1st CodeEngn Seminar

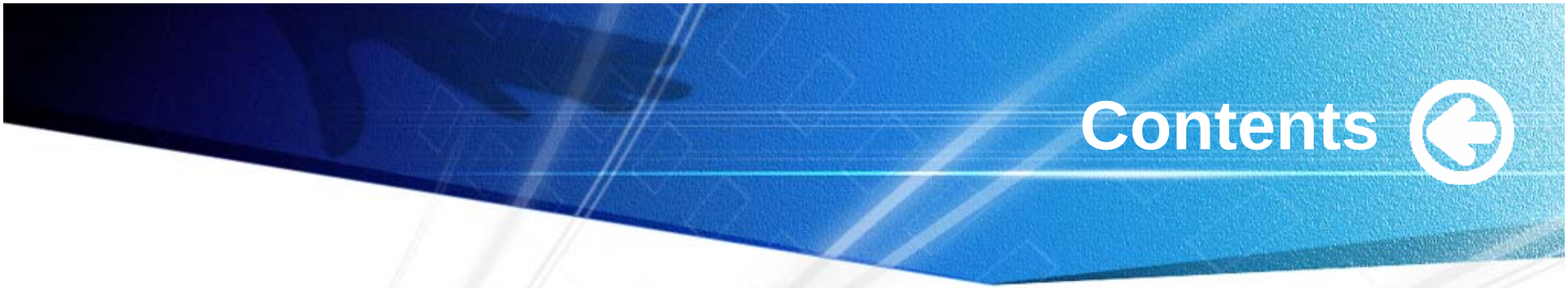
http://www.codeengn.com

Manual Unpacking for Newbies

송창현
aka.MrBrown@gmail.com

CodeEngn

Contents



❖ 언패킹 (실행압축해제)

- 언패킹이란 보호를 목적으로 암호화 및 압축된 실행파일(패킹된 파일)을 원상태로 해제 하는 것을 의미한다.

