TEMEL BİLGİ GÜVENLİĞİ-5

Internet Worm (İnternet Solucanı)

İnternet solucanı aynı zamanda bilgisayar solucanı olarak da bilinir. Bu tip zararlı yazılımlar kendi kendilerini çoğaltarak, yerel ağlarda yada internet üzerinde yayılırlar. Trojan yada diğer virüslerin aksine kullanıcı müdahalesi gerektirmeden kendi kendilerine çoğalabilme özelliğine sahiptir. İnternet üzerinden yayılan bu virüsler bilgisayara girerek, kullanıcıdan habersizce çoğalabilirler. Bu özellik virüsleri oldukça tehlikeli hale getirmektedir.

İnternet solucanları herhangi bir virüs çeşidi, komut dosyası yada program olabilir. İnternet solucanları genellikle, sistemlerin güvenlik açıklıklarından yaralanarak sistemlere bulaşırlar. Örnek olarak Conficker solucanı verilebilir.

Bazı internet solucanları ise bilgisayar üzerinde backdoor (arka kapı) oluşturarak bilgisayarın kötü niyetli bir saldırgan tarafından kontrol edilebilmesine neden olabilirler. Bu durum ise bilgisayarın zombi olmasına neden olmaktadır.

Potentially Unwanted Applications-PUA

İstenmeyen türden olabilecek uygulamalar, zararlı olmayan fakat özellikle iş ortamında kullanılması uygun olmayan, güvenlik kaygısı oluşturabilecek yazılımlardır.

Doğru amaçlar için kullanıldığında faydalı olan fakat şirket ağları içerisinde kullanımı uygun olmayan uygulamalara örnek olarak, adware'ler (Reklam destekli yazılımlar), bilgisayarları uzaktan kontrol etmek için kullanılan araçlar ve sistem açıklıklarını taramak için kullanılan araçlar verilebilir.

Antivirüs programlar ve uç nokta güvenlik programları kullanıcı bilgisayarındaki istenmeyen türden olabilecek bu tip yazılımları (PUAs) tespit ederek, raporlama yapabilmektedir.

Mobile Phone Malware (Cep Telefonu Zararlı Yazılımı)

Mobile Phone Malware, akıllı telefonlar, tabletler, cep bilgisayarları gibi akıllı cihazlar için tasarlanmış zararlı yazılımlardır. 2010'dan beri mobil cihazlar sürekli artan zararlı yazılım tehdidi altındadır. Android ve IOS işletim sistemleri için çok sayıda zararlı yazılım mevcuttur. Ancak bu oranın IOS'a göre android cihazlarda çok daha yüksek olduğu görülmektedir.

Android cihazlar, dosya paylaşım siteleri aracılığı ile popüler uygulamaların zararlı yazılım içeren versiyonlarını yüklemeye olanak tanımaktadır. Bu gibi üçüncü parti kaynaklardan yüklenen uygulamaların zararlı yazılım içerme oranı oldukça yüksektir.

Benzer yazılımlar maddi kazanç elde etmek amacıyla kişisel bilgisayarlarda da kullanılabilmektedir. Mobil zararlı yazılımlar da sahte antivirüs yazılımları üzerinden yayılarak, gizli bilgilere ulaşabilmektedir.

Birçok güvenilir kaynak risk oluşturacak derecede gizli bilgi taşıyan uygulamalar barındırmaktadır. Örneğin reklam içerikli uygulamalar kullanıcının özel bilgilerinin (konum bilgisi, telefon numarası gibi) paylaşımına olanak tanımaktadır. Bu tip uygulamalarda "potentially unwanted applications" (PUAs), yani istenmeyen uygulamalar olarak nitelendirilmelidir.

Cep telefonu, tablet gibi akıllı cihazları zararlı yazılımlardan korumak için, işletim sistemine ait güvenlik güncellemeleri takip edilmeli ve yalnızca güvenilir kaynaklardan (Google Play, Apple iTunes vb.) uygulamalar yüklenmelidir. Mobil cihazlar için olan güvenlik yazılımları da cihazları zararlı yazılımlara karşı korumak için tercih edilen yöntemlerden biridir.