BBG 644 Kötücül Yazılım Analizi: Araçlar ve Teknikleri

Bu Dersi Nasıl Yapacağız?

1. Konu ile ilgili video kaynaklardan yararlanacağız
2. Kötücül yazılımın analiz programlarından yararlanacağız
3. Arasınav yapmayacağız
4. Final sınavı yapmayacağız
5. Her öğrenci bir proje çalışması seçip bu çalışmanın sunumu (15 dakika, %50) ve raporundan (%50) not alacak
6. Sunum konularını belirlemek için yeterince zaman var, derste tartışacağız
7. Sunum ve rapor Bilişim Enstitüsü bitirme projesi formatında olacak, dosyalar basılı olarak teslim edilecek
8. Yoklama ve devam zorunluluğu olmayacak

Dersin Künyesi

- Zararlı Yazılım analiz için gerekli alt yapıyı oluşturmak
- Temel düzeyde Zararlı Yazlım tespiti
- Temel düzeyde statik ve dinamik analiz yapabilmek
- Genel olarak Zararlı Yazılım davranış yöntemlerini tanıyabilmek
- Zararlı Yazılım analizi yapabilme

Projeler

- Zararlı Yazılımların analizi uygulamalar ile ilgili güncel Zararlı Yazılımlar ele alınacaktır
- Proje raporunuzu Bilişim Enstitüsü bitirme projesi formatında hazırlayınız
- Ocak ayı sonuna kadar tüm öğrenciler proje konularını belirlemelidir

- Proje sunumları öğrenci sayısına göre dönemin son 1 veya 2 haftasında gerçekleştirilecektir
- Her öğrenci tek başına proje hazırlayacaktır
- Sunumlar 15 dakikayı geçmeyecek şekilde düzenlenmelidir.

- Konular listesi şöyledir (bu liste genişletilebilir):

    - Zararlı Yazılım tespit yöntemleri
    - Trojen Uygulamaları
    - Rootkit uygulamaları
    - Keylogger uygulamaları
    - Vorm uygulamaları
    - Virüs uygulamaları
    - Zombie, spam gönderme uygulamaları
    - Ransomware uygulamaları
    - Kripto kitleyicileri uygulamaları
    - Zararlı Yazılım oluşturma aşamaları
    - Genel Zararlı Yazılım analiz yöntemleri
    - Statik Analiz
    - Dinamik Analiz
    - Kod analizi
    - Güncel Zararlı Yazılımlar
    - Zararlı Yazılım kullanım amaçları
    - Anti-analiz yöntemleri
    - Hesperbot analizi
    - Fatmal analizi
    - Zararlı Yazılım analiz ortamı kurulması
    - Advanced Persistent Threat (APT) uygulamaları

- Her projede
    1. Projenin kablosuz iletişim boyutunun tanıtılması,
    2. Projenin iletişim boyutunun/ihtiyacının ve çözüm yöntemlerinin tanıtılması,
    3. Konunun geleceğe dönük projeksiyonu,
    4. Konunun bilişim alanı ile ilişkisi,
    5. Konu bilişim alanı dışında ise ilgili sektörle ilgili bilgilerin verilmesi
    6. Sonuçlar ve tartışma

  gibi tipik başlıklar ele alınmalıdır. Lütfen proje önerinizi öğretim üyesi ile tartışınız.

- *Neler teslim edilecek:* Proje raporu basılı olarak, sunum ve rapor karaikab at gmail dot com adresine elektronik olarak gönderilecek.
- *Ne zamana kadar:* Sunulması gereken tüm basılı ve elektronik materyal dönemin son haftasına girilmeden teslim edilmelidir.

Dersin Hocası

Dr. İlker Kara , karaikab at gmail dot com

Plan

- Günü belirlenecek, 18:15-21:00
- Ofis saatleri: Öğretim üyesinin müsait olduğu her zaman

Konu İle İlgili Çeşitli Kaynaklar

- Konu ile ilgili ders hocası tarafından hazırlanan eğitim notları
- Forensic toolkit programları
- Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software 1st Edition
- The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory
- ...

Son Güncelleme: 01 Ekim 2018