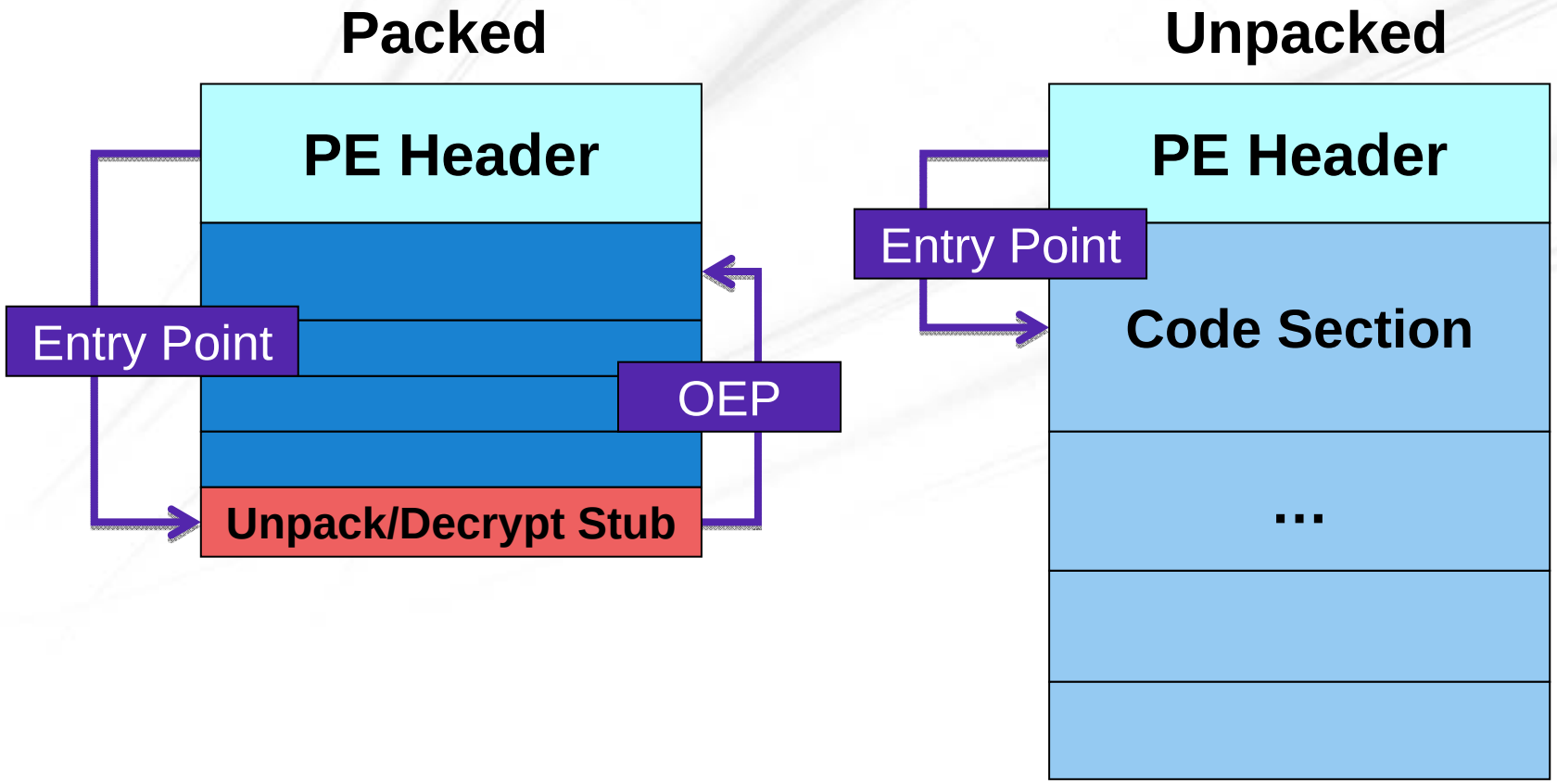
패킹 & 언패킹의 구조와 원리

- **PE** 구조

IMAGE_OPTIONAL_HEADER

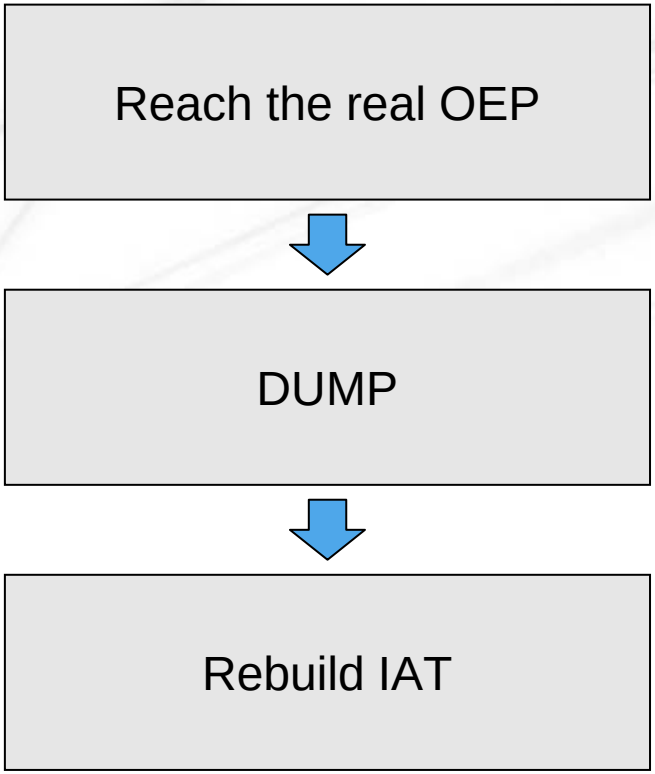
→ AddressOfEntryPoint
→ ImageBase (0x00400000)
→ BaseOfCode (0x00001000)

