
o.0048446e
RSC11"-!329144668"
RSC11"C:\"
'888
rp66E
0U
USㅐ
며＇oRDPTRDS:〔42Ei88】
'XJX
0n
EnX.며설이국DPTR55:[ESP+24]
EnX
ECX
fJOr여汕c.Oa428OD6
EDX.DU아극DPTR55:[ESP+ZC]
EDX
fjpr。d·C.ee4129R6
E離귑．E슴났
nL,B보TEPTRDS:[43O3eC〕
ESP.18
ESI,ESI
RL.R【．
HORT「jprodu。．OO4e4768
C"P
52
ES6eEZOOeo
93c0
no0C0343e0
83C418
33F6
84Ce
.v7418
>se
ESRnEZeoeo
83C404
LEn
PUSH
P(JSH
CRLL
ㄸp
PUSH
CRLL
X아극
뺨IOU
RD。
X아극
TEST
JES
PUSHE댜＜
U긔LL「Jpr。duc.ee4!Znee
姃）DESP.4
DS:[0.430n44】=002F023n
Ju"O「rone04e46E6

With the "unregistered" in the window title

Or NOT :)

Window title에서 "미등록" 함께 있다.

또는 없다 :)

Now, what does this tell us ??

이제, 무엇을 해야 하는지 알겠지 ??

시스템 생성 대체 텍스트: 슴ddre$'1HeㅐdU·O
DLsas$enbl,
CO竹ne鞠t
9e
9e
90
言 콰R4
84〔：
EPTF:SS:〔E아냐ㅓ〕
JPr여뗀
0P0PT
O.OO4O46FR
PDg:【49야놈44〕
T■ 一r7lll
、씰궂T ·
ㄴRCXI
[
TS ㅐHLflr
驟隅楷驟PUs鱗
4뱀‘saDF3B츱닐ㅓ‘F히J:UC튕O긷
'rnH6rOFCgbr댜FCq"q"9
>
… …첵｀ · · O ·
-rr∼0468D239
-"비醜6E6E6E6E柾6F邵6F
4'千44444444
넌U枋Iodpeoe什킵白pap
ㅓ빻1444444444
·닙성snpe伋pO0eo
넌UI--10白긴ap0ap0npap
.8404'Fn
OD44Ia슈4
尸미相uc.e04291:Fe l
Eq튕 '
머JOF극DPTROS볍[（各USER32.S.tULndO닐Te졈
a삵．대．ORDPTf굿DS:[4긍OR44】 .
Indeed,PlaceaBP...
aa.,．。。．。do.T“【
T·t=..FLa$hJLgs슬UProduc순r'-
hI■驕d：》eeZF82鮮놈l'Fla'hJ(9’헤Pr氓汕cㅎr【。‘nregi...',0ta
Set비tndo·TeㅐtR
■■■．■ _
T.t="Fta드hJ'9드a니Ptod"cer〔나nrㅎg'즈t·redj"
hI輛d=>eeZFeZ驪경('Fla$hJig’씸P＇여加야r("nr슬引...',cla
Set닒LndO니Teㅐtq
冬88EC28
S6
68SCe343ee
68309D4200
ES3DFDFFFF
SBOD88E!4200
'neR
8D442424
S0
5i
ESRe39e20e
8D5424ZC
52
ES6eE2e000
93co
noeCO343ee
83c418
33F6
84Ce
.v7418
>Se
ESRnE200ee
83C404
rl야ㅑ
H아》
H아＞
SUB
PUSH
PUSH
PUSㅐ
CnLㄴ
『1이』
PUSH
LEn
PUSH
PUSH
CRLL
LER
PUSH
CnLL
X아극
뺨IOU
RDD
XOR
TEST
JES
ESP.Ze
ESI
「Jprㅇduc,ee43830C
fjpr。d니c.0e42903e
'Jpr。l밉O.UU륵盼륵륵6.
ECX.미JORDPTRDS:〔42Ei88】
rp·b겯훵DEFaO
愚UO內U00白p뱁1
r'','rr珊‘
、·4444
댜SC11"-!329144668"
RSC11"C:\"
,뎨를ORDPTR55:【ESP+24]
X
X
Or여囊IC.OO428eD6
騙翩톄ECfJ
EDX,DUORDPTR55:〔ESP+ZC】
X
pro벼·C.e64129n6
.ERX
BVㅜEPTR。S볍[43O3eC】
SSL
탭‘EnH
…
T「jproduc.Oa4O4768
”쭌ESPESI磻
PUSHE아《
댜LLfJOrodu。．0041爵겸oe
姃》DESP.4
EFaO349E3OIBFO쌤‘rpnHB027RCEO16
泌泌기7l기717172租7272花跆緇柏乙747474겨74걔花花75
4444444444444444444444444
려a빕仕pap00仕p仕p仕pnp仕킵aponp仕pape白탭佺papa빕ap000npo仕pnp內긴
144444444444444444444444444444
dpedpapdo습깊eeap0Opod킵O000Oed킵edpeee쇼pdp쇼po
너apdpap00仕깊dOO乙po白．e色긴apa긴oapoapO什pap00ap0Oapo
DS:[0.43OR44]=O02Fe23n
Ju"p「rone04046E6
■■■■■■■■■■「

Indeed, place a BP…

BP를 설치해...

Here by doubleclicking the opcode

Opcode를 doubleclick 해.

And re-start the app

그리고 app을 re-start 해.

And re-run

그리고 재시작 해.

We land at our BP

우리는 우리의 BP에 도착했다.

Scroll up a little to see clear ;)

명확히 보기 위해 scroll을 약간 올려 ;)

And study the code here.

여기 code를 공부해.

시스템 생성 대체 텍스트: He씨ewDebugPbghsOP加隅∥l,d
꾀뾔꽈－의꾀－뾔」쐬뾔스
더cPu-臘inthread,modulefjpro
旦의」邸셥劃최
「一
口回因
숱노r．룝홑
百聊福4乙莎珊
0e4046DB
ee4046OC
0040461)D
e04046DE
幷a4白4蝦n「
洲np
D룁룔흡튜senb밸
rmassumingyㅇu
UnderstandthatAL
deddesonjumPingto
unregisteredornot.
^IR
AL==O--->
nL.
PTR55.[ESP+4]
D^Ut'
J가―-―澈뾔崗기딨뵈―-
··갼··…＞·…
r．■■■■■■■■■■■■■■
n.-.4더수
4·‘sa팅F3
7R6r구FC
9e
9e
9e
90
9e
90
8댜4424e4
84C0
혔．nL.
4히王
46〔프
4딧EE
46「돝
4히_
45F9
46FR
47Oe
4705
4706
470C
470D
470E
470F
4710
12
440R4300
FO9C4209
r40F
HOP
HOP
＂아’
HOP
HDF'
＂以，
TEST
JES
＂醜룔
PUSH
聊欌綴殲撰撈勸4]
'JprOOUC.UU，乙젯차rU)
baㅃ맨노7
Andinit$tum,ALIS
setbythevaluefor
thepointerㅌSP+4
C산r"
쁘륫H택L-______』＿.'______...._Tl닌）「r’ㅜ벧LL_
Lㅏ룁LU.UN』r＂뺑UbIL（松UbbK礪괩·돕etUtnOO닐I샅활'》촹볍뺘＂놀00낚I솬HtH
RE맣h
SBeD
5C9242Oe
44야궈43Oe
뺨loV
C89C429e
ECX.[MORDPTRDS.【43야놈44]
fjpr。d녀c.0e429CC8
="Fta$hJLg＄홉UPr여노cer(니nreg暢tered)"
ECX
。UI】RDPTROS:r<'UBER92.S．티JindO나T·目
〔硼
'b.t뺘
=>HULㄴ
LndO닐T.HtR
8·‘F3a긷eo
6r구FC999
冬83EC28
ESP,28
ESI
uSHUSH없대oPOPDPUSUSH
PPCR"""SP
0C034300
3畔며珊p
3DFDFF'
PUSH「Jpr。duc.0043030C
힘蟾‘느‘‘·－'｀∼의닙긔눕D30
RSC11"-!329144668"
습SCll''C:\"
4723
4,29
472B
■.SBeDe8E
■·600p
■.8D44242
NOticealso
thatthepointer
ESP+415irlthe
42ㅌ】es〕
ESP+24]
EnXFFFFFFOe
EQ《FFFFFFFF
EDX00430385自SCll"hoPa즐＄>"
E타＜000808eo
ESP001ZEeZe
EBPOO12E0nC
ES!00000eeC
ED!0012FD18
E!P804046Ee「jpr。d니c.004046E0
Ce ESee2332b요to【FF「FF「FF)
P! CS00IB32bito(「FF「「「「「）
R! SSee2332b요to(FFFFFFFF)
Ze DS0e2332b(to(FFFFFFFF)
Se FSee3B32b쵸t7FFDF00O(FFF)
Te GS0eoeNUㄴㄴ
De
Oe L'$tErrERR()fLSIJCCESS《0O00e000)
EFL00200216(NO,HB,HE,R,NS.PE.GE,G)
STOenpt딪-???FFFF0004e404000404e4
STI더뺑）t,一？??FFFF00000000eOO40404
STZehpty-???FFFFe0040404ee040404
ST3.hpt,一？??FFFF0000000000040404
ST4enptye.e
STSenpt,e.e
ST6ehptye.e
ST7el'pt날e.e
32le ESPUOZ
「ST0000 Cㅇnde00e Err0ee0Oe
F（겨1272 PrecNERR,53 "a$k i1ee
6885
r구6'E
· …
■■■■■■■■■■■■■■
JL■，■■．'■■눕■，탭r
쵸O49E
뺑홑·‘1홑뱀l
77'r,r
4444
nU仕킵n힙n빕a밍n깁n틸n깁nU自UnUnUn킵npn킵nUn킹n킬a빕nU仕Dn킵·
44444괘빻4444444444444444t
dpoaOO凸Oap凸OaUnoaUapd긴apnoenUaUapdOO凸UaO--.
d긴apoapo白pn털npeeapeoeO쇼Uea긷oaUOO－너
YㅇUCan
Seethatin
(Stack)address
OO12EO24
ESP+ZC]
thepane
window
3e3OC】
Oel．뺨「탬「
Oe4O474E
組叩「鮮’,1冬
rX마극ESI,ESI
iTEST믿，nL
…JESㅐt)RTfjpr
Staok
RL』e
LㅇCa견
55:【0O12E024〕＝00
ㅜhebytethe
poirlterpoints
tㅇisalready0O
a【【름흙to衲004047D3.鱗》4048
[FF
匕L〔
「劇mfJO玆》d녜O,
스
R앗그I"(NOPa'!>"
「1'1ㅁi-.)'ljl긔k..U“「出－U
긔
一 ' ㅑ…_ ·F 옵j「｀ -
하‘숫＝D ·- 14-ㅗ
OnInl'.=…－· ·
麗汪麗正兀魂I止r
l맬■홑‘쫠스．■홑．■솥.．홑괌1'·■ㅗ.1■＊’■ㅗㅓ
n幢幟隅댜H
^·麗一
Anclthebyte
thepointer
point$tㅇiS
already00
IB,p놀B,令놉B,
죤汕8.》눔B.0摹B,
-----－떽盼.
SOfarthePane
Window,butwecan
alsc)lookitupinthe
dumpWindow
VFr매·巨
WhilstalsㅇAL
isalreadyzerㅇ
0C
0'
04
白U7
'1.
冬1.
'1
니
l랙
길v찮슴一룐＇｀컁
0042E0B0
0e42E0C8
0e42E0D0
e042EOES
na'1伊「n「n
e01驪05이畛
0012E0541 SB
000110
IC!B70
Opqr룔tuv·뒤VZ...·
繃｀'B......？댔｝CRt·
4nn輟l「＂츤겹룔＾f즐^".OT·山山
0012Ee58
001ZEe5C
0012E060
00408F!C
001ZFD18
0040SEC0
uHthene.SBlc1B7e
RETUR쳐t。勺pr。duc.O04OSFICft。∥f,jpr。出‘c.00404710
fjproduC.OO4OSECO
n킵In
白U44
03r
nU44
걔弱댄
ㄴ驪442 ㄴ졈6744
盼盼盼騁애엣쁘뻗미엔헤盼6676盼觸
牝42애紇애盼鉀맺미-.；碣盼6S花ee蝕
U白p44e4
U06707
딩033e더
VaO6787
깊e22e<
일e67e蝦
딩aU쨈‘''Zq
일仕p'74'
'仕pgeE요
·037n7
·n디SF4U
닐03684

