دوره ی آموزش ساختار فایلهای PE

Site: onhexgroup.ir

Youtube: onhexgroup

Telegram: onhex_ir

X: onhexgroup

Github: onhexgroup

ارائه شده توسط

onhexgroup

Youtube: onhexgroup

Section Table

- فایل **PE** از بخش های (**Section**) مختلفی تشکیل میشه.
- هر **Section** دیتای و هدف خاصی داره.
- برای مدیریت این **Section**ها از **Section Table** استفاده میکنیم.
- بلافاصله بعد از **Optional Header** میاد.
- هر ردیف از **Section Table** رو **Section Header** میگیم.
- تعداد ورودی ها در **FileHeader** فیلد **NumberOfSections**

x: onhexgroup

Section Header

- ساختار **Section Header** در **winnt.h**: (۴۰ بایت)

```
typedef struct _IMAGE_SECTION_HEADER {
    BYTE    Name[IMAGE_SIZEOF_SHORT_NAME];
    union {
            DWORD   PhysicalAddress;
            DWORD   VirtualSize;
    } Misc;
    DWORD   VirtualAddress;
    DWORD   SizeOfRawData;
    DWORD   PointerToRawData;
    DWORD   PointerToRelocations;
    DWORD   PointerToLinenumbers;
    WORD    NumberOfRelocations;
    WORD    NumberOfLinenumbers;
    DWORD   Characteristics;
} IMAGE_SECTION_HEADER, *PIMAGE_SECTION_HEADER;
```

Telegram: onhex_ir

Section Header

- **Name**: آرایه ای به اندازه ی IMAGE_SIZEOF_SHORT_NAME که نام **Section** هارو مشخص میکنه.
  - IMAGE_SIZEOF_SHORT_NAME برابر ۸ است.
- این فیلد یک رشته‌ی ۸ بایتی است که بصورت **UTF-8** و **Null Padding** هستش.
- **Null Padding** با **Null Terminated** فرق داره.

Github: onhexgroup

Section Header

- **PhysicalAddress** یا **VirtualSize**:
  - **PhysicalAddress** : معمولا در سیستمهای قدیمی استفاده میشه و مربوط به لوود فایل در مموری هستش.
  - **VirtualSize** : سایز واقعی **Section** در مموری (بعد لوود)
- **VirtualAddress** : در فایلهایی اجرایی ، آدرس اولین بایت **Section**، وقتی در مموری لوود میشه رو نگه میداره. **(RVA)**
  - مضربی از **SectionAlignment**

Site: onhexgroup.ir

Section Header

- **SizeOfRawData**:
  - برای فایلهای **Object**: سایز **Section**
  - برای فایلهای اجرایی: سایز سکشن روی دیسک
- مضربی از **FileAlignment**
- در **PE BEAR** با عنوان **RAW SIZE**

Youtube: onhexgroup

Section Header

- **PointerToRawData**: آدرس آفست اولین بایت از داده Section درون فایل.
- برای ایمیجها مضربی از **FileAlignment**
- اگه بخش فقط حاوی داده های **Uninitialized Data** باشه، مقدارش صفر خواهد بود.
- در **PE Bear** با عنوان **RAW Addr**
- اگه مقدار **Raw ADDr** رو با **Raw size** جمع کنیم، آدرس سکشن بعدی مشخص میشه.

Youtube: onhexgroup

Section Header

- **PointerToRelocations**: آدرس افست که ابتدای جداول **Relocation** برای این سکشن از اونجا شروع میشن. برای ایمیجها مقدارش صفره.

- **NumberOfRelocations**: تعداد ورودی‌های **relocation** در اون سکشن. برای ایمیجها مقدارش صفره.

Youtube: onhexgroup

Section Header

- **PointerToLineNumbers**: آفست به جدول **LineNumbers** سورس‌کد مرتبط با این سکشن. با توجه به منسوخ شدن **COFF debugging**، استفاده نمیشه. مثلاً آدرس 00401020 در فایل اجرایی، مربوط به خط ۴۲ از **main.c** هستش.

- **NumberOfLinenumbers**: تعداد ورودی های **LineNumbers** منسوخ شده.

Youtube: onhexgroup

Section Header

- **Characteristics**: فلگ هایی که ویژگیهای Section نشون میدن.
- لیست کامل