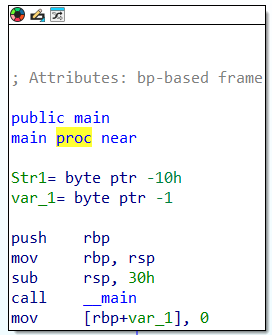
IDA: Disasassemblr ve debugger aracı diyebiliriz. Yazılımların assembly kodlarını analiz ederek tersine mühendislik yapmaya yarar.

Özellikle zararlı yazılımların analizinde ve hata ayıklamada kullanılır. Gelişmiş özellikleri sayesinde, kodun nasıl çalıştığını anlamaya yardımcı olur.



Burada ki **public main**; main fonksiyonunun başlangıcını ifade eder. **Main proc near** ise fonksiyonun “yakın” bir prosedür olduğunu belirtir. Yani aynı kod segmentinde çağırılabilir.

**Str1** ve **var\_1** adlı değişkenlerin stack üzerindeki yerlerini ifade eder.

**Str1= byte ptr -10h =** Str1, RBP'ye göre -0x10 (16) offsetinde.

**var\_1= byte ptr -1 =** var\_1, RBP'ye göre -0x1 (1) offsetinde.

!!! **Stack**, program çalışırken fonksiyonların yerel değişkenlerini, geri dönüş adreslerini ve diğer geçici verileri saklamak için kullanılan bir bellek bölgesidir. **Offset**, bir değişkenin referans noktasına olan uzaklığını belirtir.

**push rbp =** Stack'e mevcut RBP değerini kaydeder. (Önceki fonksiyonun stack frame'i korunur.)

**mov [rbp+var\_1], 0**

**mov komutu**, bir veriyi kaynaktan hedefe taşımak için kullanılır. Veriyi kopyalar, ancak kaynağı değiştirmez. mov [rbp+var\_1], 0 örneğinde olduğu gibi, bu komut stack üzerinde bir değişkene sıfır değeri yazmak için kullanılır.