I'm assuming you understand that AL decides on jumping to unregistered or not.

AL == 0 ---> badboy

AL이 jump에서 미등록 됐는지 등록 됐는지 결정한다는 것을 이해할 거라고 생각한다.

AL == 0 ---> badboy

And in its turn AL is set by the value for the pointer ESP+4

AL이 바뀌는 것은 pointer ESP+4의 값에 의해 set 된다.

You can see that in the pane window

너는 pane window를 볼 수 있다.

Notice also that the pointer ESP+4 in the (stack) address 0012E024

Stack address 0012E024에 ESP+4 pointer가 있다.

And the byte the pointer points to is already 00

Byte pointer는 이미 00을 가리킨다.

The byte the pointer points to is already 00

Byte pointer는 이미 00을 가리킨다.

Whilst also AL is already zero

또한 al은 이미 zero다.

So far the pane Window, but we can also look it up in the dump window

지금까지 pane Window를 살펴봤다. 그러나 우리는 dump window에서 볼 수 있다.

시스템 생성 대체 텍스트: 우0
98
9e
9e
9e
9e
sr"424
더CpU-脫inthread,
奫굻빎些…
m繃uleflproduc
004046DB
nn4n4八n「
004046DD
e04046DE
l1，〕4너，퀼卜Dㄷ
〔1040돈
너．'4llh
84c8
4더4F
ellee仕킹eo룅
CPaHILSTDO
12
440R4300
「09C4200
D룁‘흡’senbl,
HOP
HI:iF'
r샐OF'
"OF'
HOP
HDF》
"J,nL.·八EPTRS훠tESP+4]
TESTnL..nL L>
JES테ㄳT「Jprㅇduc.'b功4046「R
"OU티긔X.며＇ORDPTRDs:〔430R44】
PUSH「Jpt。duc.Oe429C「O
h.'nt ^
n헴
ER님
EO쐽
EDX
EBX
ESP
EBP
ESI
EDI
EIP
="F!a$hjt'’魯니Pr여노。솬r"
'》HLjLㄴ
-―그耳―---l
1드5C924290
PUSㅐERX
CnLL며．하D
RET꺼
PTRDS찧t＜各USER32.SetUind。닐T텨
『rex零
l떼U.d
'S솥t비
LndO낚T솥ㅒt슴
4·‘seF3
쨍rR65FC
SBOD44鮮궈43Oe
68C89C42e0
5l
FF155C924200
C3
9e
9e
9e
ECX.山룔ORDPTRDS딥[43야놈44]
f,jpr。duc.ee429CCS
뜨生＿________..______ ... . _lI쁘n브
。．UHU「'HUb:L<'UbbH珊귑급騙．옇U'ndo닐I·目'b층t뻐
므"FLa$hjig＄홉UPro＜노cer(니nregi$ter.d)"
=>HULL
L혀’슬낚Te닝tR
冬83EC28
56
680C034300
693OgD42ee
ES3DFDFF「F
SBOD88E!42Oe
6Rop
8D442424
5e
5i
ESneSgeZee
SD드424Zc
52
ES60E200e0
33ce
ReeCO343ee
83c418
33F6
84C8
.v74IB
뺨1대』
PUSH
PUSㅐ
CRLL
REY꺼
HOF》
HOF》
HO죤
SLjs
PUSH
PUSH
PUSH
CnLL
"OU
PUSㅐ
LER
PUSㅐ
PUSH
C「ILL
··갼··…＞·…
r．■■■■■■■■■■■■■■
ESP,28
ESI
!NF○:
EFL
STe
첵쵯
fjpr。d니
「Jpr。d니
루．】p戚X눕
C.0043030C
C.00429D30
4··=r'239RO드6CDEF0349F
EF"E’」FFFF000apo仕p01llii
U66'b67'，·"r7"r7rr7렇r77뺐r
44444444444444444
ECX.며솥아귑D
.며를ORD
×
X
004。446.
PTRDS:t42E!85〕
PTR55:〔ESP+24】
473n
473B
LERE
PUSH
Cr룁L
X아국
『10V
RDD
XOF귑
TEST
JES
pnX눌0.ee428e06
.아룔아국DPTRSS:[ESP+ZC】
X
아혀눌O.ee4129Re
.ERX
머’TEPTRDS'[43O3OC】
.18
,ESI
,qL
Tfjpr。du。．00404768
AmomentagO,lwrotethathere,the
unregisteredteXt15writteninthemain
window(or『lot).HㅇwdoIknㅇwthat71fyou
dㅇubtaboutsㅇmething,TAKEALOOKin
Win32.h-p(abouttheAPlls,remember?).
Althㅇugh1thinkit15clearwhatthisAPIdoes。
(SeepreViㅇuspartsinthisseries).
翩翩EPEcfJ嘶EDfJ翩L.SPsl亂매
r' E E쵸Hr드E H
39BFe16
褪7272組柏73跆
4444444
apZ면r貧CE
444444
55:[eolZE024」=00
Oa【！름흙t。衲004047D3.00404880
鬱貯鬱47貯47'kol
刊舵牝牝牝牝牝舵牝柏物舵柏舵牝舵柏牝舵犯柏舵柏舵牝牝牝盼柏犯柏媤‘鄒쾌ca
困l-lC騁卵觸卵開開觸四開卵的애騁卵舵開卵開開騁舵觸ee騁oeee開ee觸卵沁꼴St亂Lo

INFO :

A moment ago, I wrote that here, the unregistered text is written in the main window (or not).

약간 전에, 나는 이것을 썼다. 미등록 test는 main window에 저장되어 있다.(아니거나)

How do I know that? If you doubt about something, TAKE A LOOK in Win32.hlp (about the API's remember ?).

내가 어떻게 아는가? 무언가를 의심한다면, Win32.hlp를 살펴 봐.(API's에 대하여 기억해?)

Although I think it is clear what this API does. (See previous parts in this series).

이것은 내 생각이지만 이 API가 하는 일이 명확하다.(이 series의 이전 parts를 봐라)

시스템 생성 대체 텍스트: … -- ……
더cPU,颱inthread,釀넌ulefjProd
습ddre''1HeHlu"p
COhnent
C■ ㅡ ㄲ
L· ㅡ P
7v.p녹gUh
0e404邵IB
슴O써녹4蝦OC
0닌404匕DD
UU404미IE
OO404BDF
EOU
J"P
뺑‘Far)a긷eo킹
5FC999
…
0e40’拓E｀추
이〕4046「E
004046EE
너0404bEO
004046F2
004046F3
004046F9
004046FR
00404700
0e404705
0e404706
0040470C
004e470D
004047OE
0040470F
e0404710
00404713
e04a4714
004047!9
eO40471E
00404723
004e4729
0040472B
004a472F
0040473e
00404731
00404796
0040473n
0e40473B
0e404740
Oe404742
00404747
0040474R
0040474C
e040474E
9O
닉‘1
닐니
90
98
9O
후e슈“2404
84C8
.v7412
R1440n4380
'8「OgC42ee
드e
I미”%e沁냐
HOP
허OF'
더OF'
HOP
HI)P
HOP
I＂여，nL.驪八E
…TESTRL..nL.
S냈尸ㅜfjprㅇdu
兀
臼P+4]
4046FR
nX,山솥ORDPTRDS:〔43解枓4]
(Jpr。duc.Oe429CFO
="F【．'hJLg'a눠Pr여汕c.r''
PUSㅐ
「F155C9242e이야룁L
C3 REr"
PTRDS:t《各USER32.S.tUtn
:>HLjLㄴ
나놀do닐T솥ㅐtR
>SBOD44eR43Oe…hOUECXr
.'8C89C42ee …PUSHfjp
DPTRDS.L43야놀44]
''0e429CC8
…PUSㅐECX
1드5C9242Oe'凶Lㄴ며．ORO
REr써
:r《各USER32.S.tUindㅇ니T.:
Text="F1.'hJ19'a닐Prcx加cer【니nregL$tet。d)"
h따nd:ZNUI.L
S솥tIJ'ndㅇ낚T.H七R
螺83EC28
56
'80C0343
'8309D42
ES3DFDFF
SBODe8EI
6Rop
80442424
50
51
ESp0SgeZ
SD드424ZC
드2
Ee60E200
33Ce
ReeCO343
88c418
33F6
84C0
.v7418
■扱Fc):' - - 직
"Plair1StuPidpatching''wo미dN○Pthecond
jumpherㅌ댜―enC티theprㅇgramwㅇuldnever
」umptowritethe''unregisterecnstringin
themainprㅇgram'5titlebar.Hㅇwever,yㅇu
certainlyunderstandthatthisaCCㅇmPlisheS
nㅇthingmㅇrethenanaestheticalpatch.ㅜhe
programwoulclst∥―beunregi$terecl.50;we
neecltodigdeeperandpatchthereasㅇn
whytheunregistereclstring15writtenn!!
!St츨OkSS:[0012E024]:00
IRL=Oe
L。。al。a【l드주ron004047D3,00404880

INFO :

"Plain stupid patching" would NOP the cond jump here.

