



1st CodeEngn Seminar

<http://www.codeengn.com>

Manual Unpacking for Newbies

송창현

aka.MrBrown@gmail.com



<http://www.CodeEngn.com>

Contents

-  언패킹이란?
-  패킹 & 언패킹의 구조와 원리
-  기초 매뉴얼 언패킹
-  언패킹을 방해하는 각종 기법
-  프로텍터 언패킹



❖ 언패킹 (실행압축해제)

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

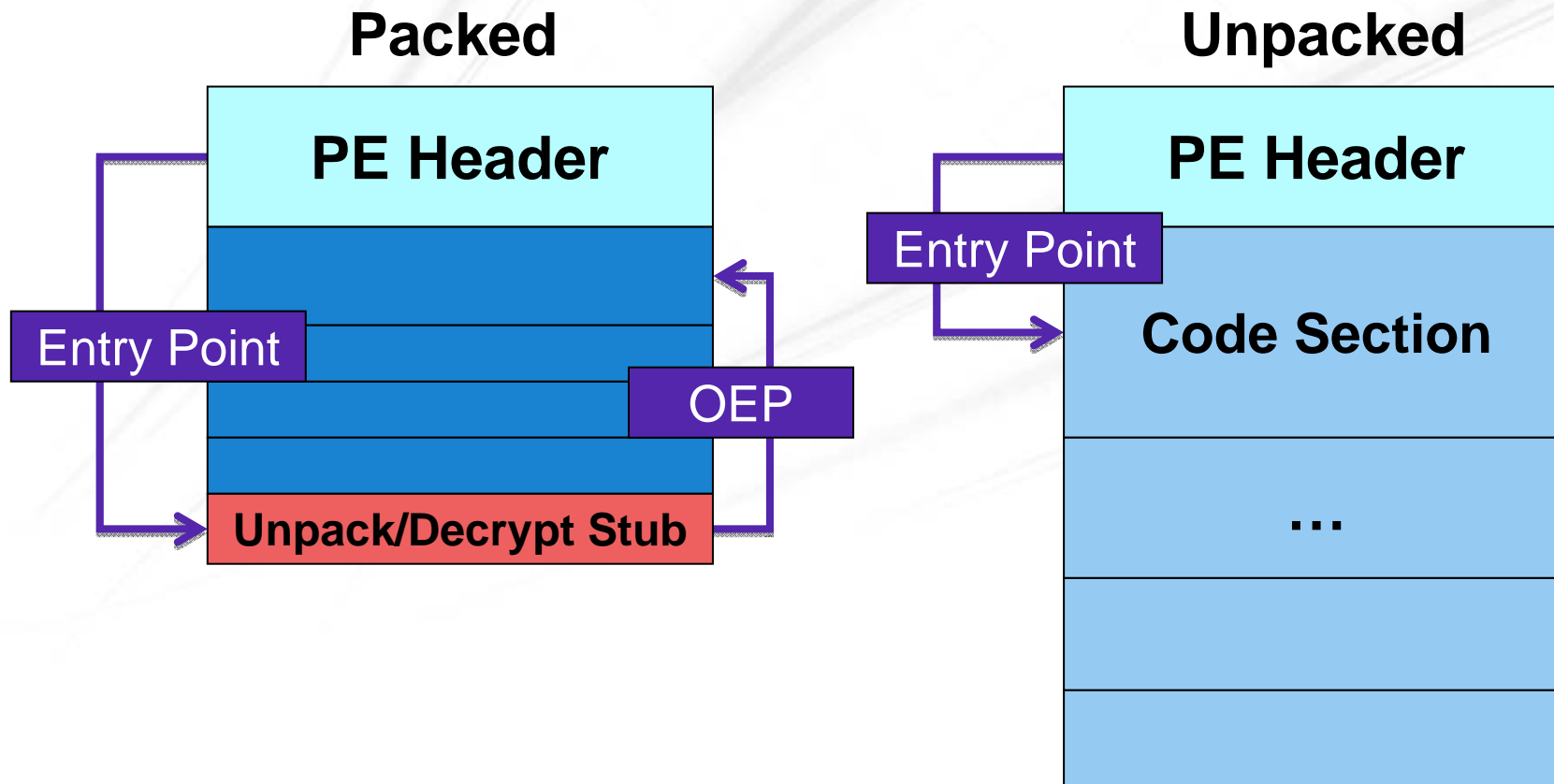


- **PE 구조**

IMAGE_OPTIONAL_HEADER

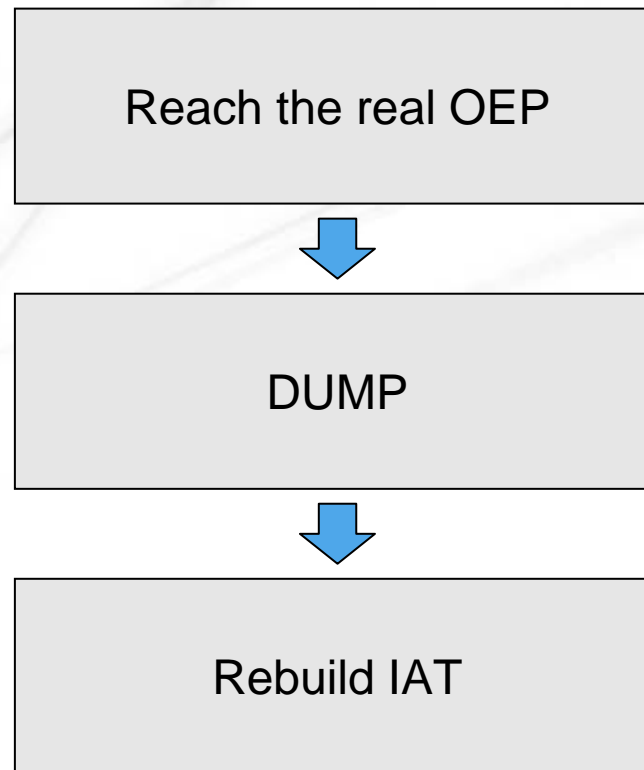
- AddressOfEntryPoint
- ImageBase (0x00400000)
- BaseOfCode (0x00001000)

패킹 & 언패킹의 구조와 원리





- 일반적인 매뉴얼 언패킹 과정





❖ UPX (Ultimate Packer for eXecutables)

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

기초 매뉴얼 언패킹



Packed



기초 매뉴얼 언패킹



HEADERS INFO

Address of Entry Point: Real Image Checksum:

Field Name	Data Value	Description	Field Name	Data Value	Description
Machine	014Ch	i386	Section Alignment	00001000h	
Number of Sections	0003h		File Alignment	00001000h	
Time Date Stamp	468E524Bh	06/07/2007 14:31:39	Operating System Version	00000004h	4.0
Pointer to Symbol Table	00000000h		Image Version	00000000h	0.0
Number of Symbols	00000000h		Subsystem Version	00000004h	4.0
Size of Optional Header	00E0h		Win32 Version Value	00000000h	Reserved
Characteristics	010Fh		Size of Image	00009000h	36864 bytes
Magic	010Bh	PE32	Size of Headers	00001000h	
Linker Version	0006h	6.0	Checksum	00000000h	
Size of Code	00004000h		Subsystem	0002h	Win32 GUI
Size of Initialized Data	00004000h		Dll Characteristics	0000h	
Size of Uninitialized Data	00000000h		Size of Stack Reserve	00100000h	
Address of Entry Point	00001050h		Size of Stack Commit	00001000h	
Base of Code	00001000h		Size of Heap Reserve	00100000h	
Base of Data	00005000h		Size of Heap Commit	00001000h	
Image Base	00400000h		Loader Flags	00000000h	Obsolete
			Number of Data Directories	00000010h	

← Original

HEADERS INFO

Address of Entry Point: Real Image Checksum:

Field Name	Data Value	Description	Field Name	Data Value	Description
Machine	014Ch	i386	Section Alignment	00001000h	
Number of Sections	0003h		File Alignment	00000200h	
Time Date Stamp	468E524Bh	06/07/2007 14:31:39	Operating System Version	00000004h	4.0
