ABDULLAH GÜL ÜNİVERSİTESİ

OKULLARIN VEYA ÖĞRENCİLERİN İLGİ ALANALARINA GÖRE
VERİLEMESİ PLANLANAN
EĞİTİMLERDE SUNUM ÖRNEĞİ VE İÇERİĞİ

21. Yüzyılda
Siber Saldırılara
Pratik Önlemler
Dr. Öğr. Üyesi Samet TONYALI

KONUNUN İÇERİĞİ:

- Gündem
- Düşmanlarımızı Tanıyalım
- Riskler
- İstatistikler
- Siber Saldırılar ve Korunma Yöntemleri
- Mobil Zararlılar
- Kablosuz Ağlarda Güvenlik
- Halka Açık Kablosuz Ağlarda Güvenlik
- Tatilde Güvenlik
- Düşmanlarımızı Tanıyalım
- Zararlı/Kötücül/Kötü amaçlı yazılımlar (Malware)

Konuk programa ihtiyaç duyanlar

Tuzak kapısı (trap door)
Yazılım/mantık bombası (logic bomb)
Truva atı (trojan horse)
Virüs
Kötücül tarayıcı eklentileri, uzantıları, betikleri vb.

Düşmanlarımızı Tanıyalım

Bağımsızlar
Solucan
Zombi ağı (botnet)
Gelişmiş sürekli tehdit (advanced persistent threat/APT)

- Riskler
- Kimlik hırsızlığı
- Güven kaybı
- Veri kaybı
- Finansal kayıplar
- Biraz İstatistik
- %70 web sayfaları, %18 ofis belgeleri ve %12 yürütülebilir ve komut dosyaları
- CERT-GIB 2020 ilk yarı raporu

Analiz edilen e-postaların %43'ü casus yazılım ya da zararlı yazılımları indirmek için bağlantılar
Arka kapılar
Bankacılık truva atları

- Biraz İstatistik

Bunların üçte biri kullanıcı bilgileri, kredi kartı, banka giriş bilgileri veya diğer hassas bilgileri hedefliyor
Oltalama (kimlik avı) saldırıları pandemi sırasında nerdeyse iki katına çıktı
Sahte web sayfalarının %46'sı oltalama için

- Ağa bağlı diğer sistem ve cihazlara da bulaşmak
- Siber Saldırılar
- Oltalama saldırıları
- Hedefli oltalama ve sosyal mühendislik saldırıları
- Seksüel zorlama (Sextortion)
- Fidye yazılımları (Ransomware)
- Siber Saldırılar
- Nesnelerin interneti (IoT) ve akıllı ev cihazları
- Kullanıcıları aldatmaya yönelik yapay zeka ve sohbet botları
- Evden çalışan personeli hedefleyen saldırılar
- E-ticaret saldırıları
- Nasıl Korunabiliriz?
- Parola seçimleri
- Kaybolan ve çalınan cihazlar
- Olta e-postalara/SMSlere karşı önlemler
- Wi-Fi ve bluetooth
- VPN kullanımı
- USB kullanımı
- Mobil Zararlı Yazılımlar
- Mobil Zararlı Yazılımlar
- Android cep telefonlarının %87'sinde en az bir kritik zafiyet (Cambridge Üniversitesi)
- Android telefonların %95'I basit bir SMS ile hacklenebilir (Zimperium Labs)
- XcodeGhost milyonlarca iPhone kullanıcı adı ve parolayı çaldı
- Mobil Zararlı Yazılım Türleri
- Bankacılık zararlı yazılımları
- Mobil reklam zararlı yazılımları (Mobile Adware)
- Virüsler ve truva atları
- Mobil fidye yazılımları
- Mobil oltalama saldırıları
- Drive-by indirmeler