"명백히 멍청한 patching" cond jump를 NOP 하는 것이다.

Hence, the program would never jump to write the "unregistered" string in the main program's title bar.

그리하여, program은 main program's title bar의 "unregistered" string을 쓰기 위하여 절대 jump 하지 않는다.

However, you certainly understand that this accomplishes nothing more then an aesthetical patch.

그러나 너는 명확히 심미적인 patch보다 더 이상 성취된 것이 없다는 것을 이해했다.

The program would still be unregistered. So : we need to dig deeper and patch the reason why the unregistered string is written !!!!

Program은 여전히 미등록 상태다. 그래서 : 우리는 깊게 들어가는 것과 미등록 된 string을 작성된 이유를 patch 해야 합니다.

시스템 생성 대체 텍스트: 더cPU-m이nthread,m이lulefjproduc
Heㅐ鞠np
n흽sa'senb〔，
HOP
HOF'
COn轍ent
0040460R
0e40460B
nn4n4八n「
004046D더
004046。E
n긋4"，추「DF…
9O
98
9e
90
9e
90
8슈“24e4
84c0
브
12
440R43ee
FO9C4200
1드5C924200
憮m。－B묾騙一‘,
땡궝엷山마
엷碗F「綴嫩
계■■탭·
*
="F【솝shJLg'a눠Pr여희cㅎr"
* '》HLjLㄴ
…功改瑙TeHtn
4''eeF3
뺑rR6rgFC
SBeo44여긔430e
68C89C42e0
r샐OF'
HOP
HOP
HOF'
"0U
TEST
JES
"OV
PUSH
PUSㅐ
Cr룁L
REVH
뺨1아』
PUSH
瘢＇·
51 …PUSㅐ
FF155C9242OaCRLㄴ
C3 REY"
90 …H아》
ge HOP
ge …HOP
83EC28 SUS
56 PUSH
68eCO34300 PUSㅐ
6830904200 …PUSH
E83[)FDFFFF :CnLL
SBOD88E!4200110U
6Rop PUSㅐ
8D442424 …LER
se …PUSㅐ
51 !PUSH
ESR039eZee CnLL
SD드4242C :〔탸l
드Z PUSH
ES60E200e0 Cr룁L
33CO XOR
ReeCO343eo 11）」
83C418 RDO
39F6 …XOR
ECX.山＇아큼
「Jprㅇdu
ECX
며．ORDF
LabeI
COlnment
Brea驕曲t
H·ttraCe
RLIntraCe
므"Fla$hjig＄홉닐Pr여노cer(니nregi$tered)"
＝》HULL
L혀콰O닐TeHtR
#·갼··…＞·…
r■■■■■■■■■■．■■■■
0.:．ㅓ0눈E4
너J4너차[>
n.:.4n4卜E프
rJ239nn룅rO6C
山6F6F6F6F柏70沁花
뗀녠44444444
DEF
0乙UO
썅홉맣■욥
Lr kr
or冬
GOto
"-1529144668"
빳j\"
34a7E
뱁욥이■츱J■솥솥．홑겸겸욜
''7r'7씽‘7쨍f쨍r7
444444444
· (Mem이yaddress
84C8
F土17갰18
TEST
JES
ESP,28
ESI
「Jpr。d너
「Jpr。d너
시酸여눕
ECX.며．아＝
0n
티IX.山·OF
ERk
EC님
fjpr。dU
EDX.［ㅄOF
EDX
fJ아여눕
E댜驪．ERX
RL,BVTE
ESP.18
ESI.ESI
nL,습L
HORTfjp
gBFei6pBnp勺드''nHC
72詮袗乙松乙73乙걔74겨74겨
4444444444444
刊舵牝牝舵牝40舵牝40柏舵舵牝舵舵牝舵舵貂舵舵牝舵牝40舵牝舵牝舵媤섭aC珌
빗o0卵애에騁애朋盼00애卵騁卵恥腑盼盼盼ee騁ee騁Oe騁00ee00ee開卵애驪St離
LOCa
kSS:[eolZE024〕＝Oe
0
IOa【【룔予ro衲004047D3.OO404880
쬐욘w
COPytoexeαl松lb논
Af님멥‘
Bookmark
陜翩pdebuggedproc·55
Make改jmPofPr。C·ss
〕 ^빼묘｀鋼
쁘난르텟9의쁘맺9므으뾔饅쁘난르앳…앳윳1.
勿pearanCe
」톼l
」羸M來蕣쩌
.,,.=FFO
久더4負더且슛
''<Nn
P＾떽｀'
■自탭닙닙탭■r
·■r 계■·
F히贓inDu叫’ ■■■

Follow in dump

Dump를 따라가자.

Memory address

시스템 생성 대체 텍스트: 竺쁘颱i"thre삔module-fjprod삔eeesㄷ｝
n깅apapn다edp
999999
令닌．．룔홑
百驪福耳乙百兩
004e460B
00404螺DC
004046DD
e04048DE
0e4〔14EDF
H인L숩결蜘D
I마쁘뜨휀브닛__ __
HOP
HI〕F'
r샐OF'
HOF》
HOP
HOP
I＂以，nL.태八EPTRSS·tESP+4]
iTESTnL.,自L.
JESㅐORㅜfjprod니ㅇ．O04O46FR
…＂炚夕EnX.山풀（)RDPTRDs:L43聊枓4]
PUSH「Jpt。duc.oe429CFe
h·．=「．t ^
브
＇』．댜424e4
84C0
.v7412
계■■뱁
0e4046E4
00404L．댜［
004046E크
00404。ㄸ，
004046F2
Oe4046F3
004046「9
Oe4046FR
0e404700
0e404705
0e404706
0040470C
0040470〔
0040470〔
nn4t-1건一
더n'
「’
l
R1440R4300
68FOgC420e
離、、。。242e이
巍擺騶컨
라l、5c924沸”
C3
PUSㅐERX
="F!a$hJ'9$a닐Pro＜加c샅r''
=>HLILㄴ
CnLL며．여出PTRDS찧t＜各USER32.SetUtn
R「Y뒤
t뺘'ndo"Teㅒtn
"OUECX.山룔ORDPTRDS:[43야놈44]
PUSHfjpr。duc.e0429CCS
PUSㅐECX
CRLL며JORDPTRDS:t《各USER32.S．티“nd여놜T버
RETH
HOP
'IOP
HOP
SLjsESP.28
PUSHESI
PUSㅐfjpr。duc.0043030C
PUSH「Jpr。d니c.00429D30
Cr뵙Lfjm여눕。．。04044'e
"OUECX.며，아극DPTR05:[42E188]
PUSㅐ야눕
LERERX.며j0RDPTR55:tESP+24]
PUSㅐER×
PUSHECX
CrLLfj따여눌。．ee42여106
LERE마《．[L아국DPTR55:[ESP+ZC]
PUSㅐEDX
CRLLfJprod녀C.004129Re
XOREnX.ERX
"ol)RL.B부TEPTRDS'【43O3OC】
[
Teㅐt="Fn恪hJLg＄홉닐Pr여加c슨r(니nregi$tered
h따n．」＝」＇ㅓULㄴ
S*tU＂놀d。낚T．냠tR
90
9e
>
OO40471E
00404723
00404729
0040472B
0040472「
0040473e
0e404731
00404796
0040473n
0e40473B
00404740
00404742
00404--'
一一-一_,1＿닙U …
ES3DFDFFFF .
8B0D88E142001
6ROR i
-'一1 [-.죙盼
8D442424
5e
51
ESne39eZeo
SD드424ZC
드2
ES60E200eO
33Ce
ROeC0343ee
q슥「4 1負
nn.,근
p l」
Hㄴ‘,.'
LㅇCal
AndSeeWhatALWIllbeCOme
whenstepPingthis"neofcode
喆F六芯涵乙礪屎茄弑髓了－
_1요륵이I L______________
ECel230000000008. 4OC.9011.....
ee7ㅌ3800C08E4O0e.........卄8.닙9.
37eoIn드810e!Oeoe6516드4'47.,[》0..
18FD!200COSE40oep◆α‘쉈）.’뉼*.닙·．
607E3800CSSE4000....p샅8.'뀨8.닉딩．.
98534200FFF「FFFFSO’【．．솥．걀욤B.
10el몌00eo000000490닐90활．*0......
CORSBR。DC00000008'1..L벼〕．볍鰻．-....
i8E!!200E44드【）277신솥．닙0.袗수．蓴E르닐
le01eo00oeeeOeee닝‘..90..》0......
ECe12300no3067eo，》..*0..囊0鷺．욥＝9.
00O0O0O000e00000얽．..0...........
000eoe0000O0eoee*...0...........
0000e000C8Eei2000...........'O*.
6704D477BO41DZ77'.仇‘.0*.9수솥驪Fn솥닐
nq q「 n爭 77더q 더a qaqn '竇솥』증츱．.
泌jr컫미灼’
騙r」toflㄷ」
. . .· . ' 띱튿띱r
00430334
00230!EC
00000000
OO0eeOOe
0O00O0e0
00387Eee
00408ECe
36313536
3436343드
SB!ROe37
OOeoello
SB!CIB7e
00408FIC
0012FLlls
0040SEC0
RSC11＂《NOPa55
千jptㅇd"C.004080
uHthe"e.SB!R003;
uㅐthene.SBICIB7I
RETURHt。「jprㅇ．
fjproduc.00408E'
一紛2C銘5438沈4044454c秘읽貂螂秘
Veoeapeaoed킹eeeeoeo
一조花2E麗2Eㄾ2E汪ZEZE正2EㄾZEZE
一騁沁沁盼沁盼泌盼애騁油盼盼盼秘
凹駝34四盼盼eeoe매ee매Oe에盼硼鹹
紇腑36柏3512盼柏柏盼盼eees硼12怜
·盼ee348F7EElel麗SEel이ee盼eeEZ디
4erOCOOpCaUeCellapa밍더
3e317孔pECCEleees'
Fe60OaUB7dUeeeoee찧rn
Fe公jC!n빕r큐7OeO0eoe뺑rn
驪皺
■■■■■텨■■■■

And see what AL will become when stepping this line of code

이 code line을 넘길 때 AL이 어떻게 되는지 보자.

