Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Fidye Yazılımlar (Ransomware)

Fidye Yazılım (Ransomware) Nedir ?

Fidye Yazılım (Ransomware) kurbanlarının belgeleri ve diğer dosyalarını yok etmekle tehdit eden, bugünlerde Internet üzerinden aktif olarak yayılan özel bir zararlı yazılım türüdür. Zararlı yazılım -kötü niyetli eylemleri gerçekleştirmek için kullanılan bir bilgisayar yazılım. Fidye yazılımlar, zararlı yazılımların bir çok farklı türünden biri iken, suçlular için çok karlı olduğundan, bu denli yaygın hale gelmiştir. Fidye yazılım bilgisayarınıza bulaşıp sonra, belirli dosyaları veya belki de tüm sabit diski şifreler. Daha sonra tüm sisteminiz kilitlenir veya örneğin belge veya fotoğraf gibi önemli dosyalara erişemezsiniz. Bu yazılım sonra size dosyaların şifresini çözmenin ve sisteminizi kurtarmanın tek yolunun siber suçluya bir fidye ödemek olduğunu bildirir. (bu nedenle adı Fidye Yazılım). Çoğu zaman fidye dijital para çeşitlerinden biriyle, mesela BitCoin ödenmelidir. Fidye yazılımlar da, diğer birçok zararlı yazılım türü gibi yayılır. En yaygın yöntem mağdurları virüslü bir eki açmak veya saldırganın web sitesine yönlendiren bir bağlantıyı tıklamak için kandıran zararlı e-postaların siber saldırganlar tarafından iletilmesidir.

Konuk Yazar

Lenny Zeltser, NCR Corp'da müşterilerin BT operasyonlarını korumaya odaklanır ve SANS Institute zararlı yazılımlarla mücadele konusunda eğitimler verir. Lenny, Twitter'da **@lennyzeltser** hesabı ile aktiftir ve **zeltser.com** adresinden yayınladığı bir güvenlik blogu bulunmaktadır.

Fidyeyi Ödemeli misiniz ?

Bu zor bir soru. Sorun şu ki daha çok insan bu suçlulara ödeme yaptıkça, suçlular da başkalarına bulaştırmak için daha motive oluyorlar. Öte yandan, dosyalarınızı kurtarmak için başka hiçbir seçeneğiniz olmayabilir. Uyaralım, eğer fidyeyi ödeseniz bile, yine de dosyalarınızı geri alacağınızın garantisi yoktur. Suçlulardan bahsettiğimizi unutmayalım, onlar dosyalarınızın şifrelerini çözmeyebilir, ya da ödeme karşılığında bir şifre çözme yöntemi sunsalar bile, şifre çözme işlemi sırasında birşeyler yanlış gidebilir veya bilgisayarınıza yeni zararlı yazılımlar bulaşmış olabilir.

Dosyalarınızı Yedeklemek

Belki bir fidye ödemeden bir fidye yazılımdan kurtulmanın ve dosyalarınızı kurtarmanın en iyi yolu yedeklemenizden geri dönmektir. Bu şekilde, Fidye yazılım bulaşmış olsa bile, bilgisayarınızı yeniden kurduktan veya temizledikten sonra dosyaları kurtarmak için bir seçeneğiniz var. Yedeklemelerinize enfekte sistemden erişmeniz durumunda fidye yazılımın silebileceği veya yedekleme

Fidye Yazılımlar (Ransomware)

dosyalarını da şifreleyebileceğini unutmayın. Bu nedenle, saygın bulut tabanlı yedekleme hizmetlerini kullanmak veya her zaman sisteme bağlı olmayan harici sürücülerde yedekleri depolamak önemlidir. Buna ek olarak, birçok kişinin yaptığı yaygın bir hata yedekleme dosyalarından geri dönüş testleri yapmadan, dosyaları kurtarabileceğini varsaymaktır. Düzenli olarak yedeklemelerinizin çalıştığını test ederek, sisteminize Fidye yazılım bulaştığında gereken dosyaları kurtarabileceğinizden emin olun. Yedeklemeler, yanlışlıkla sildiğiniz dosyaları kurtarmak ya da bozulan bir disk nedeniyle dosyalarınızı kaybetmemek için de önemlidir.

