TEMEL BİLGİ GÜVENLİĞİ-1

Advanced Persistent Threat (APT)- (Gelişmiş Kalıcı Tehditler)

Gelişmiş Kalıcı Tehditler olarak Türkçe adlandırabileceğimiz hedefli bir saldırı türüdür. APT ticari ve siyasi hedeflere yönelik siber suç kategorisinde yer almaktadır. Bu türden saldırılarda hedeflenen bir ağ içine sızma planı için zaman ve bilgi birikimi iki önemli parametredir. APT ler hedeflerde zarara yol açmaktan çok hedefteki hassas verileri ele geçirmek için gerçekleştirilir.

Saldırganlar, açıklığı bilinen ve çok sayıda kişi tarafından kullanılan popüler bir program/yazılım aracılığıyla kötücül bir ortam hazırlar (Örneğin MS Office, Adobe). Saldırgan oluşturduğu bu ortamı/dosyayı/program parçacığını kurbanların ilgisini çekecek şekilde onlara iletir ve arka planda kötücül program parçacığı çalışarak saldırganın uzak bileşen (PC, Sunucu, Ağ) üzerinde kontrolü ele geçirmesini sağlar. Buradaki amaç, bileşenleri ele geçirmekten çok, daha gelişmiş etkili ve kalıcı saldırıları tasarlamak ve yönetmektir.

Gerçek dünyadan: Stuxnet bu saldırıya örnek gösterilebilir.

Adware (Advertising-Supported Software)

Adware'ler reklam destekli yazılımlardır. Bu yazılımlar bir uygulama kullandığınızda bilgisayarınızda pop-up veya banner reklamlarınızı görüntülemeye olanak tanır. Adwareler mutlaka kötücül yazılımlar değillerdir. Bu türden reklamlar özellikle *ücretsiz* yazılımların geliştirilme aşamasında fon sağlamak için kullanılmaktadır.

Ancak Adwareler aşağıda belirtilen durumlarda sorun teşkil edebilirler;

- İzin verilmeden kendisini bilgisayara yüklemesi
- Sizin kullandığınız uygulamaların dışında ekrana gelmesi ve reklam görüntülemesi
- Internet tarayıcınızı ele geçirerek (Hijacking), daha fazla reklam görüntülemesi
- İzin verilmeden web tarayıcı bilgilerinizi toplaması ve internet aracılığı ile bilgilerin başkalarıyla paylaşımı (Spyware)
- Adware'i kaldırmanın zor olacak şekilde tasarlanmış olması

Adware'ler bilgisayarı ve reklamların indirilmesi internet bağlantı hızını yavaşlatabilir. Adware'daki programlama hataları bilgisayarı üzerinde beklenmedik hatalara yol açabilir.

Adware programlarını yetkilendirebilir yada bilgisayarınızdan kaldırabilirsiniz.
Not: Adwarelerin tespiti için de özel programlar bulunmaktadır.

Anonymizing Web Proxy

Proxy sunucu, bir web tarayıcısı (Internet Explorer, Chrome gibi) ve Internet arasında aracı (Vekil) işlevi gören bileşendir. Anonim Vekil Sunucular, IP adresini ve web kimliğini gizleyen vekil sunucularıdır. *Anonymizing Proxy* yöntemi kullanıların web tarayıcıları üzerindeki aktivitelerini gizlemekte kullanılır. Bu yöntemle Web güvenlik önlemleri bypass edilebilmektedir. Bu şekilde bir iş bilgisayarından engellenmiş bir web sitesine erişim sağlamak mümkün olabilir.

Anonymizing Proxy işlemi güvenlik ve sorumluluk riski taşımaktadır. Web güvenlik önlemlerini atlayarak (bypass ederek), kullanıcıların web sayfalarına yetkisiz erişimlerini sağlar. Kullanıcılar

yasadışı MP3, film, yazılım vb. indirmeleri üçüncü parti lisans haklarını ihlal edilmesi gibi etkileri de bulunmaktadır. Organizasyonlar kullanıcıların erişimi engellenmiş sitelere ulaşması durumunda yasal sorumluluk altına girebilirler. Proxy sunucular, bazı web içeriklerine ve kötü amaçlı yazılımlara filtre uygulayarak güvenliğin artırılmasını sağlarken, Anonymizing Proxy yöntemi bu güvenlik önlemini ortadan kaldırır.