시스템 생성 대체 텍스트: 「7하芮측11《n
〔노［仕의l으의
Re
LSter'
FF「FFF
FFFFFF
0049e3
(「PU)
儡。11”沕Pa">"
Ooe0O
001ZE
翩CX뗘BXSP
EEEEE
Ofcours이AL15alreadyo
becaLJSeunreglstered
P! CS001832bito(FFFFFFFF)
RI SSee2332b요te(FFFFF「FF)
20 DS002332bitO(FFFFFFFF)
Se FS0e3832bit7FFDF000lFFF)
TO aS0e00「IULㄴ
De
oe ㄴa$tErrERR（】fㄴSUCCESS【00000000)
EFL00200216댜10..［·．h티R.NS.「E.bE,bl
STeenpty-???FFFF0e040404eOO40404
STI鉀뼁》t,－수수？「FFF00000e0e0ee4e404
STZehpt,－수수？FFFF00040404ee040404
ST3ehpt,-？수？FFFF8000000ee0040404
ST4ehpt,0.e
ST드.nptye.e
ST6순hotye.0
ST7enptye.0
큔욘10 ESPUllZE
FST0000 COf、deeee Err0ee0eee
FO.1272 PreㅇHEnR,53 Ha$k l1eel

Of course, AL is already 0 because unregistered

물론, AL은 이미 0이다. 왜냐하면 미등록이기 때문이다.

So, let's see where ESP+4 is set to 0

그래서, ESP+4가 0으로 set 되는 것을 보자.

Now, let's take a look just before this code

이제, 이 code 후를 보자.

And find where ESP+4 is set to 0

ESP+4가 0으로 set 되는 곳을 찾자.

INFO :

I will show you here the basics of finding your way in the code.

code에서 기본적인 너만의 찾는 방법을 보여줄 것이다.

There are a lot more advanced ways to do this.

이 일을 하기 위해 꽤 많은 진화된 방법이 있다.

We will discuss these in later parts in this series.

우리는 이 series의 나중 part에서 이것을 의논할 수 있다.

However, like told many times already : I think it is good to know the basics too …

그러나, 이미 많은 시간 동안 말했다 : basic을 좋다는 것을 알고 있다.

For example : we can get where we want to arrive by using the Call Stack or by using the Stack or by placing a memory BP on write on the byte at 12E024 etc etc.

예를 들어 : 사용하고 있는 Call Stack이나 사용하고 있는 Stack이나 memory에 위치한 BP에 의하여 12E024, etc, etc에 도착할 수 있다.

Be patient, all in due time ;)

다 때가 되면 돼. 조금만 참아.

By the way,

This place of code is in calls

Calls에서 code 조각이다.

So point this line

이 line은 가리킨다.

시스템 생성 대체 텍스트: CpU,mainthread,modul이jproduc
dre$'1Heㅐdunp
D죙sa$senbt,
CO衲nent
탬·■ d
팁녑'슴
e댜·eeaFJa딩
90·999q-
0닌404b'R
0e404帆）B
004046DC
U려4［ㅗ匕b니
U.4긷｀4'〕E
nj40수「gF…
0.1’ㅓ0눈E4
너．'4너차［꽈
0.1.4〔14논E프
UU4니一b윕틀
004046F2
004046F3
004046F9
004046FR
OO4O47eO
0040470드
0e404706
004047er
0040．후70
00.10470
nn4n''-
各1,·
3p442404
84CO
TEST
JES
pL.머·TE‘꺄꺽99:「E：뜨P+4〕
RL..nㄴ
OP%OP盼OPOPoV
HH"HHHh
i2
44en439e
「09C4200
볘e
티경X
Tf〕prㅇduc.Oe4046FR
.며츨0f극D
USH「jp＇。due.
PTRDS:〔430R44】
00429CF0
155C924200
PUSㅐ
CRLL
RETh
맡10U
PUSH
PUSㅐ
C「l【．L
RE채
HOP
HOP
NOP
SLjs
PUSH
PUSㅐ
PIJSH
CnLL
ㅒOV
ERX
며．ORDPTRDS.t<'USER32.S.tl.in
l『i己‘乙'.’「l部hJ쵸＇＇헤Pr伊눕아r"
녜hl．陋d볍》NLjLL
do닐Te쫠'Set닒U、do낚TeㅐtR
-―꿱――·
4'leeF3
7nH65FC
r■■‘
8B0044鮮겹4309.
68C89C42ee …
드l
FF155C92429e
L塔
9e
90
9e
83EC28
56
680CO3430e …
ECX.山졀ORD
fjpr。肉c
ECX kt
며．ORD「r
PTRDS:【43아吾44】
.0e429CC8
DS.[（各USER32.s.tl.ind이JT·目
Teㅏ'="Fla'hjig＄괘Prod나cer("nr.gL$t.red】"
hl■脯d= H내·L
S슨tULnd。닢Te냠tR
零·卄··…＞·…
f■■■■■■■．■··■■■■
ESP.Ze
ESI
-.1.853e9D4200
47lEll.E83【）FDFFFF
rod니C.0043030C
rodUC.00429D30
fjpr。d니
「jpr。du
시O戚X눌
RSC11"-1329144668"
습SCll"C:\"
SBOD88E!42Oe
6nen
8D442424
5.
5l
ESnO39eZee
ECX.며．ORD
PUSH聊눕
LERERX.
PUSHER×
PUSHECX
Cr札L루jo
며쵤ORD
0040446.
PTRDS:t42E!88]
PTR55:tESP+24】
rod나C.0042읫乙6
andfo∥owthecalls
(wearelucky,only2)
.ESI
,qL
HORTfjpr。duc.00404768
OREs댜
XTJ
4723
4729
472B
472F
473e
4731
4736
4799
473B
474e
4'42
4747
474R
474C
474E
8DC424
52
ES6eE츨
33CO
peOCO톤
83C4!8
33F'
84C8
.v7418
apape白탭佺poa빕ap00000仕UapO
4444444444444444
00000쇼Oapedpeee쇼pdp쇼po
apa긴oapO000ap00ap0Oapo
LOOa【。a【l'fr。n004e471恪．'004048얹l
SCI
R
4Ca팅O－닌I더－
3Fn딩aUI넌I=-
310nI0ㄷ
aUnren-n·l
390nIJ-．빙?
4층닙n-더Il-.Ut*
onrp·尸－n··궁
內Un乙nLnlt-1→4-11
敞’dr슬륭＄
Understandthattheaboveroutine
towritetheunregistereclstring(or
not)inthemainwindowtitlebaris
calleclfrㅇmWithinthesetwㅇcalls
’「
〔28
「’[C
「즉n
므；‘후
"<NOPa冬료:
너 노」－1.’』
더p쥴요E08·
너r료'9」)4
OolZEeR4
np4q-F-FO
L
- - 술 - －■-…-
戚4浚》욥4沙5
『·r노뱁r놀r騙7노7씸．7
lpr'
.」“'
.」．江.an4〔I：긍F
7n히＜r，移하E혜
-깼꽁추뱄의
--.- r．「놀뱀r노r놈r노겯씸

And follow the calls

(we are lucky, only 2)

이 calls을 따라간다.

(우리는 운이 좋다, 오직 2가지 밖에 없다.)

Understand that the above routine to write the unregistered string (or not) in the main window title bar is called from within these two calls

Main title bar에 등록되지 않은 문자열(또는 아니거나)을 작성하려면 위의 routine이 2 호출에서 호출되는 것으로 알고 있습니다.

시스템 생성 대체 텍스트: 「무｀-------
더cPU,騰inthread,洲넌uleflproduc
습ddre뜨鷺1HeH
dunp
눼「各
Disㅋ＄$ehbl,
HOP
OU404bDD
＂君41:14ㅏDE
004046DF
닐틀
'.
9B
98
e슈수4魯수04
84Ca
앙Ue 논":e
믈hs ㅜL∥S
r·■L r■■L
5C92420B
44毓各43OB
4·‘8·FS
?RZprOFC
004이추6E｀혹
0．〕404LE6
004046EB
U0404bE0
004046F2
Oe4046F3
004046F9
004046FR
00404700
0e404705
00404706
004047OC
0040470【
00.1047aL
n040470F
12
44聊눕43Oa
F댜9C420e
SBOD
OL．나7TF．驛논요층：rE와令→4〕
RL.nㄴ
넌嫩ㅜ「Jpr。duc.OO4e46FR
EnX,山．ORDPTRDs:[43驪경44】
'‘뮷r。duc.ee429C「。
며．하DPTRDS.t＜各USER32.S.tUind。닐T이
ECX.山를ORDPTRDS.[43야뇰44) …
「Jpr。duc.oe429CCS '
ECX
며．며괵。PTRDS:t《‘USER32.S.'UindO닐T。：
8·‘F3e·e
'6FC999
$·終··…＞·…
r■■··■■■■■■■■■■■
83E후28
ESP.28
ESI
6888
S'‘ㅌ
이〕4O47ler零
匯길40421『.·
더nJ여d7':l·
n겨pC·Jyn'‘걜X·Pr
eCLEE굿7DErTRㄴ츤05
r' E ㅌnHFE
Oe4O47lE
0e404723
00404729
0040472B
0040472F
Oe40473e
00404731
00404736
00404799
0e40473B
00404740
00404'42
00404747
0040474R
0040474C
0040474E
0C.34390
309D420e
3DFDFFFF
H〕P
더OF'
lㅓOP
H()P
HOP
HOU
TEST
JES
＂醜j
PUSH
PUSㅐ
CnLL
RE채
뺨10V
PUSH
P(JSH
CnLㄴ
RETh
H아》
"OP
"OP
SUS
PUSH
PUSㅐ
PUSH
CnLL
"OV
PUSH
LER
PUSㅐ
PUSH
CnLL
LEp
PUSㅐ
CnLL
X아극
『IJ」
nnn
X이《
TEST
JES
,r놔.0
「Jpr。du。．0043050C
fjpr。duc.00429D30
畔』
R9
퓌】O戚X눕0.
SB6D88E1420B
ECX.며．아극D
'pop
eD442424
5.
Sl
"nO9,eZeo
8D54242C
S2
Ee6eE290ee
3SCO
R.OC.343ee
8없겨18
3aF'
84C8
.v7418
며츨ORD
0040446.
PTRDS:【42E!88]
PTR55:tESP+24]
X
X
p戚날눕。．ee42이）D6
.며柏RDPTR55:[ESP+aCI
X
m여눕O.eO4129Re
.ERX
머를TEPTR05:【43O3OCJ
.1요 ／〃…
야．
HoR
ESI
RL
Tfjproduc·
Andf이IOW
thefiFStCal-
니냉盼Ic'【【＄
't。口얘아짜
숩。4山4슛소n
COpyPanetodpbcnrd
eC-IUe-
O00d긷-
았엽r슬훵륭
Oe12EO24
00!2E084
Oe12E04’후
00!2E054
■ 4뿌C.90뺨．
········· O·
651솝54b47.+[
p+L【J略．수含t.
l군J그
Lr
blㄴ
4죠긴rDC-
3쵸U3''-
Fn킹6B솔
FO35-
Fn밈''Cl
Fa길3뺑‘-
FC밍rOB-
盼re31I
轟恥걘

And follow the first call

Place BP

And push <enter> to follow the call back

첫번째 call을 따라가자.

