API Redirect on Themida

부경대학교 정보보호동아리 CERT-IS

김연재 / Yeonjae Kim

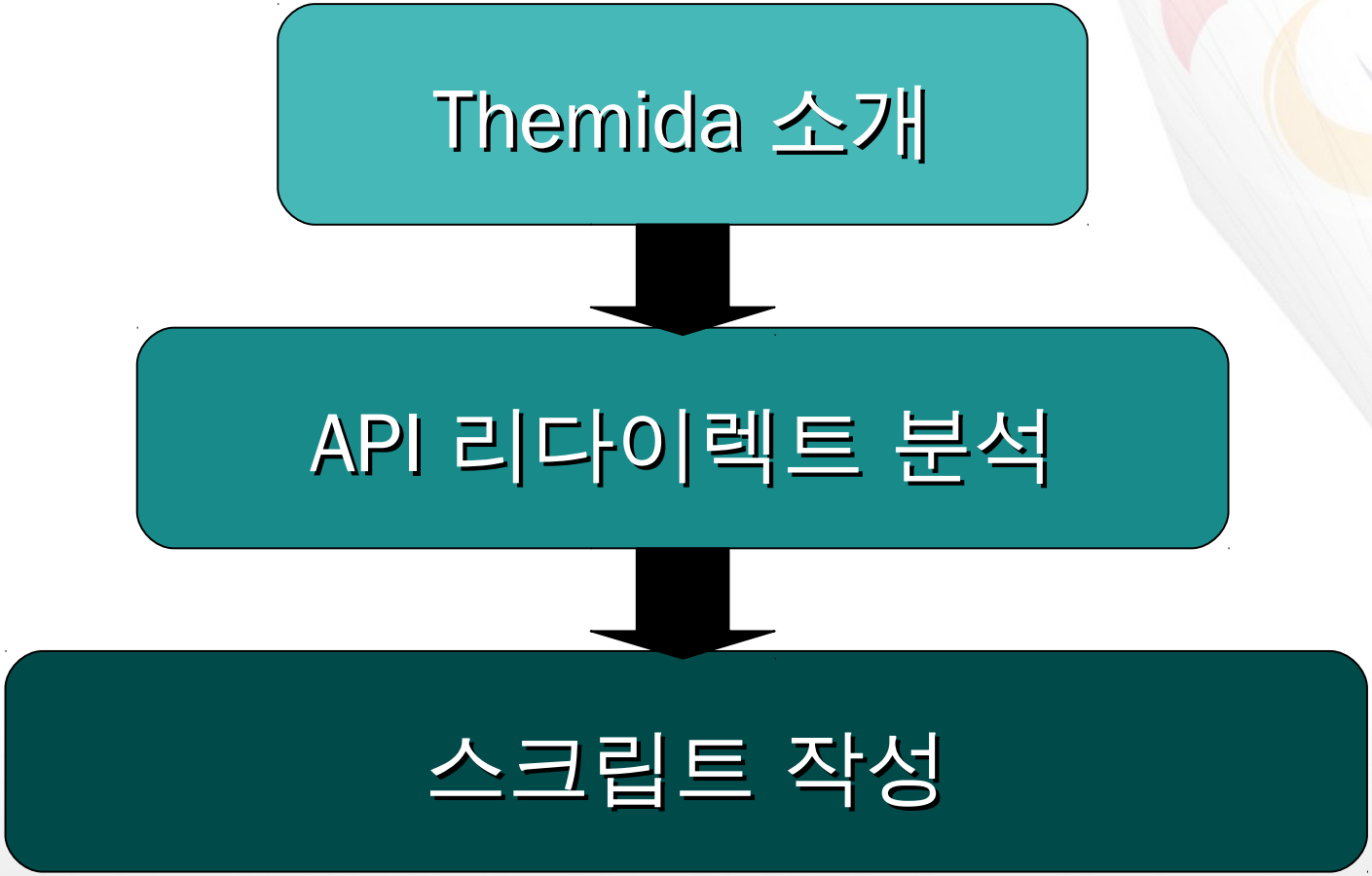
e-mail : 6l4ck3y3@gmail.com

twitter : @6l4ck3y3

KISA 한국정보보호진흥원

KUCIS 대학정보보호동아리연합회

순서



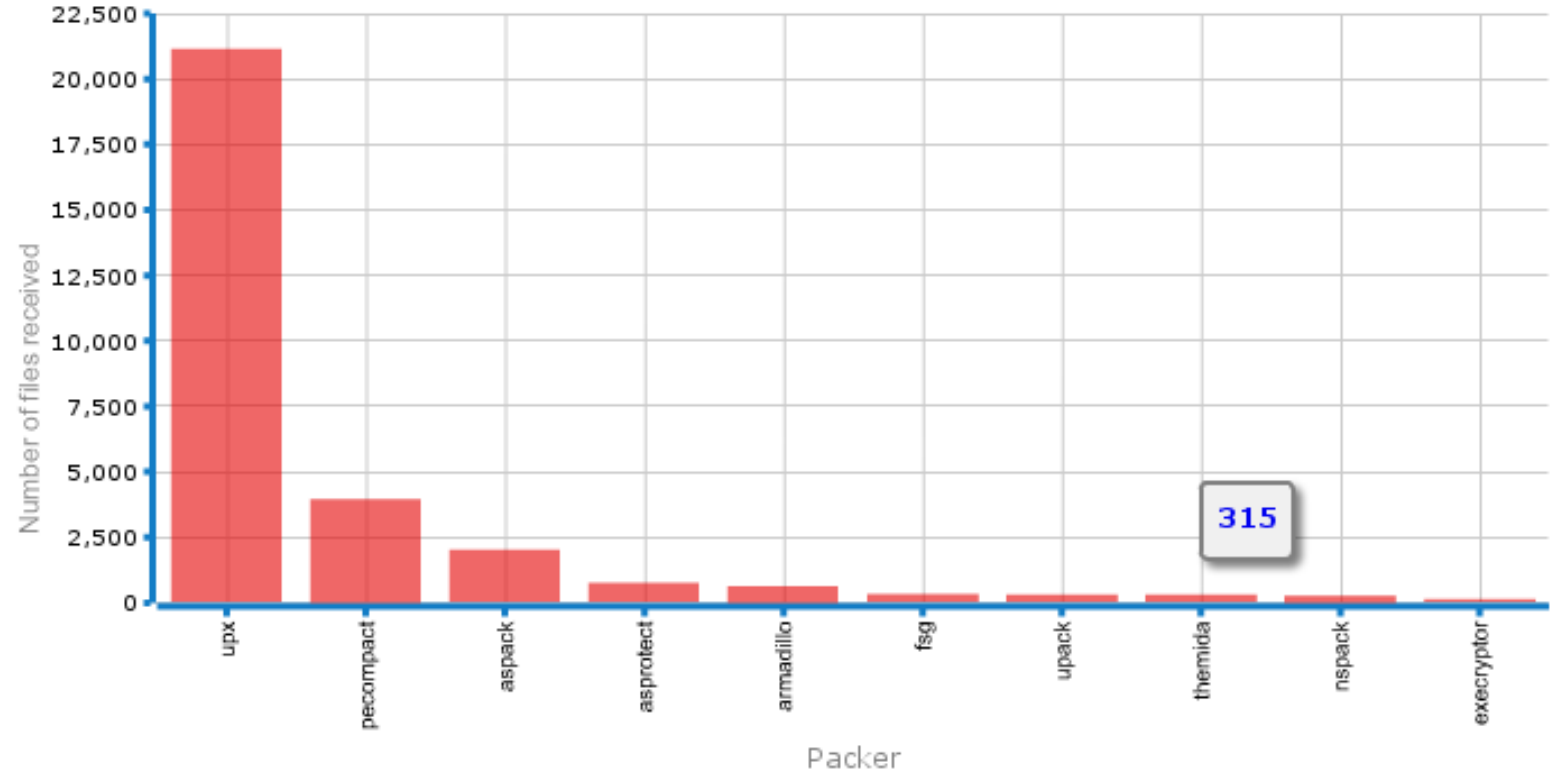
KISA 한국정보보호진흥원
KUCIS 대학정보보호동아리연합회

Themida 소개

Oreans Technology

상용 프로텍터

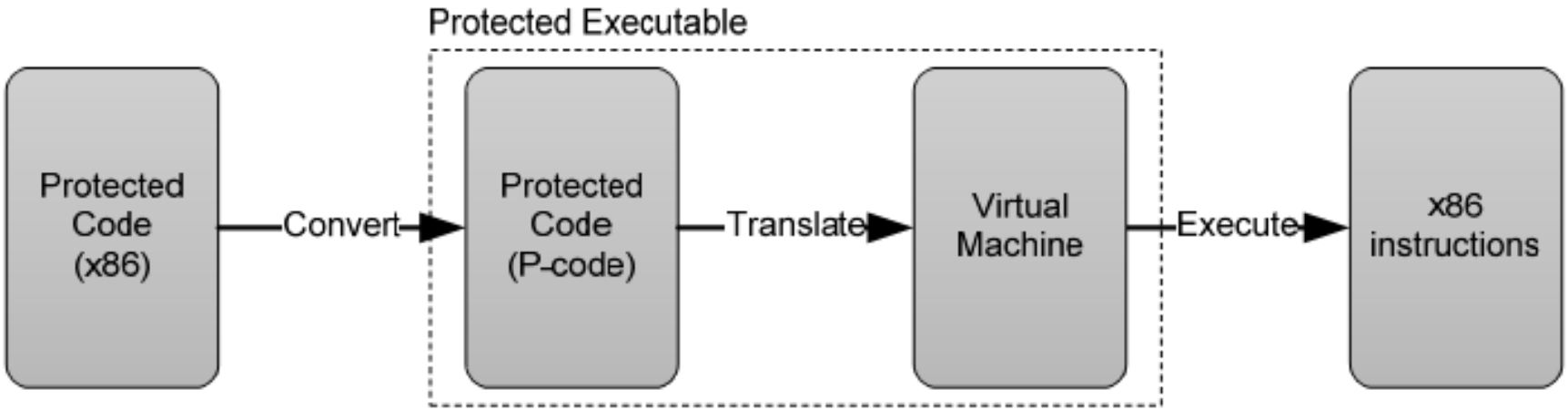
