Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Kişiye Özel Dolandırıcılık

Genel Bakış

Siber suçlular, insanları kandırmanın yeni ve akıl dolu yollarını bulmaya devam ediyor. Yeni bir dolandırıcılık türü popülerlik kazanıyor – kişiye özel dolandırıcılık. Siber suçlular milyonlarca insan hakkında bilgi bulur ya da satın alırlar, daha sonra bu bilgileri saldırılarında kişiye özel olarak kullanırlar. Aşağıdaki örnek bu dolandırıcılıkların nasıl işlediğini ortak bir örnek üzerinden geçerek göstermektedir. Bu tür dolandırıcılıklar hakkında ne kadar çok şey bilirseniz, onları tespit etmeniz ve durdurmanız o kadar kolay olur.

Nasıl İşler?

E-posta veya telefon dolandırıcılığı yeni bir yöntem değildir. Siber suçlular yıllardan beri bu yöntemleri kullanarak insanları dolandırmaya çalışmaktadır. Örnekler arasında "Piyango Kazandınız"veya kötü şöhretli Nijeryalı Prens dolandırıcılığı sayılabilir. Ne var ki, bu geleneksel dolandırıcılıklarda siber suçlular kimi hedeflediklerini bilmezler. Onlar sadece genel bir mesaj oluşturur ve milyonlarca kişiye gönderirler. Bu dolandırıcılık çok genel olduğundan, çoğunlukla tespit edilmesi de kolaydır. Kişiye özel bir dolandırıcılık farklıdır, siber suçlular önce araştırma yapar ve hedeflenen her kurban için özelleştirilmiş bir mesaj oluştururlar. Bunu, kişilerin adlarını, şifrelerini, telefon numaralarını veya diğer ayrıntılarını içeren bir veritabanı bularak veya satın alarak yaparlar. Bu tür bilgilere, saldırıya uğrayan tüm web siteleri nedeniyle kolayca ulaşılabilir. Ayrıca, sosyal medya sitelerinden ve kamuya açık devlet kayıtlarından da yaygın olarak bulunabilir.. Suçlular daha sonra hakkında bilgi sahibi oldukları kişileri hedef alır.

Siber suçluların yaygın olarak kullandığı hilelerden biri, para ödemeye zorlamak için korkutmak ya da baskı yapmaktır. Saldırı şöyle gelişir. Ele geçirilmiş web sitelerinden, kullanıcı bilgileri ve şifreler hakkında bilgileri bulur veya satın alırlar. Kullanıcı hesap bilgilerinizi böyle bir veritabanından bulurlar ve size (ve veritabanındaki diğer herkese), saldırıya uğramış web sitesinde kullandığınız orijinal şifre de dahil olmak üzere sizinle ilgili bazı kişisel bilgileri içeren bir e-posta gönderirler. Suçlu, şifrenizi kendi bilgisayarınızı veya cihazınızı ele geçirmenin kanıtı olarak referans gösterir, bu elbette doğru değildir. Suçlu daha sonra, bilgisayarınızı ele geçirdiğini ve aynı zamanda sizi çevirimiçi pornografik içerikler izlerken yakaladığını iddia eder. Ardından bir e-posta ile, bu şantaj karşılığında para ödemediğiniz takdirde, aileniz ve arkadaşlarınızla utanç verici çevrimiçi etkinliklerinizin kanıtlarının paylaşılacağı konusunda tehdit eder.

Bu ve benzeri hemen hemen her durumda, siber suçlu, aslında sisteminizi ele geçirmemiştir. Kim olduğunuzu ya da hangi web sitelerini ziyaret ettiğinizi dahi bilmemektedir. Dolandırıcı, sizinle ilgili yalnızca birkaç kişisel ayrıntıyı kullanarak sizi ya da cihazınızı ele geçirdiğine inandırmaya, korkutmaya ve para ödemeniz için kandırmaya çalışmaktadır. Unutmayın, kötü niyetli kişiler aynı teknikleri bir telefon görüşmesi aldatmacası için de kullanabilirler.

Ne Yapmalıyım?

Bunun gibi e-postaların veya telefon görüşmelerinin bir aldatmaca olduğunun farkında olun. Birisi sizinle ilgili kişisel bilgiye sahip olduğunda korkmuş hissetmek doğaldır. Ancak gönderenin yalan söylediğini unutmayın. Bu tarz saldırılar, sizi doğrudan hedefleme girişimi değil, büyük bir kitleyi hedefleyen otomatik bir kampanyanın parçasıdır. Günümüzde siber suçluların kişisel bilgileri bulması veya satın alması çok daha kolay hale geliyor, bu nedenle gelecekte daha fazla kişiye özel dolandırıcılık girişimi ile karşı karşıya gelebileceğinizi düşünebilirsiniz. Aranacak bazı ipuçları:

- **Çok acil bir e-posta, mesaj ya da telefon çağrısı çok şüpheli bir durumdur. Birisi korku ya da aciliyet gibi duyguları kullanıyorsa, sizi bir hata yapmak için acele ettirmeye çalışıyordur.**
- **Biri sizden BitCoin, hediye kartları veya diğer izlenemez yöntemler ile ödeme talep ediyorsa**
- **Şüpheli bir e-posta aldığınızda, başkalarının da benzer saldırılar rapor edip etmediğini görmek için Google'da arama yapın.**

Sonuçta sağduyu, en iyi savunmanızdır. Ancak, çevrimiçi hesaplarınızın her biri için her zaman benzersiz ve uzun bir şifre kullanmanızı öneririz. Tüm şifrelerinizi hatırlayamıyor musunuz? Bir parola yöneticisi kullanın. Ayrıca, mümkün olan her fırsatta iki faktörlü (adımlı) doğrulamayı etkinleştirin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

Konuk Editor

***Lenny Zeltser**, Minerva Lab şirketinde kötü niyetli yazılımlara karşı koyacak çözümler geliştiren ve SANS enstitüsünde güvenlik eğitimleri veren deneyimli bir siber güvenlik uzmanıdır. Lenny Zeltser ayrıca yönetilen güvenlik hizmetleri ve danışmanlığı alanlarında da tecrübeye sahiptir. Onu zeltser.com/blog adresinden ve Twitter'da @lennyzeltser hesabından takip edebilirsiniz.*

Kaynaklar

Sosyal Mühendislik:	https://www.sans.org/u/MUU
Oltalama Saldırılarını Durdurmak:	https://www.sans.org/u/MUZ
Kendinizi Çevirim-içi Arayın:	https://www.sans.org/u/MV4
Parola Yöneticileri:	https://www.sans.org/u/MV9