BP를 설치해.

<enter>를 눌러 Call back을 따라가자.

*번역 주)번역을 하면서 알게 된 점. Enter는 바로 call문으로 들어가는 것이고 F7은 그 line에서 call문이 있을 때 따라 들어가는 것이다. 즉 enter는 다음 EIP가 가리키고 있는 주소가 아니더라도 바로 call문을 따라 들어갈 수 있다.*

And follow the second call too

And put BP

And restart app ….

2번째 call을 따라가자.

BP를 설치하자.

App을 재시작 해.

And re-run the app to see ….

보기 위해 app을 재시작 하자.

….(scroll up)….

Scroll 올려

….where ESP+4 is set

ESP+4가 set 되는 곳이다.

So, this is the call that is interesting for us

그래서, 이 call은 우리에게 흥미롭다.

Meaning that this is the call that calls the routine at startup that sets the unregistered text(or not) on top of the main window

이것은 Startup routine을 부르는 call 이다. 이 call은 main window top에서 미등록 text로 set한다.

Let's remove the other BP

다른 BP는 삭제해.

시스템 생성 대체 텍스트: F넓e
－태
WindowHelp
녜』」
희희꾀그」꾀희의희희희희」희셥1쬐
wDeb四Pbg"OP坎’ns
LOg 시t孔
Exe이勿盼e戱欣」esAIt+E
Mem아y Alt＋서
produc
一L一F그
．팠》흠，
Thre出S
whdoWS
Han뎨es
C휜
581ch히n
PJ出郞
Callstack
Zpr。
懦
dUC.e0430334
dUC.oe429DOS
et니rnB汀「「''=「jpr。dUc.004303:.4
d니C.00429Di4
P쟈궉05:L<'k티겸「EL82.e·tPrLuat.
씨t+C
'Dn넌니C.00490994
j轉r。山。．0e40464e
訖
1驢tK놀O.Oe404'EB
DefauLt="＜낙柏PaS$->"
Ke딧:>.Pa'＇냐。n「
S슨CtLOnr∥ReqL$trat쵸On"
B빵tPrLv.t·Prㅇf'【estttngR
RSC11＂《H。P騙5>"
;)
Alt춈8
《．出＇ORDPTR55:LESP+8」
<.110
S닐딩toh【CaS상＄110..111)
WaU논S
Ref눙슨nc한S
RUrltraCe
SOUFCe
食뵤JrCe恪ES
Case111Ors닐itCh8O4e47E4
S니Ltoh【C숩딥esi..7ED】
r■■‘
brbL낟p팀J…7꺼노ㅑkㅏVpOPVPhH낱P
H논
T슨xt卄Ie
1
OdUC.e04e4944
r。duㅇ·ee4049엣［
RX,놔ORDPTR55:【ESP+1e
.7EC
仇句C.eO484918
어노C.OO4e48BO
T주Jprodu。．0040482R
rod니O.ee4e499C
.며，ORDPTRS히tESP+8]
'0481티
執
FF!52C9242OOCRLLDUORDPTROS:[<'USER32.EnclDL.【。O》】
Ca＄·2。「‘닐itchOO4O47FC
R*＄니.t·2
h盼놀d
EndDialo'
騙ew
■■■■

:)

시스템 생성 대체 텍스트: 同
광뇨 棚노
‘·1■■－
nd（汁수‘5
→047
004047Les
ne4O47E;._
Ul.'4O47ElQ
U.404。’[=
004더47C광
뎨〕404긴［D
0e404'DZ
蠟헨
「－
dunp
乙百一囊柏34泌O一
68089D4200
51
68149D42ee
FFis'89e4200
Oit't｀●람“,
PU하［l》pr。duc.ee430334
^·R.O요‘헝．r룔IFPU)
PUSH
P(JSH
PUSH
CrLL
PUSH
C「LL
PUSH
CPLL
nD【）
POP
RDD
RETH
驢IOU
SUB
시prㅇd니c.00429D08
EC났
Ret
bef
kPV
ent
■■■■．·■
니ra
a녜I
f卜r一fjprodUc.0043e334
-'(-NOPas드－》＂
「Jpr。duC·00429D14
며．ORDPTRDS:［《‘k티괭NEL92.G。tPriuat·
eot'On
"Pa$S냐O戱r'
="R솥gtttrat힁on"
683403430e
ES'EFEFFFF
드0
ESe8F「FFFF
83C408
5E
83C428
C3
8B442408
ZD10O1000e
드6
.v0F84540le00
48
.v0F85RseleOO
0FB74424le
3DECO70080
pr이luc.岬43叩얜
미「O蠟·C.e0484648
X
6etPt｀·긔t.Pr。수1Iestl-LngR
RSCll＂了H。P〕55샌’
OrO벼·0.OO4O46EO
eO4047【Ia
U040470B
004047DC
0e4047DF
004047E0
()e4047E4
004047E9
004047En
004047F0
004047FI
0e4047F7
oe4O47FC
00404801
00404807
0040450D
OO4O480E
00404810
00404811
00404817
0040451B
0040481D
0040491E
Oe404824
0e4e4526
00404e27
0040482p
0e40452E
Oe4e4830
0e4e48긍5
Oe40483n
0040483B
00404841
너'404P:
ㄸ증:FFFFFFFF
ED:.:0043e335RSCI
태《e000O0eO
ESP0012E024
邙P0012E0RC
ES!e00eoeeC
卽!0012FD18
E!P004047D3ㅏJpr
CO ESOe굽날32bL
0 1 츤: n伋,D 즙하「굽
'XJn·J
rrZrEZT
ESF.8
ESI
ESP.2
ERX.
E아《．
ESI
휘nBrea沖枷tS
미丁－ -－큰
트
ㅏJprO
EnX
R改lre'S
깠需騙
쁨締驪篆
Disa’톨히出l,
nOVRL.B'l'TE
:[ESP+4그
톄뎨더
…^
'-1ptl)duoIPI닐커，'
EEc限
.v8FSF14ele0OO
.veF84R300e000
48
.v74!R
49
.v0FSS85eleeOO
8B4424es
6RaZ
5e
「F】gZC勺242Oe
33c0
!000
742408
28
340343e0
EBO7O00e
…"OUZ
…C『IP
:JG「
…JE「
DEC
:J〔－S
!DEC
IJNZ
IUOU
IPUSㅐ
IPUSH
…CrLL
l닝얘
IP珊
ㅣRㅌTrl
…UO니
PUSㅐ
「Jpr
XEn
티媤．
JprO
Jprㅇ
탸樹
H()RT
탸拐
「jpr
티樹＇
2
印닝
미JO
탸IX.
ESI
le
0040489ef〕Dr。duo
n[．쵯겯S
야L
dL
L
fjp'。duc.OO4O46EO
fjp數닝노0.OO4046Ee
this15theuselessone
ICO"＂翩t
卞
…
DP邢괭
8[E요P수e
山恪찬ZCf엥
L캥뎨仕OD4O47FC
늡·휵
쵸
걍Un
’。騙
D。〔
ESI.며JORDPTR55:【ESP+8】
28
Ca츨elo「＇닐it하놀e84047FC
pro
B
1
dUC.00438334
C.ee4SO334
(2e27.)
164C924泌헥
ORD
X
PTR
시7EES예테매
USHUSHUSHLUSHL
PPPCPC
EZBCH88콘bFnU
른큐C8666r큐Fr큽
FF1530984온Oe
ORDPTR
ㄴ‘쵸n요닙놉－--－요a－크」n地乙n요－올
O04O46EO=FJpr어汕c.ee404'Ee
OStE<LUSER32.6.tD【glt히｀》！
DS:【＜驢USER32.Getl·indo닐Te:
no·r4르논a층츱」1

This is the useless one

이것은 필요없다.

시스템 생성 대체 텍스트: 희즈」희꾀긔꾀꾀의희희勉꾀」희쬐쐬의
」눕ㄴ 」·■L
Yㅇucanalsocometㅇthebreakpoints
綸，，싫鶩鷲땄땄窯

You can also come to the breakpoints window clicking this button :)

너는 또한 이 button을 click해 breakpoints window로 갈 수 있다.

시스템 생성 대체 텍스트: OBrea沖l)ints
톄91.
히H
nddr.SS
OO4e46Le
"Od일
RCtLV
D〔크크＄＄히｀bt,
COhhent
00404승8
「．Jpr
'Jpr
「JF;
니C
UC
C【겯L
닐ayF
닐a99
ㅑ十4
:nㄴㄴ
邙표LL
Rㄴ.B무TEPTR스
f,ptㅇd．』C.004046라〕
fjDroduc.004e4乙타’
hHRO
Ieweodod써
嚥Sabl죤
耿囊tcond敏）n
F하IOwIn嚥sa“텨山뇬r
SPace
Enter
｀극DP7F
【캥비놀8砂룝847FC
以”비eal
맷r
Qpyto呻board
시p.aranC큰
UORDPTR55:L__
》l
닐'tCheO4e47FC
탭탭··탭·
．■．■

;)

Now think with me …

나와 같이 생각하자...

… it must all happen in this call

이 call은 무슨 일이 발생한다.

Because in this call, the program needs to know already if it is registered or not(to put the "unregistered" or not)

왜냐하면 이 call은, program은 이것이 등록하는 것인지 아닌지 알기 위해 필요하다.("unregistered"를 넣는지 아닌지)

And we note that push EAX….

EAX에 넣어라.

