TEMEL BİLGİ GÜVENLİĞİ-3

Hoax (Asılsız Metinler)

Hoax (Asılsız Metinler), internet üzerinden yayılan, kullanıcıları kandırmak yada dolandırmak amacıyla, asılsız ve yanlış haberler içeren metinlerdir. Hoax'lar, para talebinde bulunmak, kullanıcı bilgisayara zararlı yazılım yüklemek yada bant genişliğinizi tüketmek amacıyla kullanılabilir. Hoax'lar yayılırken genellikle e-posta kullanılır ve e-postayı alan kullanıcılar mesajları sürekli çoğaltarak iletmeye teşvik edilir. (forward etmek)

Hoax'ların kullanıcıları kandırmaya yönelik içerik taşıdıkları birkaç ipucuyla anlaşılabilir. Hoax kullanıcıya ulaştığında;

-Yeni bir zararlı yazılım hakkında sizi uyarıyor olabilir.

-Özel bir konu başlığı ile gönderilerek, e-postanın zararlı yazılım içerdiğini söyleyebilir.

-Uyarının önemli bir yazılım şirketi tarafından, internet servis sağlayıcınızdan yada bir devlet kurumu tarafından gönderildiğini iddia edebilir.

-Bir zararlı yazılımın normalde olanaksız bir işlemi gerçekleştirebileceği konusunda bilgi içerebilir.

-Metini birçok kişiye iletmeniz (forward etmeniz) için uyarı içeriyor olabilir.

-Bir sosyal paylaşım sitesinde, bir hikayeyi, metini yada kişiyi beğenmenin yada paylaşmanın maddi bir yardım oluşturacağı gibi vaatler içeriyor olabilir.

Günümüzde de; internet ve sosyal paylaşım ortamlarında sıklıkla rastladığımız bu türden metin içerikleri ve örneklerini çoğaltmak mümkündür. Amaç, kullanıcıya aldatmaca bir hikayeyle istenilen işlemi yaptırmaktır. Hoax'ların paylaşılması e-posta seline neden olmakta ve e-posta sunucularının kapasitesini zorlamaktadır.

Hoax'lara karşı en iyi savunma yöntemi, kullanıcıların farkındalık düzeyini artırması ve bu türden asılsız metin örnekleri hakkında bilgilenerek dikkatli olunmasıdır.

Keylogging / Keylogger

Keylogging, kötü niyetli kişiler tarafından son kullanıcıların klavye üzerindeki tuş hareketlerini kayıt altına alınmasıdır. Keylogging işlemi, kullanıcı adları, parolaları, banka hesap bilgileri ve birçok hassas bilgiyi zararlı yazılımlar aracılığıyla uzaktan ele geçirmeyi amaçlar.

Keylogging, bir yazılım yada donanım ile gerçekleştirilebilir.

Keyloggerlar kimi firmalarda Bilgi Teknolojileri bölümü tarafından teknik sorunları giderebilmek için de kullanıldığı bilinmektedir.

Bazı keylogger yazılımları ile yalnızca klavye tuş hareketlerini kaydetmekle kalmayıp, ekran görüntüsü yakalama, mikrofon ile ses kaydı yapma özelliğine de sahiptir. Normal keylogging programları yerel sabit disk üzerine verileri kaydederken, bazıları ise bir ağ üzerinden uzaktaki bir web sunucu yada bilgisayara verilerin aktarılmasını sağlayabilir.

Keylogger yazılımları, kullanıcıların bilgisi olmadan bilgisayarları üzerine zararlı bir yazılım paketi aracılığı ile yüklenebilirler. Bilgisayarda bir keylogger'ın varlığını tespit etmek zor olabilmektedir. Keylogging sistemlerinin tespiti içinse, anti-keylogging programları geliştirilmiştir.

Browser Hijacker

Browser Hijacker, bilgisayarın varsayılan tarayıcı ayarlarını değiştirerek, sizi istemediğiniz bir web sitesine yönlendiren zararlı yazılım türüdür.

Bu yazılım bilgisayara bulaştığında, manual olarak tarayıcı ayarları değiştirmeye çalışıldığında değiştirilemediği görülecektir. Bazı Hijackerlar, tarayıcı araçları bölümünden seçenekler kısmını kaldırarak, başlangıç sayfasını yeniden yapılandıramaz hale getirilebilmektedir.

Browser Hijacking yöntemi arama sonuçları sıralamasında bazı sitelerin Page Rank(Sayfa sırası) değerlerini değiştirmek için de kullanılır. Bir açıdan, Siyah şapka SEO (Search Engine Optimization) yöntemlerinde olduğu gibi, reklam gelirlerini artırmanın bir yolu olarak kullanılır.

Saldırganlar ClickJacking olarak bilinen, web sayfası üzerine şeffaf ve opak katmanlar ekleme işlemi de gerçekleştirmektedirler. Bu tuzak sayfalar aracılığı ile web sayfasına yönlenen kurbanları, sayfa üzerinde bir butona yada linke tıklamaları için kandırarak, amaçlanan diğer bir tıklama işlemi gerçekleştirmelerini sağlarlar.

Bu türden saldırılar bilgisayar üzerinde bir etki sağlayamasalarda, tarayıcı performansınızı düşürürler.