دوره ی آموزش ساختار فایلهای PE

Site: onhexgroup.ir

Youtube: onhexgroup

Telegram: onhex_ir

X: onhexgroup

Github: onhexgroup

ارائه شده توسط

onhexgroup

Youtube: onhexgroup

NT Headers

- با عنوان **PE Headers** هم شناخته میشه.
- تاریخچه مایکروسافت:
  - فرمت **DOS HEADER – MZ** - مثلا **MS DOS**
  - فرمت **NE Header – NE (New Executable)** – مثلا **Windows 3.1**
  - فرمت **PE** در **NT – NT (New Technology)** **Windows NT 3.1 – Header**

Site: onhexgroup.ir

ساختار
NT HEADERS

- از سه بخش تشکیل شده:
  - Signature
  - File Header
  - Optional Header
- ساختارش در winnt.h با عنوان IMAGE_NT_HEADERS و در دو نسخه تعریف شده:
  - ۳۲ بیتی با عنوان IMAGE_NT_HEADERS32
  - ۶۴ بیتی با عنوان IMAGE_NT_HEADERS64
- تفاوت نسخه ها در Optional Header هستش.

x: onhexgroup

Signature در NT HEADERS

- اولین عنصر در ساختار **NT Headers**
- سایزش **DWORD**
- یک مقدار ثابت داره: **0x00004550** اسکی: **PE\0\0**
- بعنوان امضاء میشه ازش استفاده کرد.