시스템 생성 대체 텍스트: ...WriteS0inAL...
뱐臘얹차br】
...atthistim티
perhapswecan
..,．。匕ㄴO
36313536
34363435
SBIR0037
00000!!e
SBICIB7e
00408F!C
oe1ZFD!8
004OSECe
000eeO00
fjpr。d■．
changethatfor
futureStartupS
uㅐth。ne.SBIRO037
uㅐthe꺼e.드BICIB7e
RETUR"to「Jpr。dl』c.e04e8F!C「roh「〕Drc.l九（.匯나04710
「jproduc.00408ECO
48C
444
eee
騶여馹邵秘여
eeeoeo
ㄾZEZE汪汪ㄾ汪2E
에盼盼卵e8卵舵沁

...writes 0 in AL…

AL에 0을 써.

… at this time, perhaps we can change that for future startups

… 이 시간에, 아마 우리는 미래의 startup을 바꿀 수 있다.

… in ESP+4 …

ESP+4 에서

So, AL writes zero …

AL은 zero를 썼다.

시스템 생성 대체 텍스트: C슬두．
.0뇨‘
O「！낚itCh004047FC
youst∥―remembertheaddress구)
1 .＿듀
卜ab.Uab·
''p.OOB.
르크
....0쮸B.
i숴B.....
卜궂B.....
碣B.fj饉
衲ervoy요
)1234드67
구hijkl開
卄뱁닛Z·…
.？댔솔CRtl
,。OT■山自
0012E028
0O12E02C
OO12Ee3O
OO12Ee34
eo!2Ee38
001ZEeSC
eOI2Ee40
0012E044
0012E048
001ZEe4C
0이2E858
OO12EeS4
ee12Ee58
OO12E05C
00i2E060
0012Ee64
e0430334
00480206
eO0eeoeo
0O00000e
eO0eeoeo
00387E00
00408EC0
36313536
34363435
SBIROO97
00000!!0
SBICIB7O
OO4OSF!C
001ZFDis
OO488ECe
OOeoeoeo
R엇그I"<HOP｀르드》＂
스
fjproduc.OO4OSECO
uHthrn.'58lROe87
uㅐtl珊衲e·SBICIB7e
RETURHt。「Jpr。dt』c.叭껴08FI;D「r。r.FjDl'o.Jl'c.匯나04710
fjproduc.oa4OSECO

(did you still remember the address ?)

(지금도 이 address를 기억해?)

So, place BP here

BP를 여기에 설치해.

시스템 생성 대체 텍스트: 더Cp【j-
m이nthread,m어lulefjproduc
H.XdU"p
D쵱룔aS5ehbl,
IniF나eHa聘-..C:\O。에n翩t$andSettLng$'Ikt'L。calSettin
BuF5LZe=28(40.)
Reh.rn以‘F룐닙．'시pr。duo.e0436334
DefaU【tr"(－더0Pa룔S->"
K.uZ["Pa'｀닐。rJ'
r■■■■·····L
色楢【맡＄욜
蕨耳砂＊-
andPress<enter>tofollowtheca∥
toseewhat'salㅣhappening
心re00
仕깊O麴p白긷
e04驪뉴．
004047c2
004e47C8
■■■■■■■
004e47Dㅌ
■■■■■■■
0e40470읗
0e404·柏6
004047DC
OO4O47DF
004047E0
0e404'7E4
더e404'E'
0e4047E「I
0e4047F0
0e4047FI
004047F7
004047FC
00404891
00404807
OO4O48OD
0040480E
004048!0
00404811
00404817
0e4048!B
0e4048lD
0e4048lE
00404824
00404826
0e404827
ee40482R
0040482E
ee404830
Oe40483드
e040483FI
el〕40489B
FF
68
E8
50
E:3
5689e4200
34e34300
CRLL
IPUSH
ICf룁L
…PUSH
CnLL
R。D
P(r
n。D
.RㅌTH
"OU
SUS
며．ORDPTRDS:[（驪KER"EL32.BetPtLvat·
盤：꽈gn-二販무l룔trat寧에r
betHrb』ateHrofL[ebtrlF놀gH
nSC11"<NOP슬55>"
俉汗FF
0：上■．1FFf7
「Jpr。duc·e0430익나
干J醵여눕c.0040484e
ER죠
「Jpr。山c.OO4O46EO
ESP.e
ㅌ51
ESP.Ze
ERX.뎨＇ORDPTR55:tESP+8]
ERX.110
a· 00
0 2
24es
0010000
4 4 4
麗E3C3B4
858C8
S닐ltoh【CaS상冬118..111〕
84드4eleO00
…
85R드e1eO0e…
B74424!e …
ECO7O00O
PUSHESI
JEfJpr。duc.e04e4944
DECEnX
JNZ「Jprㅇd니ㅇ．OO40499C
H醜，ZXERX.놔ORDPTR55:【ESP+!e]
Ca'elll。f｀닐itch8O4847E4
읽“toh〔c슬딥·횻1..7EDI
rU거R닙거O닌n
綸鹹HO테시테2
rr 슨9 ㅐ
硼6EㄸEEcNzouuS
CJJOJDJ"P
8F
84
in
!4e!0000
R3000000
E댜《，7EC
「Jpr。duc·eO4e4918
8드8501Oaao
어노C.004048BO
T주Jprodu。．鱗＞4048즈놀
rodUO.0040499C
.며J아국DPTRSS:tESP+8〕
D6FSFFDFF848F
Zr구04e0380474o
8B4424es
6ReZ
5e
「ns2C9242Oe
33co
드E
CZIO0e
8B7424es
6R28
683403430e
68EBO7eoeo
56
FFIS4C924200
PUSHERX
C.LLO·여DP가t05:t<'USER32.E"dDL홉【。O＞】
XOREp《．E自X
P아》ESI
Rㅌr"1.
"J』ESI.대를ORDPTR55:【ESP+8]
PUSㅐ28
PUSH「Jpr。d니c.ee438334
PUSH7EB
PUSHESI
CnLLDU아궉DPTR05:t<'USER92.6.tD【glt슨n》
[
Ca｀·2。「，닐itchSO4O47FC
Fe:니lt Z
h.I,I「d
EndDial。g
C슬즐e!O주＇낚itch0e4047FC
-o'nt=28(40.j
E:．』「f슨r=f
C。ntr。【!D
ㅑ．(.:rld
Jpr。dUc.e043e334
=7EB(2e27.〕
GetDlg!t·｀
· · · · · · · · · · · · · · · · · · · … …녹7 … - ·
■■■■■‘
00404640=FJprodu。．BO404640

And press <enter> to follow the call to see what's all happening

무슨 일이 일어나는지 보기 위해 이 call을 따라가자. Enter를 눌러.

시스템 생성 대체 텍스트: 더cPU,mainthread,modulefjProduc
緇씀뻐뿜
dunp
83ECZC
56
8B742434
eBC6
〔쵱sa$$enb〔，
COh쑈ent
du예
SrO에m
ECsIES시畝sP
E EE
8D50el
8D4900
》8습08
40
8’홑Cg
.^75Fg
ZBCZ
83F804
.v73e7
》32CO
SE
83c4ZC
C3
>6Re3
68C49C42e0
56
E86티검Releo
83C4eC
8드Ce
.^76ES
68BSEe42eo
8D4424es
50
8D4C2410
5l
83C6e3
56
ES7FE4eoeo
8B4424!4
83C410
83F808
.^7CCl
68OCe343eo
ESFgEZOOeo
83C4e4
33F6
8【》642400
》33D2
ISUSESP.ZC
PUSHESI
"OUESI.메·ORDPTRSS:[ESP+34]
h0VE댜＜.ESI
L티놀EDX,며＇ORDPTRDS:〔ERX+l]
:L타콤EO료．미JOR〔PTR【》S:〔EC닝】
r叩pCL.댔군TEPTRDS'［타仇〕
11螂ERx
ITE륵TC니CL _
｀』7SHORTfjpr。d녜。．00484650
SUBERX.ED닝
C衿PERX.4
JNBSHORT「Jpr。d니c.e04e466드
XORnL.RL
…POPESI
nDOESP.ZC
RET"
eU매
PUSㅐ
PUSㅐ
CnLL
R晄l
TEST
J『42
PUSH
L타놀
PUSH
匡O
PUSH
:叩p
…PUSH
Cr룁L
＂아」
…RDO
:아IP
JLS
PUSH
Cr(L
RDO
…XOR
3
희pr。du("00429CC4
ESI
RSC11”「Jr"
「、】pt。duc.ee4lFeEe
EgP,0〔
ERk,Eg《
H〕F-·、:'..1．」 .004〔t'4도
f7pro·土』:.0042티〕B：프 b르
타L;,미d아；DF'TR55:〔ESF柏그
ERX
ECX.며．아국DPTR55볍tESP.le]
RSCll"0123456789삵乙def功룁Jkl삐。pqr$t니v닐Hyz"
c.OO412B10
DPTRSS:[ESP+14】
mmmmm,itseemswelandInthe
reglstrationkeyverificatior1D
E야＜.8
HORT주jDr。duc.0040465E
l
pr。duc.ee43B30C
Or여눕O..O4129ne
RSC11"-1329144668"
I.ESI
rrfTSS
EE
勺규48C"DnO즐‘쵸Jr랴-，·gCEnUㅓ‘4드7CDZrp79E2378BCirDcoBD27n
6464얘646465朽朽朽邵朽朽朽666666666666恥67햐6767676868秘6868696969696969胡胡胡
444444444444444444444444444444444444444
npo仕킵n뱁apnU仕pa긴npapapapap仕pap00nUO仕딩쵸pa킵쇼ponUapaUOn빕apap0Oap00000np
4444444444444444444444444444444444444444
0白긴00eapodpO00eapeeape0000000쇼UOO000仕Odpdodp麴peeeee
O000apa긴apa긴0000npO仕p0000仕깊0000轟UO色긴000000000000白p
괘404〔
nC
Ee
LEnESP,山쵤이궉DPTR55:rESPI
「XOREDX,EDX
ESP=OO12E024
L。c.tCa【l'frㅇ．004e3998,
0e4047CD.e0404856,ee48B873
·■r 체■■

Mmmmm, it seems we land in the registration key verification ;)

음, 우리는 registration key 검증하는 곳에 도착했다는 것을 보여준다.

Scroll down to see better

좀 더 보기 좋게 scroll 내려.