149 € = 225,747 원



http://www.virustotal.com/stats.html

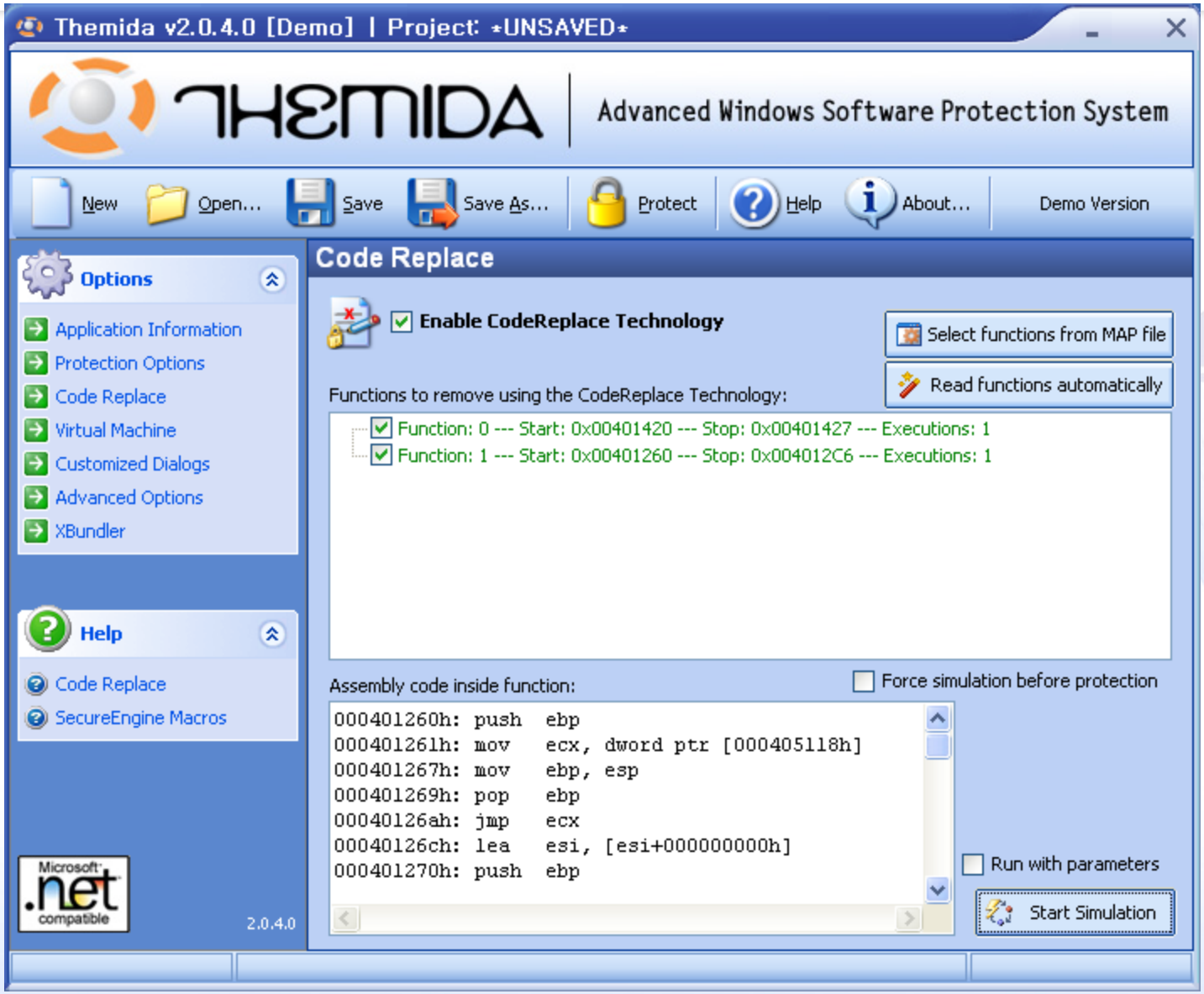
KISA 한국정보보호진흥원
KUCIS 대학정보보호동아리연합회

코드 가상화



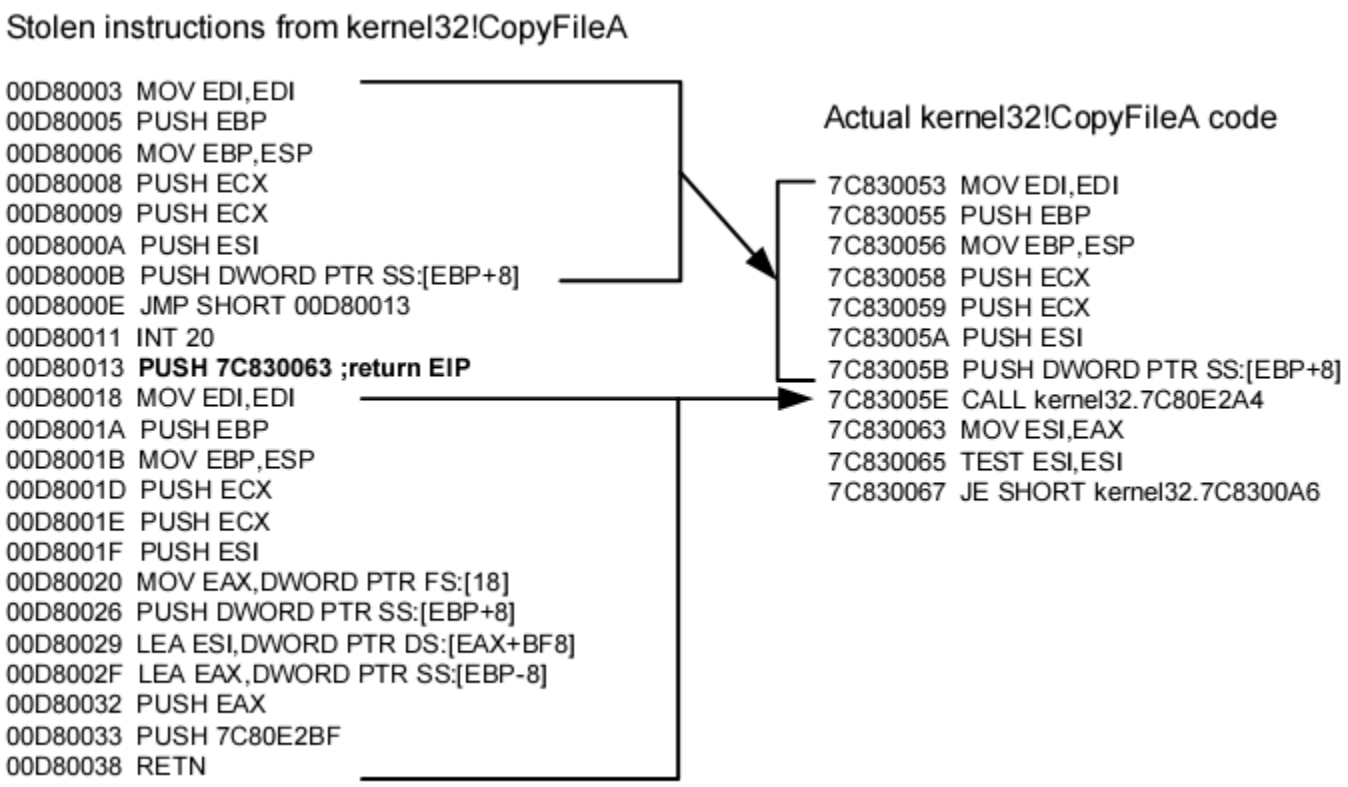
The Art of Unpacking

KISA 한국정보보호진흥원
KUCIS 대학정보보호동아리연합회



KISA 한국정보보호진흥원
KUCIS 대학정보보호동아리연합회

API 리다이렉트



KISA 한국정보보호진흥원
KUCIS 대학정보보호동아리연합회

KISA 한국정보보호진흥원
KUCIS 대학정보보호동아리연합회

