دوره ی آموزش ساختار فایلهای PE

Site: onhexgroup.ir

Youtube: onhexgroup

Telegram: onhex_ir

X: onhexgroup

Github: onhexgroup

ارائه شده توسط

onhexgroup

Site: onhexgroup.ir

ساختار Optional HEADER

- **SectionAlignment** : مشخص کننده سایز تراز هر سکشن در مموری. (آدرس شروع مضربی از این مقدارست)
  - مقدار پیش فرض یک صفحه = 4kb=4096b=0x1000
  - باید بزرگتر یا مساوی **FileAlignment** (سکتور/صفحه)
- **FileAlignment** : مشخص کننده سایز تراز هر سکشن در فایل. (آدرس شروع مضربی از این مقدارست)
  - مقدار پیش فرض معمولا ۵۱۲=0x200

Youtube: onhexgroup

ساختار Optional HEADER

- **MajorOperatingSystemVersion** :
- **MinorOperatingSystemVersion** :
- نسخه ی حداقلی اصلی و فرعی سیستم عامل رو نشون میده.
- لیست کامل

Youtube: onhexgroup

ساختار Optional HEADER

- **MajorImageVersion:**
- **MinorImageVersion:**
- نسخه ی اصلی و فرعی فایل رو نشون میده.

Youtube: onhexgroup

ساختار Optional HEADER

- **MajorSubsystemVersion:**
- **MinorSubsystemVersion:**
- نسخه ی حداقلی اصلی و فرعی زیرسیستم رو مشخص میکنن.
  - منظور از Subsystem: محیط اجرای باینری. مثلا کامندلاین، گرافیکی و ...

Github: onhexgroup

ساختار Optional HEADER

- **Win32VersionValue**: یک مقدار رزرو شده که همیشه برابر صفر.
- **SizeOfImage**: مشخص کننده سایز باینری در مموری
  - به مضربی از **SectionAlignment** گرد میشه.
- **SizeOfHeaders**: مجموع **DOS Header** و **DOS stub** و **NT Headers** و **Section Headers**
  - به مضربی از **FileAlignment** گرد میشه.
  - در حالت کلی اگه اندازه فایل رو منهای اندازه کل**Section** ها کنیم، این مقدار بدست میاد یا به عبارتی میشه گفت، این مقدار مشخص کننده آفست اولین **Section** هستش .

Telegram: onhex_ir

ساختار Optional HEADER

- **Checksum** : یک مقدار عددی که برای بررسی یکپارچگی فایل استفاده میشه.
- داخل **IMAGHELP.DLL** تعریف شده. (MapFileAndCheckSumA)
- برای موارد زیر محاسبه و بررسی میشه:
  - همه‌ی درایورها
  - **DLL**هایی که در زمان بوت لود میشن (**Ntdll** و ...)
  - **DLL**هایی که وارد پروسس های حیاتی ویندوز میشن (**kernel32** و ...)

Youtube: onhexgroup

ساختار Optional HEADER

- **Subsystem** : محیط اجرای باینری رو مشخص میکنه.
  - لیست