Step over the code to see what happens(F8)

무슨 일이 일어나는지 보기 위해 code를 실행 해(F8)

시스템 생성 대체 텍스트: …-－·■■■■．===--. - ----===＝∼－∼‘ㅑ숩＝===＝「－-
히cptj-mainthread,m어lulefjproduc
OVOVOPOPDDETHOPOPOPOPU8f-ISHOU미태태刪懈TEs棚
93FE뱁‘3nDa띠aUn따
snr큐드8C9999
幽헨
「7
d너np
01룔as‘활않기，
CO여內e孔t
1564e3430o11
680343ee
C4e4el0000
DUOROPTR05:t4303641.EDX
미氾RDPTRDS:【430368].ERX
EDI
ESI
ESP,!04
一규l - 'EFU
'·卜황 뇨꽈-터l'J꽈긍4
·b、brob'C乙O'D－卜'b'b6
44444444444
0色p쇼U仕pdp0000鐘po
1뺙4444444444
00仕긴0000000e
000白po柏p白Un빕轟U凸po
00404649
畛4q4p44
0e4041349
0e404E.4n
0040464D
00404850
Oe40455a
0040465:
n驪「’4r「「
ESP,2C
EST
ESI,며룔여극
ER,.,F7工
E마《．[VOR
DPTRSS:[ESP+34]
ECX.며．아궉D
CL.머＇TE
ERX
PTRDS:[ERX+l〕
PTR05:tECX]
PTRDS'〔E냐＜】
T＿야1댜·_ --- --
SHORTfjprod녜C.0040465e
H∥PPRRkjn""n"nSFZll너Lㄴr■■．.L
'SUSER닝．EOX
노깊1 "
ㅓ1ㅓ1. r
너．4H」f:[
e04046번O
冬83ECZC
드8
8B742434
궁EC一
SD6eei
8049oe
>8R08
40
84C9
r·■ 。닙'
ZBCZ
8크FS04
.773e7
>貶CS 」군
SE ＇군＇
POPESI
虹LfSP.ZC
68C49C42e0
드6
ES6EnR0leo
83C4eC
8드Ce
.^75ES
'8B8E04200
。PU아r3
PUSHfJprod니O.00429CC4
:PUSHESI
CRLLfjp꺼낱눕C.OO4lFeEe
。RDDESP.eC
ㅜESTEnX,EnX
JIㅓZSHORTfjproduc.'｀더江，수b5L
RSC11＂「j
PUSㅐ「_i
roduC.OO42EeBS
…치LESP+8]
nSCll''el23456789abc（」efghLjk．삐。pqr'tuv닐ㅐ，z"
Jlr·－一 -∼ …=7·巴7
' ''卜'스·헝＇7
rE떼出딩‘논＇술닙-논＇술찧·bZUZU
Oops,we」umppasttheRETN
【ESP+10]
0040468e
Oe40468日
e04048》긴
빳盼3
FS7FF400ee
RDDESI.3
PUSHESI
CRLLfJpr。duc.O0412Bi.
Ju얘》L$t.ken
e0404665＝「jpr。duc.e04e4666
■■■■■■■■■「

Oops, we jump past the retn

웁스, 우리는 retn을 지나서 jump 한다.

시스템 생성 대체 텍스트: 더CPU-Indin
… 7rr히H
thread,moduleflpmduc
쁘牛脾
dunD
Disassenbl,
h이jEll.IORDPTRD3:
「J 一――一一一一一一一一一깁Z
■■■■■■■■■■■■■■■■■■■■■■■■．■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
CC驢「松．Er.t
1564034班쟁0
680348e0
[430
【430
364】.ED닝
368】.E댜＜
스
비즈‘
FO「‘
〔IlilOF.DFTRD도
ㄸ＇.
ES;
OPDD매OPOPOPOPUB
PRRkjn"nㅒnZnS
C4e4e!oeOB
ESP.!04
큐
98FE13aoa따aod따
SCLr구58C9999
83ECZC
·노Z … 논궂
■■■■■■■L '
■＇＇·■．、■1‘■1‘■｀'
L＞긍4FIB·LweDEF凸U
se-군以고35I'j려魯5즙쵸01驪4
亡盼b6Ib·b■卜·b·b、b
ㅗ쌩캬괘뺑4441톄4＊뺙4
괘VfUO－너0內빈nUI너內U
*44444444
V。U-U。U-=-轟Uni色UO
V000CUaU什U00
C'15·J
ESEfT
E
004L:1464긍
0e404644
0040464유
0040464n
0040464D
00'404b50
00404〔．드3
00'404b드3
00404〔．드C
00'104匕드7
꼬040춈6딧〕
Oe4046드C
0040465E
00404660
nn4n」r.F.1
너，〕41－쎄手.헌추
·「珩F쨉
더큐4ㅑ나卜.一
0040466C
0040466D
0e4046.'2
0040467「
UU4U4b..'
00404679
0e40467E
00404682
00404883
00404687
56
8B742434
슝ECE
8D6801
8D49oe
>8R08
40
84C9
7忽「즘
ZBCZ
8〕FSn4
.v7907
>32c8
드E
83C4ZC
C3
》'ne3
68C49C42e0
S6
E86티긔ne!eo
83C4eC
8드Ce
.^75ES
'8B8E042e0
8D4424es
5e
8D4C2410
5!
PUSH
I＂以』ESI
InQll캬괘
IL티광ED거
Iㄴ타경E댜닉
I『n먀ICL
111峰E'
IT탸TC
ㅗ니nZ＿욥뛰
ISUBER거
!以IPEn>
IJNBSHn
IXOR믹。
IP아’ESI
19叩ESF
18r텨
뻑PU딤H3
PUSH「J
PUSHES
…CnLLf」
PTR55:[ESP+34)
PTRDS.[ER닝＋l〕
PTRDS:〔ECX]
CL
Tr,jpr。duc.e0404'50
:)
다
RSC11＂「Jr"
0040468히■.83C6e3
0040468BI..56
0040469C
더nan4'n써
ES7FE4eO00
ROO
ㅜEST
JNZ
P냐SH
LER
…PUSH
LER
PUSㅐ
RDD
PUSH
CnLL
ESP.eC
ERX,EnX
SHORT「jprodu=.이〕추G길b5L
「jpr。duc.OO42EOBS
ERX.아욜ORDPTR55:〔ESP+SJ
ERX
ECX.［則ORDPTR55:〔ESP+10]
RSC11"0123456789枕cdefgh'Jkl쎄。pqr$tuu니닉딧r'
X
,3
[
pnX노c.Oe41281e
n卜닒令r튠「』 DTD C《"r
J'hp「t。ne驪추驪흥6딨D

:)

시스템 생성 대체 텍스트: 더
CpU-mainthread,贓업ulefjproduc
··= R
C·－=실 T
DD P
93FE
snr갼ro
ee404628
0e40462E
0e404633
00404634
e040463s
0040463B
0040463C
004e463D
0040463E
0040463F
OO4（》4640
00404643
0e404644
OO404E·48
0e40464R
00404640
00.104b50
004046드3
00｀흩0令＝,93
OO404F.F드
0041:1ㅓ匕E7
nn4t-14F.q길
00404杜g딥
0a404〔，gE
0040466이
00404〔．61'
00404664
0040466드
nn404F'.7
OO4O4t--6C
00404660
004벼L7a
0040467F
土헨
「7
dUnD
Disas$ehbl,
nollDlllORDPTR
hl3llDlilOF;DFTF:
F'0F'ㄸ11
P아》ESI
RDDESP,!04
REY"
＂《）P
H아》
"OP
HOP
SUSESP.ZC
F'l」SㅐESI
＂아夔ESI.며．아국D
＇「11FR,FrT
LERE마뱁．tMORD
ㄸRECX.미．ORD
『盼OUCL.머，TE
l工螂＿ERX
ITLbTLL,〔L
'Jt엥ZSH아국Tfj
COnne孔t
1564034麗콰0
6혀〕34300
〔43e364〕.EDX
【430368].E댜＜
slC4e4e!Oe00
C3
90
90
90
9e
冬e3ECZC
56
8B742434
광ECE
8D5801
8D49oe
>8R08
4e
84C9
55:tESP+34]
PTRDS:【ERX+1]
PTRDS:〔ECX】
PTRDS뱁〔E냐＜〕
ZBCZ
89F804
.\,780천
>32c8
SE
83C4ZC
C3
>6Re3
68C49C4200
i麗。태이〕l。。
SUS티礪．E[)X
C門PEn::.:,4
JNB하룔ORTfjpr。duc.O04O466드
XOf귄驪札．RL
…P아’ESI
…nDDE鮮＞,2C
:RET"
PUSH3
PUSㅐ「Jpr。dUc.00429CC4
PUSㅐESI
·C.LLfJOr여눕O.oe4lFeEe
:RDDESP,eC
ㅜESTEq:.:,E댜《
JNZ騈tl)RTfjpr。d"C.00404‘드E
PUSH「jpr。d니c.e642EeBS
LEnE냐＜,며비（)RDPTR95:tESP+8]
峰
RSC11"Fjr"
83C4eC
,\8드CO
.t75E드
溫緞뜀
戀囊［훼
刪緞훑―
인쌨勞랖퀴
8B8Ee42e0
D4424oe
n驪그I"Oi23456789at》cde「샅“jkl뼈。pqt'tu닌닐ㅐ92"
0
D4
ESP+le]
nH∥：
m니．
8'C
잭
Ea
Aha!Butweju
backup
already
004046드E=FjDr。dl」c.004046드E
탭■■■■自■『

Aha! But we jump back up already !!!

아하! 우리는 jump 하기 전으로 jump 한다.

We jumped to this XOR, AL, AL

우리는 XOR AL, AL을 jump 했다.

So, from here on we can't miss the RETN anymore

그래서, 여기에서 더 이상 retn을 놓치지 않을 수 없다.

And it is clear that AL is set to zero here

이것은 명확하다. AL은 여기에서 zero로 set 된다.

This is the place to patch

Patch 하기 위해 여기에 놓자.

