# Zararlı Yazılım Analizi Dersi

written by Mert SARICA | 15 January 2015

Bildiğiniz üzere günümüzde bilginin hızlı ve kolay erişilebilir olması günlük hayatta işlerimizi kolaylaştırdığı gibi aynı şekilde art niyetli kişilerin de işlerini kolaylaştırmaktadır. Bu sayede art niyetli kişiler, sistemlere nasıl sızabileceklerini, nasıl zararlı yazılım geliştirebileceklerini kısa sürede öğrenebilmekte ve öğrendiklerini kısa bir sürede uygulamaya geçirebilmektedirler. Bu durum hem kurumlar hem de son kullanıcılar için büyük bir tehdit oluşturmaktadır. Özellikle son yıllarda bazı devletler tarafından, politik ve stratejik bilgileri uzun süreli izleme, manipüle ve tahrip etme adına gerçekleştirilen siber saldırılarda zararlı yazılımların kullanılması ulusal güvenlik için de bir bir tehdit oluşturmaktadır. Sonuç itibariyle günümüzde zararlı yazılım analizi hem kurumlar hem de devletler için önemli bir ihtiyaç ve gereksinim haline gelmiştir.

Siber güvenlik alanında bu ve benzeri ihtiyaçların ve gereksinimlerin karşılanabilmesi adına Bahçeşehir Üniversitesi'nde 2013 yılında Siber Güvenlik Yüksek Lisans Programı hayata geçirildi. Bu program ile kamu ve özel sektörün ihtiyaç duyduğu siber güvenlik uzmanlarını yetiştirilmesi hedefleniyor.

Şubat ayı (2. dönem) itibariyle bu programda ikinci defa, Zararlı Yazılım Analizi 101 dersi vererek katkıda bulunacağım.

Bu derste teorik bilginin yanı sıra zararlı yazılımların, sistem (davranışal) analizi, yazılım (statik ve dinamik kod analizi) analizi, bellek analizi vb. çeşitli analiz yöntemleri ile farklı platformlarda nasıl analiz edilebileceği uygulamalı olarak öğrenciler ile paylaşılacaktır.

Zararlı Yazılım Analiz 101 dersi, Salı günleri saat 19:00 – 21:30 arasında, Bahçeşehir Üniversitesi Beşiktaş Kampüsü'nde verilecektir.

Programa başvurmak için http://www.bahcesehir.edu.tr/fenbilimlerienstitusu/basvuru_kayit adresini ziyaret edebilir, detaylı bilgi almak için ise Yrd. Doç. Dr. Selçuk Baktır (selcuk.baktir@bahcesehir.edu.tr) ile iletişime geçebilirsiniz.