TEMEL BİLGİ GÜVENLİĞİ-9

Ransomware (Fidyeci Yazılımlar)

Saldırganlar, Ransomware ile bilgisayar ve dosyalarınıza erişiminizi engelleyerek tekrar erişiminiz karşılığında fidye talep ederler. Bu türden zararlı yazılımlar kullanıcı verilerine erişerek rehin alırlar. Örneğin; kullanıcı bilgisayarında bulunan dokümanları parola ile korumalı bir dosyanın içerisine kopyalayarak, orijinal dokümanları siler. Verilerinin bulunduğu dosyaları kullanıcı açmaya çalıştığında kullanıcıya bir mesaj bırakarak fidye karşılığında verilerinin bulunduğu dosyanın parolasını vereceğini taahhüt eder. Fidye ödenmediği takdirde verilerin silineceği ya da kötü amaçla kullanılacağı gibi tehditler gönderebilirler.

Ransomware yoluyla saldırganlar kullanıcılara resmi otoriteler olarak da görünebilir. Pop-up penceresi, bir web sitesi ya da e-posta gibi yollarla, kullanıcıya mesaj göndererek, program ve dosyalarına erişebilmek için, kullanıcıda istenilen fidyeyi iletmesi istenebilir.

Kullanıcı bilgisayarına yüklendiği tespit edilen ransomware zararlı yazılımıyla ilgili olarak, temizlemeye yönelik güvenlik çözümleri kullanılmalıdır ve özellikle dönemsel olarak yaygınlaşan bu tip yazılımlara karşı dikkatli olunarak, farkındalık sağlanmalıdır.

Drive By Download

Drive By Download, zararlı yazılım içeren bir web sitesini ziyaret edildiğinde zararlı yazılımın kullanıcı bilgisayarına bulaşması durumudur. Yalnızca bir web sitesinde gezinirken ya da bir yazılım yüklemesi durumunda onay verilmesi halinde zararlı yazılım bilgisayara indirilmiş ve arka planda çalışmaya başlamış olacaktır. Drive By Download türü zararlı yazılımların bulaştırılması tamamen kasıtsızca gerçekleşir.

Bu zararlı yazılımlar, tarayıcının, işletim sisteminin ya da bir uygulamanın güvenlik açığından faydalanırlar. İlk etapta indirilen zararlı yazılım kodu ise oldukça küçük bir kısım oluşturur, bu kodun görevi ise uzaktaki bilgisayarla bağlantı kurup kodun geri kalan bölümünü tamamıyla bilgisayara, tablete yada akıllı telefona indirilmesini sağlamaktadır.

Web sitesi, bilgisayarda bulunan güvenlik açıklıklarıyla/zayıflıklarla eşleşecek şekilde alternatif olarak farklı türlerde zararlı yazılım kodu içerirler. Zararlı yazılımların görevi tarayıcıdaki güvenlik zafiyetlerini de açığa çıkarmak da olabilir. Bu tür zararlı yazılımlar, meşru web sitelerine de ilgi çekebilecek linkler aracılığı ile bulaştırılabilirler. Bu tip sosyal medya sitelerine, mail adresleri vb. yönlendirme linklerine tıklandığında, çoktan zararlı yazılım bilgisayara yüklenmeye başlanmış olur.

Bu tür saldırıların önüne geçmek için, zararlı ve tehlikeli web sitelerine (Yetişkin içerik, dosya paylaşım siteleri vb.) giriş yapmaktan kaçınılmalıdır. Internet tarayıcısı ve işletim sistemi güncel sürümü yüklenmeli, güvenilir arama motorları kullanılmalı ve antivirüs programları kullanılmalıdır.

E-Posta Zararlı Yazılımları

Zararlı yazılımın birçok örneğinin e-posta ile bulaştırıldığı bilinmektedir. Günümüzde ise e-posta yerine birçok kişiye web üzerinden zararlı yazılımların daha kolay yayılabildiği aşikardır. Eskiden ise zararlı yazılım içeren dosyalar e-posta ekinde hesaplara dağıtılıp, eke tıklanması halinde zararlı yazılımın indirilmesi işlemi gerçekleşmiş oluyordu.

E-postaların halen zararlı yazılım bulaştırmakta kullanıldıkları görülmektedir. Zararlı kod içeren web sitesi vb. linkler e-posta içerisinde dağıtılıp, daha fazla kişiye temas etmesi ve zararlı koddan etkilenmesi sağlanıyor.

Zararlı yazılımlara karşı önlem olarak antivirüs programlarının kullanılması ve güncellenmesi önemlidir.