Siber Güvenlik Bülteni: Fidye Yazılımları

Fidye Yazılımları Nedir, Nasıl Bulaşır ve Etkileri Nelerdir?

- Kullanıcıların bilgisayar ve mobil cihazlarında yer alan elektronik verilere erişimini engelleyerek yeniden erişim için fidye talebine hizmet eden zararlı yazılımlardır.
- Fidye yazılımlar bulaştığı sistemlerdeki dosyaları şifreleyerek ya da cihazın tamamen kilitlenmesine neden olarak kullanıcıların verilere ulaşmasını engeller.
- Bilgilendirme mailleri, anlık mesajlar, aldatıcı bağlantıların tıklanması ve sosyal mühendislik gibi yollarla kullanıcıların cihazlarına bulaşmaktadır.
- Saldırganlar, bulaştırdıkları bu zararlı yazılımlar neticesinde kullanıcıların verilerine tekrar erişebilmesi için belirledikleri sınırlı bir sürede genelde günümüz sanal para ödeme sistemleri ile ödeme yapmasını belirten bir uyarı ekranı ile fidye taleplerini iletirler.
- Fidye yazılımları; çalışma kesintisi, kalıcı veri kaybı, fikri mülkiyet hırsızlığı, gizlilik ihlali, itibar kaybı ve yüksek kurtarma maliyeti gibi sonuçlar doğurabilmektedir.

Fidye Yazılımlara Karşı Alınabilecek Güvenlik Tedbirleri

- Fidye yazılımlarına karşı alınabilecek en etkili önlemlerin başında cihazınızda güncel anti-virüs yazılımının bulunması ve veri yedeklemesi gelmektedir.
- Verilerinizin kritiklik seviyesine göre yedekleme sıklığını arttırmalısınız.
- Kaynağını bilmediğiniz ya da şüpheli olarak düşündüğünüz hesaplardan gelen elektronik postaları dikkate almayınız, gönderilen bağlantıya tıklamayınız ve gelen eki indirmeyiniz. Kişisel bilgilerinizi kesinlikle paylaşmayınız.
- Size ulaşan elektronik mesaj ya da bağlantının kaynağı, bildiğiniz ya da güvendiğiniz bir hesap olsa bile hesabın saldırganlar tarafından ele geçirilmiş olabileceği bilinci ile veri paylaşımında bulunurken temkinli olmanız gerekmektedir. Şüpheli durumlarda, farklı bir kanaldan hesap sahibi ile iletişime geçip içeriğin doğrulaması yapılmalıdır.
- Güvenilir olmayan internet sitelerini ziyaret etmeyiniz. Resmi ve güvenilir kaynaklar haricinden program indirmeyiniz.
- Güvenli sitelerin isim benzerliğinden yararlanıp sahte siteler yaparak sizin bilgilerini ele geçirmeye çalışan siber tehdit aktörlerinin varlığını unutmayınız.
- Uygulamaların, işletim sisteminin, tarayıcının ve anti-virüs yazılımı güncellemelerinin etkin bir şekilde yapılmasına özen göstererek saldırganların olası güvenlik açıklarından faydalanıp erişim sağlamasını engelleyiniz. Bu konuda otomatik güncelleme yapılandırmasını gerçekleştirme önemli olacaktır.
- Taşınabilir medya cihazlarını kullanırken virüs taramasının yapıldığından emin olunuz.
- Cihazınıza uzaktan erişim gereken durumlarda bu erişimin güvenilir programlarla yapılmasına özen gösteriniz.
- Halka açık internet kullanımlarında dikkatli olunuz ve sanal özel ağ (VPN) ile erişim sağlanmasına dikkat ediniz.

- Saldırganlar verilerinize ulaşabilmek için harf, rakam ve özel karakterleri de içeren şifre üretici programları kullanarak şifrelerinizi ele geçirmeye çalışabildiğinden mümkün olduğunca karmaşık şifreler belirleyiniz. Basit düzeyde şifre belirlemeniz saldırganların işini kolaylaştıracaktır.
- Bazı kimlik bilgileriniz ele geçirilse bile ek kimlik doğrulama bilgileri olmadan hesabınıza erişimi engelleyecek olan çok faktörlü kimlik doğrulamayı etkin şekilde kullanmalısınız.
- Kurum cihazlarından ve kurum uzantılı hesaplarınızdan kişisel amaçlara yönelik olarak e-posta, uygulama ve web sitesi kullanımı gerçekleştirmemeye özen gösteriniz.

Fidye Yazılımları Bulaştığında Neler Yapılmalıdır?

- İstenen fidye talebi gerçekleştirildiğinde erişim sağlanamama ve diğer saldırılar için motivasyon sağlama ihtimali olduğundan gelen fidye notuna cevap verilmemelidir.
- Virüs bulaşmış cihazdan ayrı bir cihaz kullanılarak fidye yazılımın yüklendiği cihazda erişilen tüm hesapların şifreleri ivedilikle değiştirilmelidir.
- Profesyonel destek alınıp kolluk güçleri gasp talebi ile ilgili olarak bilgilendirilmelidir.
- Saldırganların hedefinde olduğunuzu zamanında fark ederseniz başarılı olmalarını engellemek için adımlar atabilirsiniz. Bazı fidye yazılımlarının amacı sadece sizin cihazınız değil o cihazın dahil olduğu tüm ağa yayılmak olduğundan, cihazınızın ağ bağlantısını kesip cihazı ağdan izole etmek yayılımı engelleyecektir.

Fidye Yazılımlarının Geçmişten Günümüze Gelişimi

- İlk fidye yazılım örneği 1989 yılında Dr. Joseph Popp tarafından gerçekleştirilmiştir. Dünya Sağlık Örgütü tarafından Stokcholm'de düzenlenen AIDS konferansından sonra 90'dan fazla ülkede bulunan konferans katılımcılarına 'AIDS bilgileri-Tanıtım disketleri' etiketi ile toplam 20.000 disket gönderdi. Popp, bu disketlerin bilgisayarda çalıştırıldığında C sürücüsündeki dosya isimlerini simetrik şifreleme yöntemi ile şifreleyerek kullanıcıların bilgisayarlara erişimini engelleyecek bir zararlı yazılım oluşturdu. Disketin bilgisayara ilk takıldıktan sonraki belirli sayıdaki açılıp kapanmasıyla etkinleşen bu zararlı yazılım ile Panama'da bir posta kutusuna 189 Dolar gönderilmesi karşılığında, mağdurun dosyalara tekrar erişim sağlayabileceğini belirten bir uyarı ekranı karşılarına çıkardı.

- Fidye yazılımlar, AIDS Truva Atı olarak isimlendirilen ilk fidye yazılımından sonra internet ve sanal para birimlerinin ortaya çıkışı ile farklı tekniklerle gücünü arttıran siber tehditler arasında bulunuyor. Bu saldırıların günümüzde grup ve çetelerle gerçekleştirilmesi yaygın olup fidye talep aralığı oldukça geniştir.
- Geçtiğimiz yılın en büyük fidye talebi 70.000.000 Dolar ile bir teknoloji firmasına yönelik olarak gerçekleştirildi.
- Gerçekleşen diğer bir fidye yazılım saldırısında ise Amerika Birleşik Devletleri'nin en büyük enerji nakil hattına yönelik olarak gerçekleştirilmiş olup bu saldırı 4.400.000 Dolar değerinde sanal para ödemesi ile sonuçlanmıştır. Güvenlik güçlerinin takibi ile ödemenin yaklaşık yarısı geri alınmıştır.
- Günümüzde saldırganlar daha etkili sonuç almak adına sadece mağdurun verilerinin şifrelendiği ve şifre çözme anahtarı karşılığında fidye talep ettiği gasp türü yerine verileri şifrelemeyi gerçekleştirmeden önce verileri ayrı bir sunucuda depolayıp fidye talepleri karşılanmazsa verileri sızdırma tehdidinde bulundukları çifte gasp saldırı yöntemini kullanır hale gelmişlerdir.
- Bir diğer trend ise belirli gruplar tarafından artık bir hizmet olarak verilmeye başlanmasıdır. Özellikle sanal paranın etkisiyle, siber saldırganlar daha büyük ölçekte

örgütlenip hizmet olarak fidye yazılımını (Ra-aS) devreye aldılar. Fidye yazılım araçları oluşturup, diğer suçlulara satarak başarılı her saldırıdan da belirli bir miktar komisyon aldıkları bir düzen içerisinde çalışmalarını sürdürüyorlar. Böylece, tüm bu gelişmelerle birlikte bireylerin fidye yazılım tehditleri ile karşı karşıya kalma olasılığı gün geçtikçe artmaktadır.