دوره ی آموزش ساختار فایلهای PE

Site: onhexgroup.ir

Youtube: onhexgroup

Telegram: onhex_ir

X: onhexgroup

Github: onhexgroup

ارائه شده توسط

onhexgroup

Youtube: onhexgroup

Rich Header

- یک ساختار مستند نشده و ویژه مایکروسافت هستش.
- توسط ابزارهای کامپایل مایکروسافت بخصوص ویژوال استدیو درج میشه.
- بین **DOS STUB** و **NT Header**
- شامل اطلاعاتی در خصوص محیط ساخت فایل اجرایی داره.

Site: onhexgroup.ir

ساختار
Rich Header

- **DanS ID**: مقدار DWORD هستش که XOR شده و بعنوان امضاء در نظر میگیریم. همیشه وجود داره.
- **Checksumed Padding**: سه تا DWORD هستن که مقدارشون XOR شده و مقدارشون همیشه صفره.
- **Rich ID**: امضای این هدر و مقدارش XOR نشده.
- **Checksum**: یک مقدار ۳۲ بیتی که کلید XOR هستش و بقیه فیلدهارو با این کلید میشه استخراج کرد.

x: onhexgroup

ساختار
Rich Header

- **Comp ID**: اطلاعات اصلی این هدرکه بصورت جفت **DWORD** و **XOR** شده، هستن.
  - شامل سه مقدار:
    - شناسه ساخت (**Build ID**)
    - شناسه محصول (**Type ID** یا **Product ID**)
    - تعداد دفعات استفاده در فرایند ساخت (**Count**) هستش.

Youtube: onhexgroup

COMP ID آنالیز Rich Header