패킹 & 언패킹의 구조와 원리



패킹 & 언패킹의 구조와 원리

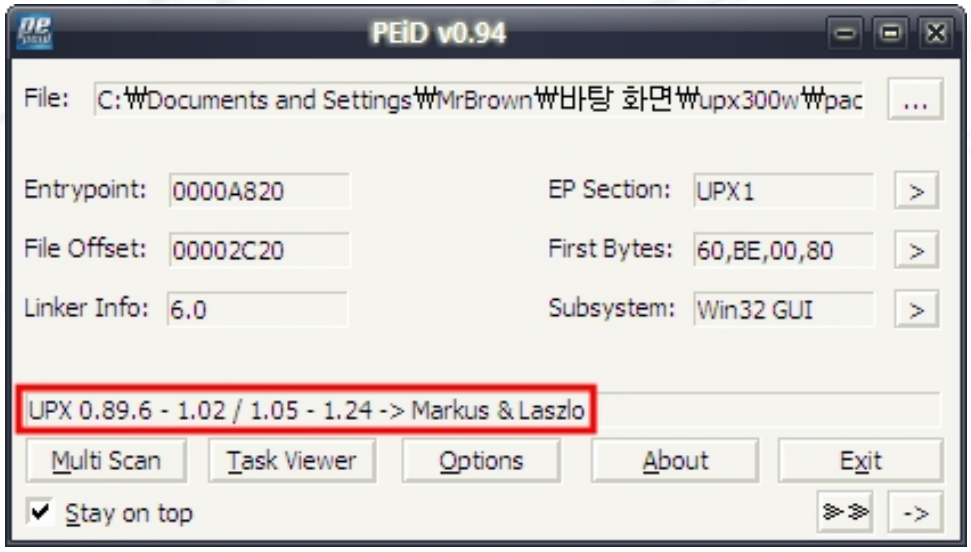
- 일반적인 매뉴얼 언패킹 과정



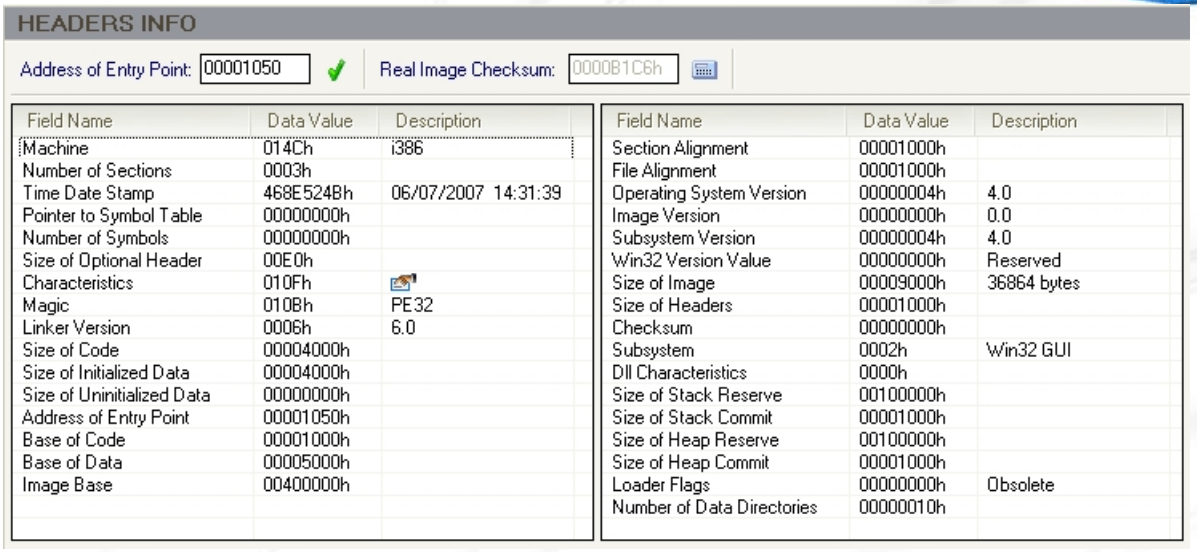
❖ UPX (Ultimate Packer for eXecutables)