Fidye yazılım (Ransomware) bilgisayarınıza bulaştığında tüm dosyalarınızı erişemeyeceğiniz şekilde şifreler.

Diğer Koruyucu Önlemler

Fidye yazılımlara karşı kendinizi, tıpkı digger kötü niyetli yazılım türlerine karşı koruduğunuz gibi koruyabilirsiniz. Güvenilir bir güncel antivirüs yazılımı kullandığınızdan emin olmakla başlayın. Bazen anti-malware yazılımı olarak da adlandırılan bu tür araçlar, kötü niyetli yazılımları tespit etmek ve durdurmak için tasarlanmıştır. Ancak, anti-virüs yazılımları tüm kötü niyetli programları engelleyemez ya da kaldıramaz. Siber suçlular sürekli inovasyon yapıyorlar, farkedilemeyecek yeni ve daha gelişmiş kötü niyetli yazılımlar geliştiriyorlar. Buna karşılık, anti-virüs sağlayıcıları kötü niyetli yazılımları tespit etmek için yeni yeteneklerle ürünlerini güncelliyorlar. Birçok yönden bu her iki tarafın birbirini atlatmak için uğraştığı bir silahlanma yarışı haline gelmiştir. Ne yazık ki kötü adamlar genellikle bir adım öndedir ve bu nedenle sizin kendiniz korumak için dosyalarınızı yedeklemeniz sonrasında aşağıdaki ek önlemleri almanızı öneririz :

- Siber suçlular genellikle yazılım güvenlik açıklarını istismar ederek bilgisayar veya cihazlara fidye yazılım bulaştırırlar. Daha güncel yazılım daha az bilinen güvenlik açıkları demektir ve siber suçluların daha zor bulaştırması anlamına gelir. Bu nedenle, işletim sistemleri, uygulamalar ve cihazlarınızda otomatik güncelleştirmelerin etkinleştirilmiş olduğundan emin olun.
- Bilgisayarlarda, “administrator” ya da “root” hesapları gibi ayrıcalıklı hesaplardan ziyade ayrıcalıkları sınırlı olan standart hesaplar kullanın. Bu, kötü niyetli yazılımların birçok çeşidine karşı kendilerini yüklemelerini engelleyerek ek koruma sağlar.
- Siber suçlular, genellikle kötü amaçlı yazılım yüklemeleri için insanları kandırır. Örneğin, size meşru görünen ve eki olan/bağlantı içeren bir e-posta gönderebilirler. Hatta belki e-posta bankanız veya bir arkadaşınızdan geliyormuş gibi görünür.

Fidye Yazılımlar (Ransomware)

Ancak ekli dosyayı açtığınız veya bağlantıya tıkladığınızda sisteminize kötü amaçlı yazılım yükleyen kod aktif hale gelir. Eğer bir mesaj, güçlü bir aciliyet duygusu yaratıyorsa, kafa karıştırıcı ise, gerçek olamayacak kadar iyi görünüyor ya da kötü bir dilbilgisi ile yazılmışsa, bu bir saldırı olabilir. Şüpheci olun, sağduyu genellikle en iyi savunmadır.

Kendinizi Fidye yazılımlardan, e-posta eklerini açmak veya bağlantıları tıklamak konusunda uyanık olarak, güncel antivirus yazılımlarına sahip olduğunuzu ve düzenli olarak yedekleme yapıp, geri dönülebilir olduklarını doğrulayarak koruyun.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Kaynaklar

Oltalama:	https://securingthehuman.sans.org//ouch/2015#december2015
Kötü Niyetli Yazılım Nedir:	https://securingthehuman.sans.org/ouch/2016#march2016
Şifreleme:	https://securingthehuman.sans.org/ouch/2016#june2016
Yedeklemeler:	https://securingthehuman.sans.org/ouch/2015#august2015
Microsoft Makalesi:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 Eğitimi - Reverse Engineering Malware:	https://sans.org/for610

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley