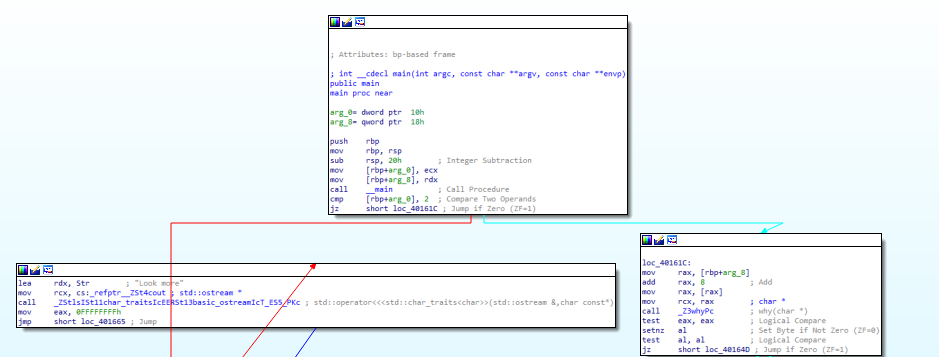
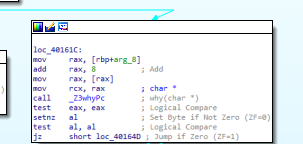
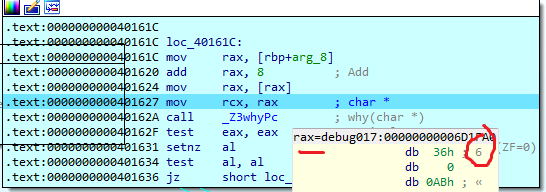
İlk çalıştırma

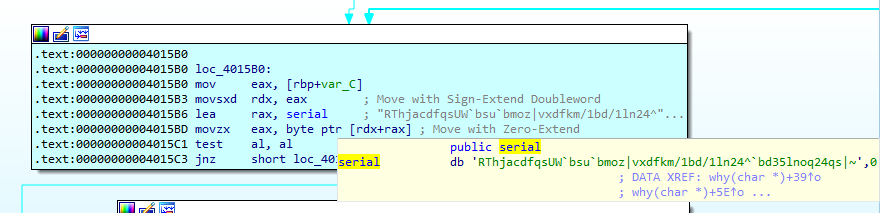
İda kullanarak analiz ettiğimde main fonksiyonunun beni yönlendirdiği “ look more ” metnini fark ettim. 

[rbp+arg\_0] ve 2 yi karşılaştırıyor ve beni oraya yönlendiriyordu. [rbp+arg\_0] degiskenini geriye doğru izlediğimde ecx te var olan degeri atadığını gördüm. Programı argüman vermeden çalıştırdığımda eax değeri 1 oluyor, herhangi bir argüman verdiğimde eax degeri 2 oluyor ve karşılaştırma işleminden sonra ZF=1 oluyor ve beni sağdaki fonksiyona yönlendiriyordu



Bu fonksiyonda call \_Z3whyPc fonksiyonu dikkatimi çekti. 

Programa verdiğim “6” değeri bu 40162A adresindeki \_Z3whyPc fonksiyonuna gönderiliyordu.



Fonksiyonun içine girdiğimde “serial” isimli flag olma ihtimali yüksek olan bu kodu buldum. Çeşitli şifreleme metodlarıyla decode etmeye çalıştım işe yaramadı.

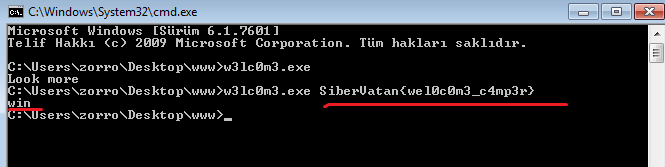
Sonra F5 basıp pseudocode görüntüleyerek algoritmayı visual studioya atıp ne yapmaya çalıştığını anlamak için debug yaptım.

Serial= RThjacdfqsUW`bsu`bmoz|vxdfkm/1bd/1ln24^`bd35lnoq24qs|~

Visual studioda debug yaparak şifreleme algoritmasını çözdüm. Verilen stringin ardışık ikili karakterlerinin arasında kalan harflerle verdiğimiz argümanı kıyasladığını gördüm(ilk karakterden büyük ikinci karakterden büyük olan karakteri arıyor).

Verilen seriali ikili harflere ayırıp flagi buldum.

RT,hj,ac,df….



Flag: SiberVatan{wel0c0m3\_c4mp3r}

Hazırlayan : Tarık yıldız