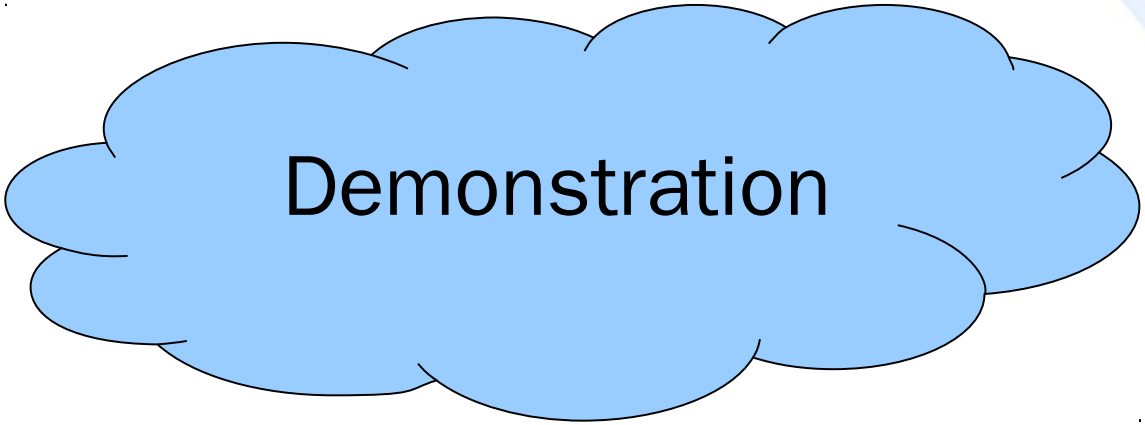
API 리다이렉트 분석

정상적인 루틴과 비교

```
0040128C     90              NOP
0040128D     90              NOP
0040128E     90              NOP
0040128F     90              NOP
00401290  ;  55              PUSH EBP
00401291  .  89E5            MOV EBP,ESP
00401293  .  83EC 18         SUB ESP,18
00401296  .  C74424 0C 200   MOV DWORD PTR SS:[ESP+C],20
0040129E  .  C74424 08 003   MOV DWORD PTR SS:[ESP+8],ThemidaE.00403   ASCII "themida 2.0.4.0"
004012A6  .  C74424 04 103   MOV DWORD PTR SS:[ESP+4],ThemidaE.00403   ASCII "API Re-Direct ??"
004012AE  .  C70424 000000   MOV DWORD PTR SS:[ESP],0
004012B5  .  E8 B6060000     CALL <JMP.&USER32.MessageBoxA>             MessageBoxA
004012BA  .  83EC 10         SUB ESP,10
004012BD  .  B8 00000000     MOV EAX,0
004012C2  .  C9              LEAVE
004012C3  L. C2 1000         RETN 10
004012C6     90              NOP
004012C7     90              NOP
004012C8     90              NOP
004012C9     90              NOP
004012CA     90              NOP
004012CB     90              NOP
```

