Fidye Yazılım

Fidye Yazılım Nedir?

Fidye Yazılım, dosya ya da bilgisayarınızı rehin tutup tekrar verilerinize erişiminiz için sizden para talep etmek üzerine tasarlanmış kötü amaçlı bir yazılımdır. Suçlular için çok kazançlı olduğu için çok yaygınlaşmıştır.

Birçok kötü niyetli yazılım gibi fidye yazılımı, çoğunlukla virüslü bir eklentiyi açtığınızda ya da bir oltalama e-postasındaki kötücül bir bağlantıyı tıkladığınızda bilgisayarınıza bulaşır. Bir kere bilgisayarınıza bulaştığında, sabit diskinizdeki dosyaları, büyük ihtimalle tüm sabit diskinizi bile, ya da bilgisayarınıza bağlı herhangi bir cihazı şifreler ki siz dosyalarınıza ulaşamayasınız. Daha sonra dosyalarınızı geri almanın tek yolunun siber suçlulara fidye ödemek olduğunu söylerler ki fidye yazılımının ismi de buradan gelir. Fidyeyi ödemeyi reddederseniz, bazen suçlular dosyalarınızı herkesin görebileceği şekilde yayınlamakla tehdit edebilir. Suçlular, Bitcoin gibi takip edilemeyen dijital para birimi ile ödeme yapmanızı isteyebilir. Eğer fidyeyi öderseniz, suçlular dosyalarınıza yeniden ulaşmanızı sağlayabilirler ancak bunun bir garantisi yoktur. Bazen paranızı alırlar ve sizin farketmeyeceğiniz şekilde bilgisayarınızı virüs bulaşmış bir şekilde bırakabilir ya da daha fazla para isteyebilirler.

Bulaşmaya Karşı Koruma

Bilgisayarınızı diğer kötücül yazılım türlerine karşı nasıl koruyorsanız aynı şekilde fidye yazılıma karşı da koruyabilirsiniz. Temel adımlar şunlardır:

- **Sistem ve Yazılımları Güncelleyin:** Siber suçlular, yazılımlarınızda bulunan onarılmamış hatalardan (açıklar olarak da bilinir) yararlanarak bilgisayar ya da cihazlarınıza kötücül yazılımlar bulaştırırlar. Yazılımınız ne kadar güncel ise o kadar az bilinen açık barındırır ve siber suçluların kötücül yazılım bulaştırmasına o kadar dayanıklıdır. Bu yüzden, işletim sistemlerinizin, uygulamalarınızın ve cihazlarınızın otomatik güncelleme özelliğinin etkin olduğundan emin olun.

- **Antivirüs Yazılımlarını Etkinleştirin:** Güvenilir bir tedarikçinin güncel bir antivirüs yazılımını kullanın. Bu araçlar, kötücül yazılımları saptayıp durdurmak için tasarlanmıştır. Ancak, antivirüs yazılımları tüm kötücül programları engelleyip kaldıramaz ve genellikle bir fidye yazılımı

bulaşmasından sonra dosyalarınızı kurtaramaz. Siber **suçlular**, saptanmalarını önlemek için sürekli yeni ve karışık bulaştırma teknikleri geliştiriler. Antivirüs tedarikçileri ise kötücül yazılımların bu yeni kabiliyetlerini saptamak için sürekli olarak ürünlerini güncellerler. Birçok yönden bu, iki tarafın da galip gelmeye çalıştığı bir silahlanma yarışına dönüşmüştür.

- **Tetikte Olun:** Siber suçlular, oltalama e-posta saldırıları yardımıyla fidye yazılımları ve diğer türde kötücül yazılımları yüklemek için insanları oyuna getirirler. Örneğin, bir siber suçlu size gerçek gibi görünen ve içinde bir ek dosya ya da bağlantı olan bir e-posta gönderebilir. Belki de bu e-posta arkadaşınızdan ya da bankanızdan geliyormuş gibi görünebilir. Ancak, eğer ekli dosyayı açar ya da web bağlantısına tıklarsanız, kötücül kodu etkinleştirip bilgisayarınıza bulaştırabilirsiniz. Eğer bir mesaj, fazlasıyla aciliyet içeriyorsa ya ada inanılmayacak kadar iyi ise, bu bir saldırı olabilir. Tetikte olun - siber suçlular sizin duygularınızla oynar. - Sağduyu çoğunlukla en iyi savunmanızdır.

Bilgisayarınız bulaşmadan önce dosyalarınızı yedekleyin

Her zaman kötücül yazılımları engelleyebilecek olmanız mümkün olmadığı için, fidye saldırılarına karşı en iyi savunmanız yedeklemelerdir. Eğer sizin için önemli dosya ve dokümanlarınızın yedeği var ise, fidye ödemek yerine yedeklerinizi kullanarak dosyalarınızı kurtarmak şansınız olur. Tüm dosyalarınızı düzenli bir şekilde otomatik olarak yedeklemeyi kullanmanız ve kurtarma prosedürlerini test ederek gerektiğinde dosyalarınızı kurtarabileceğinizi bilmeniz önem taşır. Sizin için düzenli ve güvenli bir şekilde tüm dosyalarınızı yedekleyebilen bir çok bulut ya da lokal yedekleme çözümü vardır.

Konuk Editör

Lenny, bir siber güvenlik varlık yönetimi şirketi olan Axonius'da Bilgi Güvenliği Kurulu Başkanıdır (CISO). Ayrıca kötücül yazılımlarla savaş ve teknik yazım ile ilgili SANS'da ders vermektedir. Lenny'e Twitter'da @lennyzeltser ile ulaşabilirsiniz ve zeltser.com'dan güvenlik web günlüğünden takip edebilirsiniz..

Kaynaklar

Yedekleme yaptın mı?: https://www.sans.org/security-awareness-training/resources/got-backups
Oltalamayı durdurun: https://www.sans.org/security-awareness-training/resources/stop-phish
Güncelleme: https://www.sans.org/security-awareness-training/resources/power-updating
SANS FOR610 Kursu - Kötücül Yazılımların Tersine Mühendisliği: https://sans.org/for610

Tarafından toplum için çevirisi yapılmıştır: Sema Yüce ve Selma Süloğlu