(INTERMEDIATE patching level)

(중간 patching level)

시스템 생성 대체 텍스트: 더CPU-Indin
… 7rr히H
thread,moduleflpmduc
쁘牛脾
dunD
1564034班쟁0
680348e0
Disassenbl,
h이jEll.IORDPTR
「J 一――一一一一一一一一一깁Z
■■■■■■■■■■■■■■■■■■■■■■■■．■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
CC驢「松．Er.t
D:.:〔430364】.ED닝
D캬[43e368】.E댜＜
스
비즈‘
FO「‘
〔IlilOFDFTR
ㄸ＇.
ES;
ESP.!04
즐
OPDD매OPOPOPOPUB
PRRkjn"nㅒnZnS
나 h
’긋、．、나ㄴ욜3
00404634
00404639
004e463B
01:1404691::
004e468D
0040463E
0040463F
00404640
004L:1464긍
0e404644
00404E.4유
0040464n
0040464D
00'404b50
00404〔．드3
너．-’·IUㅗ亡=:
「I.--4n4「’「
U.-’·luㅗ亡놈
n:4臼卄「길
더··4너ㅗ「〔「
C4e4e!oeOB
98FE13aoa따aod따
SCLr구58C9999
PUSH
PTR55:[ESP+34)
PTRDS.[ER닝＋l〕
PTRDS:〔ECX]
CL
Tr,jpr。duc.e0404'50
--측―
더갼4L-l零「변．꽈
U릅4U4b닙1
004e4664
00404두6드
004e41867
沁404昏昏C
0040466D
畛404卜袗
0040467.
0e404677
0e404679
0e40467E
ee404682
00404683
ee404687
00404688
0040468B
0040469C
奪e3ECZC
56
8B742434
슝ECE
8D6801
8D49oe
>8R08
40
84C9
7忽「)
ZBCZ
8：〕FS04
.v790현
f32C0
5E
83C4ZC
C3
>6n03
68C49C4200
SE.
E:E:B「q숙0100
83C4eC
8드CO
. .-5L5
'8B8Ee42e0
8D4424es
5e
8D4C2410
5l
83C603
56
ES7FE40000
＂며』ESI
"．긔'FR
L티놀ED거
出경E댜닉
『뺐XlCL
11峰EF
IT탸TC
니”25뛰
SUBER거
C:nPㅌn걍
JNB하紀
XORpL.
POPESI
nDDESF
RE채
PUSH3
다
P(JSH
F·USㅐ
·CnLL
RDO
ㅜEST
JNZ
P냐SH
LER
…PUSH
LER
PUSH
RDD
PUSH
CnLL
「Jpr。duc.00429CC4
ESI
fj鬱여눕c·ee41FeEe－륵＝
ESP.eC
Eq<,Eq《
SHORT「jprodu=·‘」더윌04‘드E
「jpr。duc.0042E0B8
ERX.아결ORDPTR55:〔ESP+S〕
ERX
ECX.［取ORDPTR55:〔ESP+10]
EO<
ESI.3
ESI
「Jp혀날눕c.Oe41281e
「r一노， nL·r놈Dr』 DTD C《"「「C【》ㅗ1」1
!NFO:
15itclearfㅇryㅇu
thattheadVanCed
patchingwi∥dig
deeperinthiscal-
Ukl쎄。pqr$tuu니닉,r'
RL=FF
Ju"O$
「ro衿00404677.

INFO :

Is it clear for you that the advanced patching will dig deeper in this call

진화적인 patch는 이 call에서 더 깊게 파고 들어야 한다.

시스템 생성 대체 텍스트: 더cpu,耐inthredd,棘업ulefjProduc
qd（늅e’딩
Up'f匕】‘논、
HeH
r7
dUho
89그드F.4O〕4갯쟁0
R3업80一홍玉쨍0
5F
5E
slC4e4e!OOee
C3
9e
90
90
90
D쵭s뒈＄$enb료，
hol〕DlllOPDPTRa3:[l덕n「F'그
hol걀DUORDFTRD캬【4=’넌:匕:〕
POFELll
POPESI
RODESP.184
RET쮜
r「
l "．시．ㅜ .＿…^
0040482티■.
00404633"》
0040469r
0040463
004e463ㅏ
〔1〔｀4046靭
0.:'40465:[
너'기〕．1〔？·
깅｀'',V예딪｀U
匯140464긍
恥4아즙4스
0040464:9
Oe40464n
OO4O464D
00‘홍04b50
ee404652
00·홍0궈드드크
自e404「g드
0e40零杜E'
n分4n4FF경
ESP.ZC
ㅐE드．1
OPOPOPOPU81-ISOUI:ll태톄
"nkjnH"SP"nLㄴ
衿（)U
IHC
ESI.며결ORDPTR55볍〔ESP+34]
하눼,「r二
E마《．야결ORDPTRDS:tE自X+!J
ECX.DU()RDPTR05:tECX]
CL.머·TEPTRDS:［티甘X]
ERX
TEST
J댕Z
C니
SHt)R
〔ㄴ
ㅜfjpr。d녜C.0040465e
U8
r1P
티樹．EDX
ER:;:,4
아刃RT니prㅇd니0.00404665
r■．·．'S츤U
INF○:
15itdearfㅇryㅇu
thattheadVanCed
patchingwi∥dig
deeperinthiscal-
N町
ㄴ2c
p '
'IP
LSS
nEE
0닌404LFC
n·】呱皿．.
肉욜홑욥ㅗ슬‘'
冬83ECZC
드6
8B742434
츤드C즌
8D5001
8049oe
>8슴08
40
84C9
7C「--.
ZBCZ
8〕FS自4
.v7307
>32C0
makesusjump
이…nㅇttㅇ
XORAL,AL
3
「Jprㅇ巾．。．ee429CC4
prod·C.oe41FeEe
.eC
:':,E톄쑈
B시SP臼
0e404677
0040467)
0040467E
00404692
004e4683
004046e7
00404〔SC
0e40468B
0040468C
7르E드
68BSE042ee
JNS
衿）R
POP
nOD
RET"
PUSH
PUSH
「’USH
CnLL
RDD
ㅜEST
님NZ
PUSH
LER
PUSH
LER
PUSH
nDD
PUSH
CnLL
하緞RlrfJ배
fjprod니C』
ERX.［져ORC
d니C.O04O46EE
e42Ee88
ijkl삐。pqt$tuu닐ㅐ9좝＂
80442408
50
8D4C2410
551〔ESP+8〕
EFIX
ECX。
히
83C'03
56
ES7FE40000
tofindwhy
andwhere
C'15'Jy
ESErTO
rL r
nL=F「
Ju삐p$
EAX15setthat
「r。．00404677.e驪빻0469B

To find why and where EAX is set that

왜 그리고 어디에서 EAX가 set 되는지 찾자.

Makes us jump or not to XOR AL, AL

XOR AL, AL에서 Jump하거나 하지 않을 수 있다.

Scroll down

Scroll 내려.

Let's try intermediate patching and see if it works.

NOTE : advanced patching is often required !!! (See later parts in this series)

중간 patch를 해라. 그리고 어떤 일을 하는지 봐.

기록 : 진화된 patching은 자주 요구된다 !!!(이 series의 나중 part를 봐)

시스템 생성 대체 텍스트: 덛「쬐
TR55:rESP+34]
ㅜhisWil-
registerus
OdU
貼麗mbleat
·睡v恥1----
陋FIll轍thNOP$
-Asse劤‘ICancel-
d니C.e04e4665
0429CC4
.4IFOEe
push<enter)toassemble
.．山麗■■
．·뻐

This will register us

Push <enter> to assemble

등록할 수 있다.

Assemble 하기 위해 <enter>를 눌러.

And save the changes

바뀐 것을 저장해.

;)

;)

Under another name

다름 이름으로

And press <enter> to save

저장하기 위해 <enter>를 눌러.

Load the patched program and verify

Patch 된 program을 load 해 그리고 검증 해

;)

1. **Testing the patched app**

And run

실행 해.

Mmmm, see this here …

… no unregistered

음, 여기를 봐.

Unregistered가 없다.

Aha, and this works too

And what if we ….

아하, 우리는 할 수 있다.

만약 우리가…

시스템 생성 대체 텍스트: ：뿟무뻐■■b
2 2 10
1 . · . ' · · ' I
질－--------.-－…
Zoe油n眈I嚆〕Ra勅勿”w販蠟（er
l口山）ns
屢】出me.,f
凶孰ow·’f
凶油a·JPg
긔 肉d
孑（·andsnaam
가긔기―기기―
B"tan截蹙en l더ctLlreRes
」璽愛
巨Erlab始Rotation
「RemoteCon眈혀
佇HeIPinPage
0042e430
ee420435
Oe420437
0042043R
0042043C
더q·1)q'1」1찻
66.81384D驪겸 CllP냈尸DPTRDS'tERX],드
.v75IF IJ꾜SHORTrjprod니c.ee42
8B483C ＂대』ECX.대튤（)RDPTR【ys요LE
e3CS …RDOECX.ERX
8139드04드e00oCnP미刃ROPTRDS:【ECX],
''7〔 '층 'IN' q눼npT '습^"＾려·.^〕q'1乙
vers즐onZ,O,O,22
w『Pr岬amID「－ ?＝締
규즉－d經-
CanC님

!

Let's close and restart huh

닫고 재시작 하자.

What do you think ???

어떻게 됐을 거라 생각해?

시스템 생성 대체 텍스트: .뜁驥醜尸톄합軫뻐）
：邙ㄱ드 「盤knn히츤仔휘炙二．.:
_i'.1盼．
，功嫩C＝ㅇ없인ㄴ
-
-
e
마 Mak
2
_A巾”」·
10 _
쇼닝（en耽IL〕Ra功勿轍．販냈乙er
」 匡】d
，욘닉
며U，僭
出me.glf
孰ow．寧f
硼ha。jPg
巳凶凶回
Bestandsr'aam
B轍and竗en【祗欌藤s
■－7긔 Cancef-
。幽愛
羈一一
FEnableRotation
rRemofet沁n眈혀
盧H轍hPage
versi。nZ,O,O,22
W松．
Pr어yamID
ap汕：··r커）헝楡vi?柳
Iena151
」F .66:813840驪눼
ㅑ、:T .v751F
C『IP呱）RDPTR
F7予j
Up낙‘U낙璜r
0042043n
0e42e43C
00420442
8B48
e3CS
8139
.v7512
3C
드0450嶼〕以
05:tE댜日.
prㅇd니o.oe4
DPTRDS딩L
X
PTRDS:【ECX】,
ㅐ戚必Pas一d
IOK -
rl힝n힝기
HCC
CIEE
円OUDD
J"n
C飇
J＂乙
미刃RD
앗퀼ORT
b」7닐므·．탬·…r씸‘
시pr。duc.0e42．댜뱃

;)

1. **Conclusion**

In this part 11, the primary goal was to learn to think like a reverser by simply following the indications from Olly's Pane window while patching an application at intermediate level.

이번 part11에서, application을 중간 level로 patching 할 때 중요한 목표는 Olly's Pane window에서 간단히 지시자를 따라가며 배우고 생각하기 위해 reverser 같이 해야한다.

I hope you understood everything fine and I also hope someone somewhere learned something from this. See ma back in part 12 ;)

네가 모든 것을 좋게 이해했기를 희망한다. 또한 누구든지 어디서든지 이것에서 무언가를 배웠으면 좋겠다. Part 12에서 보자.

The other parts are available at

다른 parts는 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 tutorial에 시간을 투자해준 너에게 감사한다.