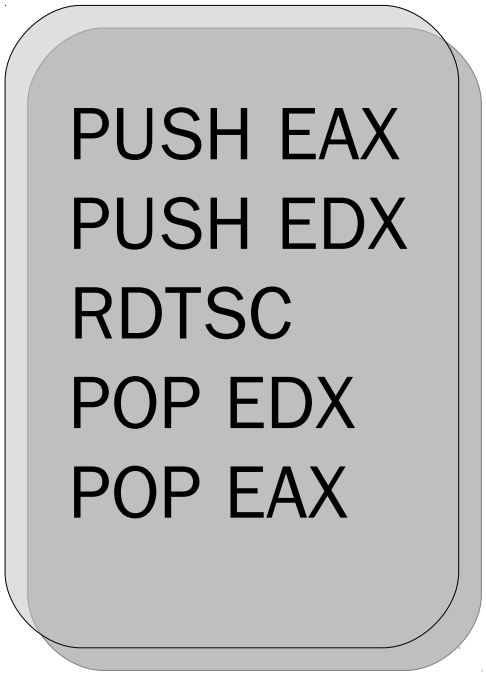
```
0040128C  90              NOP
0040128D  90              NOP
0040128E  90              NOP
0040128F  90              NOP
00401290  55              PUSH EBP
00401291  89E5            MOV EBP,ESP
00401293  83EC 18         SUB ESP,18
00401296  C74424 0C 20000 MOV DWORD PTR SS:[ESP+C],20
0040129E  C74424 08 00304 MOV DWORD PTR SS:[ESP+8],ThemidaE.00403 ASCII "themida 2.0.4.0"
004012A6  C74424 04 10304 MOV DWORD PTR SS:[ESP+4],ThemidaE.00403 ASCII "API Re-Direct ??"
004012AE  C70424 00000000 MOV DWORD PTR SS:[ESP],0
004012B5  E8 B6060000     CALL ThemidaE.00401970
004012BA  83EC 10         SUB ESP,10
004012BD  B8 00000000     MOV EAX,0
004012C2  C9              LEAVE
004012C3  C2 1000         RETN 10
004012C6  90              NOP
004012C7  90              NOP
004012C8  90              NOP
004012C9  90              NOP
004012CA  90              NOP
004012CB  90              NOP
```

