دوره ی آموزش ساختار فایلهای PE

Site: onhexgroup.ir

Youtube: onhexgroup

Telegram: onhex_ir

X: onhexgroup

Github: onhexgroup

ارائه شده توسط

onhexgroup

Youtube: onhexgroup

Optional Header

- مهمترین هدر **NT Headers**
- دو تا نسخه داره:
  - نسخه ۳۲ بیتی ۳۱ عضو (**BaseOfData**) و نسخه ی ۶۴ بیتی ۳۰ عضو داره.
  - فیلدهای زیر در ۳۲ بیتی سایز **DWORD** اما در ۶۴ بیتی **ULONGLONG** :

- **ImageBase**
- **SizeOfStackReserve**
- **SizeOfStackCommit**
- **SizeOfHeapReserve**
- **SizeOfHeapCommit**

- در داخل **winnt.h** با عنوان **IMAGE_OPTIONAL_HEADER32** و **IMAGE_OPTIONAL_HEADER64** تعریف شدن.

Site: onhexgroup.ir

ساختار Optional HEADER

- **Magic**: مشخص کننده معماری فایل اجرایی هستش. ۳ تا مقدار داره:
  - PE32 : 10B
  - PE32+:20B
  - ROM Image :107
- **MajorLinkerVersion**: نسخه ی اصلی لینکر
- **MinorLinkerVersion**: نسخه ی فرعی یا جزئی لینکر

x: onhexgroup

ساختار Optional HEADER

- **SizeOfCode**: سایز بخش کد (.text)
- **SizeOfInitializedData**: سایز بخش داده هایی که مقداردهی اولیه شدن. (.data - .rdata)
- **SizeOfUninitializedData**: سایز بخش داده هایی که مقداردهی اولیه نشدن. (.bss)

Telegram: onhex_ir

ساختار Optional HEADER

- **AddressOfEntryPoint**: آدرس نقطه ورود به برنامه یا **EP**
  - آدرس مجازی نسبی (**RVA**)
  - معمولا در:
    - برنامه ها، اولین دستور اجرایی
    - در درایورها تابع **DriverEntry** یا **DriverInit**
    - در **DLL** تابع **DllMain** اما الزامی نیست، اگه نباشه مقدارش صفره

Github: onhexgroup

ساختار Optional HEADER

- **BaseOfCode**: آدرس (**RVA**) شروع بخش کد
- **BaseOfData**: آدرس (**RVA**) شروع بخش داده– فقط در ۳۲ بیتی

Github: onhexgroup

ساختار Optional HEADER

- **ImageBase**: آدرس ترجیحی اولین بایت در مموری
  - باید مضربی از **64k** (**0x10000**)
  - بدلیل **ASLR (Address Space Layout Randomization)** نادیده گرفته میشه.
  - **relocation section (.reloc)**
  - مقدار پیش فرض برای **DLL**ها **0x10000000** برای **Windows CE** برابر **0x10000** و بقیه **0x400000**