- Open Source
- Compress , Decompress
- Linux , Dos , Windows 32-bits

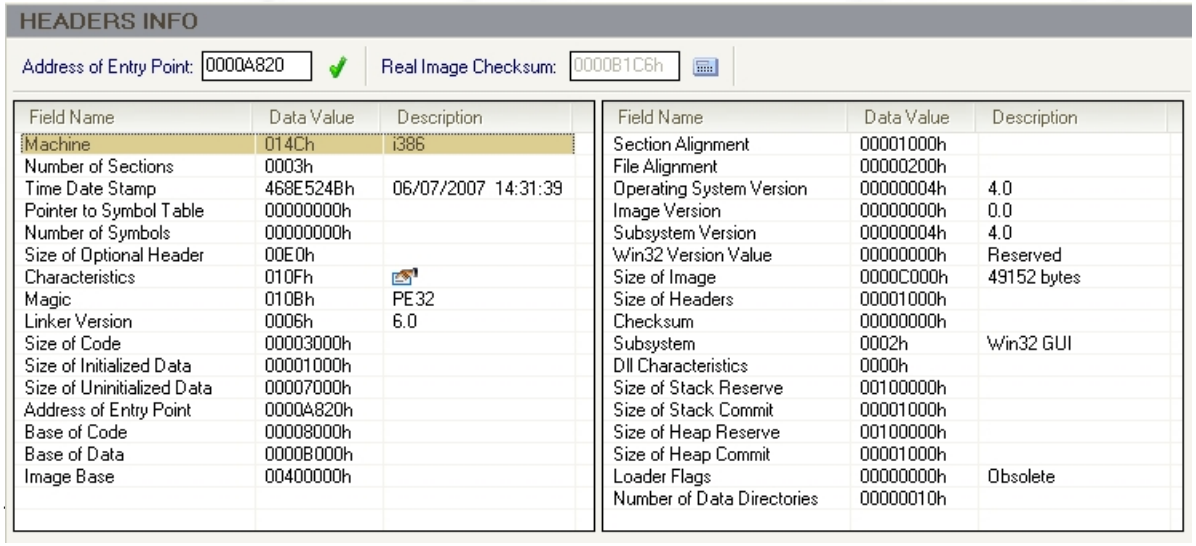
Packed


PEiD v0.94
File: C:₩Documents and Settings₩MrBrown₩바탕 화면₩upx300w₩pac
...
Entrypoint: 0000A820
EP Section: UPX1
File Offset: 00002C20
First Bytes: 60,BE,00,80
Linker Info: 6.0
Subsystem: Win32 GUI
UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
->>

기초 매뉴얼 언패킹



← Original



← Packed

CodeEngn

기초 매뉴얼 언패킹

Original

SECTION HEADERS

00001000

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
.text	000035FEh	00401000h	00004000h	00001000h	60000020h	
.rdata	000007DEh	00405000h	00001000h	00005000h	40000040h	Import Table
.data	000029FCh	00406000h	00003000h	00006000h	C0000040h	

Packed

SECTION HEADERS

00000400

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Direct
UPX0	00007000h	00401000h	00000000h	00000400h	E0000080h	
UPX1	00003000h	00408000h	00002A00h	00000400h	E0000040h	
UPX2	00001000h	0040B000h	00000200h	00002E00h	C0000040h	Import Table

UPX 시연

실행 압축된 악성코드

MEW 시연 (변형된)

실행파일 보호 기법

언패킹을 방해하는 각종 기법

Anti Debug

IsDebuggerPresent()
ZwQueryInformationProcess()
NtGlobalFlag
Process32Next()
ZwSetInformationThread()
UnhandledExceptionFilter()
TerminateProcess()

Anti BP/Trace

Anti BP(File streams,
SEH , etc …)
RDTSC
GetTickCount()

ETC

Junk Code
IAT change
Stolen Byte
polymorphic

언패킹을 방해하는 각종 기법

- **Sample Code**

```
; --- Anti Debugging using IsDebuggerPresent() ---

  CALL   DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>]
  CMP   EAX,1            ; active = 1 , not active = 0
  JE   found_debugger_action


; ------------------------------------------------------
```

언패킹을 방해하는 각종 기법

- **Sample Code**

```
; --- Anti Tracing(single stepping) using RDTSC ---
        RDTSC
        MOV   ECX,EAX
        RDTSC
        SUB   EAX,ECX
        CMP   EAX,0FFFh
        JAE   found_debugger_action
; ------------------------------------------------------------
```

Protector

ARM Protector, ASProtect, ExeShield, **Themida(**막강**)**, VMProtect, NTkrnl Protector, Yoda Protector, SKVP, Nice Protect, GHF Protector … …

[시연]

Stolen Byte (crackme)

IAT 수정 (변형된 UPX)

Yoda Protector 1.03 (Full Option)

Thanks to…

[자료 제공 해주신분들 ㄱㅅ]

SlaxCore

Certlab

시연자료

http://mrbrown.linuxstudy.pe.kr/codeengn/data.zip

CodeEngn

Thank You !

Q & A