



esnasında içerisinde şifrelenmiş olarak tutulan kod parçacıklarını, 0x1000 byte boyutundaki 0x00390000 bellek alanına kopyaladığını ve XOR ile şifrelenmiş kod parçacıklarını çözdüğünü gördüm. Çözme işlemi kısa bir süre takip ettikten sonra ortaya <http://217.23.7.125/xxx.exe> web adresi çıkıverdi. Bu web adresi, exploit.exe adı altında kayıt etmiş olduğumuz bu zararlı yazılımın bir [trojan downloader](#) olduğunu ve ana zararlı yazılımı yani tuş kayıt yazılımını, içerisine gömülü olan bu web sitesinden indirerek çalıştırmak üzere tasarlandığı anlamına geliyordu.

Haliyle bu zararlı yazılımın otomatik olarak tuş kayıt yazılımını bu web sitesinden indirip kurmasına göz yumamayacağım için manuel olarak xxx.exe yazılımını indirip hex editör ile incelemeye ve stringlere göz atmaya başladım. Kısa bir inceleme sonucunda bu yazılımın [leetlogger](#) adında bir tuş kayıt yazılımı olduğu ortaya çıktı ve dinamik analize gerek kalmadı.

Uzun uzun yazılar okumaktansa video izlemeyi her zaman tercih eden ve bu nedenle yazılarımda olabildiğince videolara yer vermeye çalışan ve sizde ister istemez bu alışkanlığı kazandırmış biri olarak yaptığım analizi özetleyen 4 dakikalık ufak bir video hazırladım, herkese iyi seyirler dilerim.