- Tarayıcı kaynaklı zafiyetler
- Ne Yapabilirler?
- Bankacılık bilgilerinizi çalar
- Kullanıcı bilgilerinizi çalar
- Kullanıcı verilerini izinsiz toplar ve satar
- Oltalama saldırıları düzenler
- Verilerinizi şifreler
- Cihazınızın kontrolünü ele geçirir
- Aynı ağda yer alan diğer cihazlara bulaşır
- Nasıl Engellenebilirler?
- "Hediye Kazandınız" bağlatılarına, WhatsApp'tan gelen bilinmedik linklere ve tanımadığınız kişilerden gelen "cazip teklif" içerikli SMS ve e-postalardaki linklere tıklamayın
- Android kullanıyorsanız Google Play Protect'i mutlaka etkin duruma getirin
- Nasıl Engellenebilirler?
- Play Store ve AppStore harici platformlardan uygulama indirmeyin
- Telefon ayarlarınızdan "Bilinmeyen Kaynaklar"dan gelen uygulamaların kurulumunu engelleyin
- İşletim sistemiyle oynanmış (Jailbreak/rootlanmış) telefonları kullanmayın
- Nasıl Engellenebilirler?
- Telefonunuza gelen işletim sistemi/uygulama güncellemelerini ivedilikle yapın
- Halka açık WiFi kullanıyorsanız kullanıcı adı ve parolanız ile giriş yapmanızı gerektiren işlemlerden uzak durun
- Tanımadıklarınızdan gelen e-postaları açmayın, açtıysanız herhangi bir linke tıklamayın veya varsa eklentiyi indirmeyin
- Nasıl Engellenebilirler?
- Mutlaka antivirus kullanın
- Kişisel güvenlik duvarı (firewall) kullanımını değerlendirin
- Uygulamayı indirmeden önce indirilme sayısına bakmak, uygulama geliştiricisini incelemek ve kullanıcı yorumlarını okumak ilk aşama
- Uygulamayı kurarken talep ettiği izinleri incelemek ikinci aşama
- Bulaştığı Nasıl Anlaşılır?
- Pil çok hızlı bitiyorsa
- Cihazın performansında beklenmedik düşüş varsa
- Veri kullanımında beklenmedik bir artış varsa
- Uygulamaların sıklıkla kendiliğinden açılması/kapanması, cihazın aşırı yavaşlaması, ekranın donması veya normalden fazla ısınması gibi durumlar yaşıyorsanız
- Bulaştığı Nasıl Anlaşılır?
- SMS mesajlarınız için bildirim gelmiyorsa veya bildirim gelmesine ragmen görüntüleyemiyorsanız
- Sizin tarafınızdan gerçekleştirilmemiş arama ya da mesajlar varsa
- Herhangi bir uygulamaya erişmeye çalıştığınızda karşınıza reklam kutucukları çıkıyorsa
- Bulaştığı Nasıl Anlaşılır?
- Sizin tarafınızdan yapılmamış parola yenileme, sosyal media hesaplarınızdan takip/beğeni/paylaşım yapılması, e-posta veya farklı gönderiler yapılması
- Bulaştıysa Ne Yapılmalı?
- Sektörde güvenilir bir antivirüs edinip cihazda tarama yaptırın
- İndirilmiş uygulamaların pil kullanımları kontrol edilmeli
- Bulaştıysa Ne Yapılmalı?
- Siz telefonu kullanmadığınız zamanda bile veri kullanımı yüksek uygulamalar incelenmeli, şüpheli görülen uygulamalar kaldırılmalı

- Son çare olarak telefonunuzu fabrika ayarlarına döndürebilirsiniz
- Kablosuz Ağların Güvenliği
- Kablosuz ağ adını (SSID) değiştirin
  Modem markasını gizleyecek bir isim seçin
- Varsayılan ağ parolanızı değiştirin
- Güçlü bir protokol kullanın
- Evde olmadığınızda modeminiz kapalı olsun
- Kablosuz Ağların Güvenliği
- Yönetim arayüzüne girişte güçlü parola kullanın
- DHCP özelliğini kapatın
- Modeminizi güncelleyin
- MAC adres filtreleme özelliğini kullanın
- Halka Açık
  Kablosuz Ağlarda Güvenlik
- Güvende olmadığınızı aklınızdan çıkarmayın
- Güvenli internet kullanım kurallarını hatırlayın
- Kullanmadığınız zaman kablosuz bağlantınızı kapatın
- Kişisel bilgilerinizi paylaşmayın
- Halka Açık
  Kablosuz Ağlarda Güvenlik
- VPN kullanın
- Şifreli bağlantıları tercih edin
- Paylaşımdaki dosyalara dikkat edin
- Cihazınızdaki otomatik bağlan özelliğini kapatın
- Tatilde Güvenlik
- Kendi kablonuzu, şarj aletinizi, adaptörünüzü yanınızda taşıyın ve sadece onları kullanın
- Araç kiralayacaksanız telefonunuzu araca bağlamayın
- Halka açık bağlantı noktalarından hassas verilere erişim sağlamayın
- Evinizdeki modemi kapatmayı unutmayın