Pointer to Symbol Table	00000000h		Image Version	00000000h	0.0
Number of Symbols	00000000h		Subsystem Version	00000004h	4.0
Size of Optional Header	00E0h		Win32 Version Value	00000000h	Reserved
Characteristics	010Fh		Size of Image	0000C000h	49152 bytes
Magic	010Bh	PE32	Size of Headers	00001000h	
Linker Version	0006h	6.0	Checksum	00000000h	
Size of Code	00003000h		Subsystem	0002h	Win32 GUI
Size of Initialized Data	00001000h		Dll Characteristics	0000h	
Size of Uninitialized Data	00007000h		Size of Stack Reserve	00100000h	
Address of Entry Point	0000A820h		Size of Stack Commit	00001000h	
Base of Code	00008000h		Size of Heap Reserve	00100000h	
Base of Data	0000B000h		Size of Heap Commit	00001000h	
Image Base	00400000h		Loader Flags	00000000h	Obsolete
			Number of Data Directories	00000010h	

← Packed

기초 매뉴얼 언패킹



Original

SECTION HEADERS						
Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
<input checked="" type="checkbox"/> .text	000035FEh	00401000h	00004000h	00001000h	60000020h	
<input checked="" type="checkbox"/> .rdata	000007DEh	00405000h	00001000h	00005000h	40000040h	Import Table
<input checked="" type="checkbox"/> .data	000029FCh	00406000h	00003000h	00006000h	C0000040h	

Packed

SECTION HEADERS						
Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
<input checked="" type="checkbox"/> UPX0	00007000h	00401000h	00000000h	00000400h	E0000080h	
<input checked="" type="checkbox"/> UPX1	00003000h	00408000h	00002A00h	00000400h	E0000040h	
<input checked="" type="checkbox"/> UPX2	00001000h	0040B000h	00000200h	00002E00h	C0000040h	Import Table

기초 매뉴얼 언패킹



UPX 시연



실행 압축된 악성코드

MEW 시연 (변형된)

언패킹을 방해하는 각종 기법



실행파일 보호 기법

언패킹을 방해하는 각종 기법



Protection Technic

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



■ Sample Code

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

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

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



■ 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 ㄱ]

SlaxCore

Certlab

시연자료

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

Thank You !

Q & A