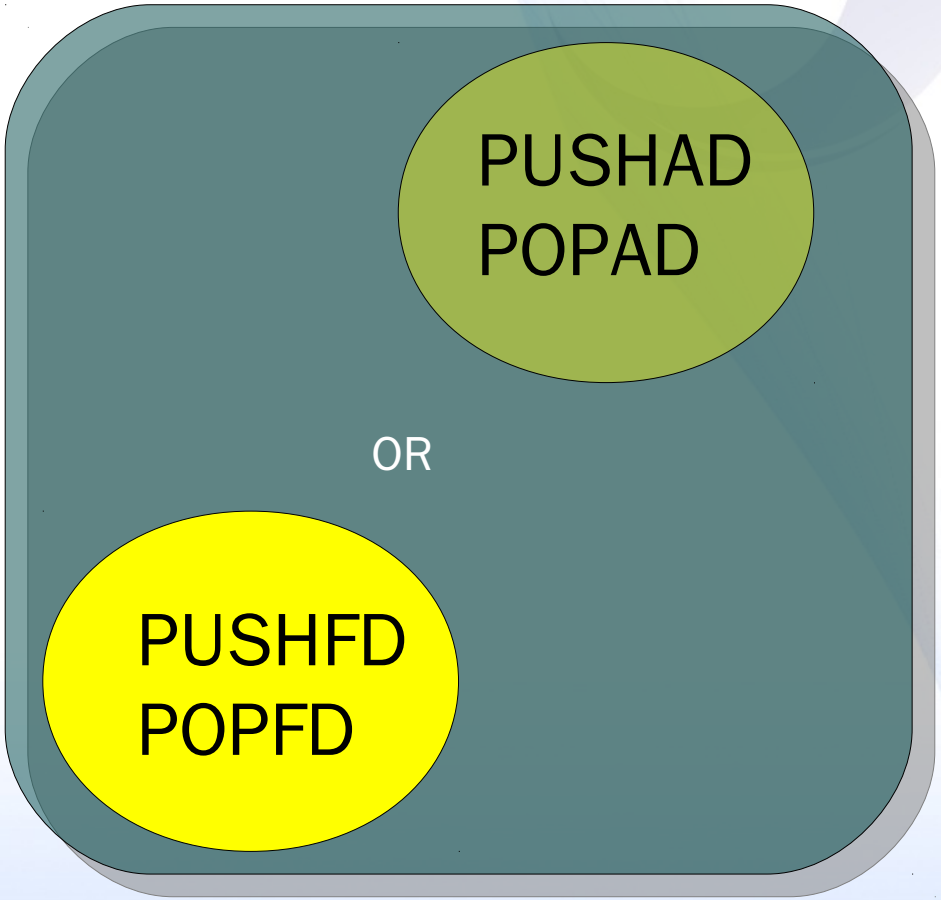
리다이렉트



난독화

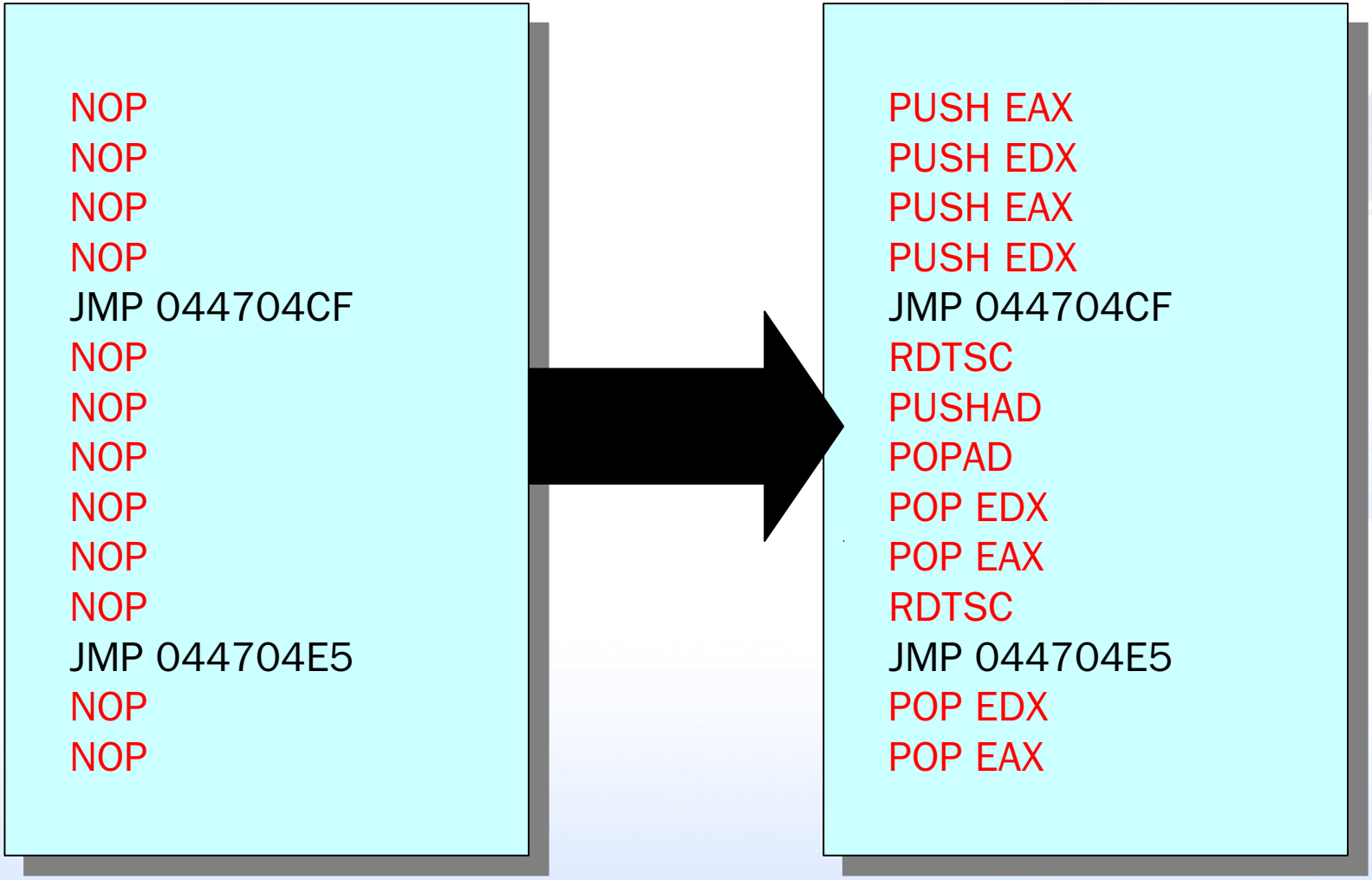
패턴 1


PUSH EAX
PUSH EDX
RDTSC
POP EDX
POP EAX


PUSHAD
POPAD
OR
PUSHFD
POPFD

패턴 2

난독화


NOP
NOP
NOP
NOP
JMP 044704CF
NOP
NOP
NOP
NOP
NOP
NOP
JMP 044704E5
NOP
NOP
PUSH EAX
PUSH EDX
PUSH EAX
PUSH EDX
JMP 044704CF
RDTSC
PUSHAD
POPAD
POP EDX
POP EAX
RDTSC
JMP 044704E5
POP EDX
POP EAX

스크립트 작성

revealapi.py

```
from immlib import *

def main (args):

   imm = Debugger ()

   eip = orig_eip = imm.getRegs ()['EIP']
```

revealapi.py

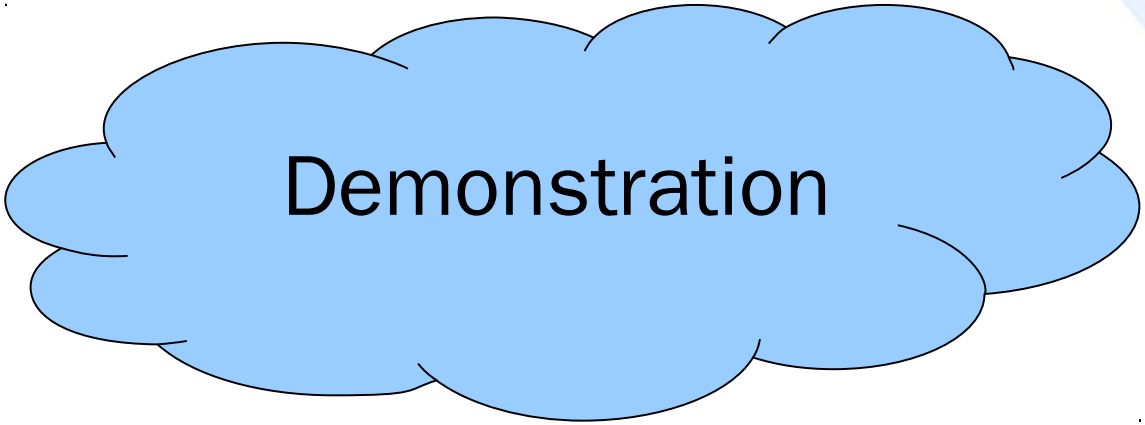
```
while (eip < 0x10000000 and limit):
        opcode = imm.Disasm (eip)

    if (opcode.isJmp () or opcode.isConditionalJmp () or opcode.isCall ()):
        eip = opcode.getJmpAddr ()

    elif opcode.isRet ():
        return "API was NOT found. Maybe here is a local func."

    else:
        eip = eip + int (opcode.getSize ())
```

revealapi.py



THANK YOU !

「The Art of Unpacking」by Mark Vincent Yason

「Design and Implementation of Virtualized Code Protection(VCP) For Anti-Reverse Engineering」by 이용일

「GRAY HAT PYTHON」by Justin Seitz

우리의 도전이 바로 보안입니다.