TEMEL BİLGİ GÜVENLİĞİ-2

Autorun Worm

Autorun bir dosyayı otomotik olarak çalıştırmaya yarayan bir program parçacığıdır. Autorun Worm (Türkçe olarak Otomatik Çalıştırma Solucanı olarak adlandırılabilir) işletim sistemindeki Autorun özelliğinden faydalanan zararlı yazılımlardır. Bu yazılımlar, bir depolama cihazı (CD, DVD, Flash Bellek gibi) bilgisayara bağlandığında otomotik olarak çalıştırılırlar. Taşınabilir cihazın içine gömülü olan virüs yazılımları Autorun özelliği sayesinde otomatik olarak aktifleşir.

Autorun Worm'lar sıklıkla USB sürücüler üzerinden bilgisayara zararlı yazılım bulaştırırlar.

Autorun özelliği virüs bulaştırma yöntemiyle birlikte tehlikeli hale gelmektedir. Autorun virüsü son kullanıcı bilgisayarlarına zararlı yazılım bulaşmasına neden olabilir. Zararlı yazılım bulaşan bileşen aracılığıyla USB Portlarını kullanan tüm taşınabilir depolama cihazlarına zararlı yazılım bulaşması olasıdır. Bu yüzden Autorun virüsünün hızla yayılımı oldukça kolay hale gelmektedir.

Virüs bulaştığının belli başlı etkileri ise; Autorun.exe dosyalarının çalışmaması, gizli dosyaların görüntülenememesi Bu virüsten korunmanın yolu bilgisayarınız üzerindeki Autorun dosyasının otomotik çalışmasını engellemektir. Bu engellemeye sağlamak için; Microsoft yeni işletim sistemlerinde bu özelliği default (öntanımlı) olarak kapalı bir şekilde sunmaktadır.

Backdoor Trojan

Backdoor Trojan'lar kullanıcıdan habersiz olarak bilgisayarın kontrolünü ele geçiren zararlı yazılım türüdür. Bu zararlı yazılımlar, yasal bir yazılım gibi kullanıcı bilgisayarında görüntülenebilir. Sıklıkla kullanılan bir diğer yol ise, kullanıcılara gönderilen spam niteliğindeki e-postalardan kullanıcı bilgisayara bulaşması yada zararlı/kötücül bir websayfasını ziyaretle farkında olmadan bulaşmasıdır. Bu türden zararlı yazılım bir kez bulaştıktan sonra kendisini bilgisayarın başlangıç rutinine ekler ve kullanıcı internete çıktıktan sonra kullanıcı bilgisayarını uzaktan kontrol edebilir hale gelir.

Kullanıcı bilgisayarı internete çıkarak online olduğunda virüs yollayan kötü niyetli olarak birçok eylem gerçekleştirebilir. Örneğin; program çalıştırma, kişisel dosyalara erişme, dosyalarda değişiklik yapma, dosya yükleme, kullanıcının klavye hareketlerini izleme, spam e-postaları gönderme vb.

Bilinen en ünlü Backdoor Trojan'lara örnek olarak Netbus, OptixPro, Subseven, BackOrifice, Zbot ve ZeuS verilebilir.

Backdoor Trojan'lardan korunmak için bilgisayarda yüklü olan işletim sisteminin en son çıkan yamalarını takip ederek, işletim sistemi açıkları kapatılmaya çalışılmalıdır. Anti-spam ve anti-virüs programlarını kullanmak da bu tür zararlı yazılımlara karşı alınabilecek güvenlik önlemleri arasında yer alır. İşletim sistemi güvenlik duvarı (Firewall) kullanarak ise, Trojan yazılımlarının internet erişimi yoluyla saldırganla iletişim kurması engellenebilir.

Boot Sector Malware

Bir bilgisayar başlatıldıktan hemen sonra, genellikle hard-disklerde bulunan Boot sektörü bularak işletim sistemini kullanıma hazırlar. Boot sektör üzerinde tutulan sistem bilgileri, bilgisayarın sözü edilen disk yada disketleri kullanabilmesi için gereken bazı temel verileri içerir. Bilgisayar yeniden açılışında Boot sektördeki verileri okuyarak düzgün çalışmak için gerekli temel verileri sağlar.

Boot Sector Malware ise, kendi boot sektörünü orijinal boot sektörleri ile değiştirir ve genellikle orijinalini erişemez hale getirir. Bu aşamadan sonra bilgisayar ilk çalıştırıldığın da zararlı yazılım içeren boot sektör üzerinden işletim sitemini çağıracak ve zararlı yazılım aktif hale gelecektir. Dikkat edilecek nokta ise zararlı yazılımın işletim sisteminden önce aktif olmasıdır.

Boot Sektör nedir?>> Bir diskin veya disketin işletim sistemini yüklemeye yarayan 1 sektör (512 byte) uzunluğundaki bir programdır. Sabit disklerin ve disketlerin sistem bilgileri kısımları Boot sektör üzerinde tutulur.