**BASIN BÜLTENİ**

**Günümüzün siber dolandırıcılık yöntemlerini tanıyarak bu saldırılardan korunmak mümkün**

**Giderek daha çok cihaz internete bağlandıkça, kullanıcıların günümüzün siber dolandırıcılık tuzaklarına düşme riski de aynı ölçüde artıyor. Fortinet’e göre, kullanıcılar, cihazları hedef alan siber dolandırıcılık yöntemlerini tanıyarak ve bu yöntemlerin verdiği sinyallere dikkat ederek saldırıları engelleyebiliyor.**

Kişilerin ve Kurumların siber dolandırıcılıklara karşı kendilerini koruması söz konusu olduğunda, her durumda uygulanabilecek genel geçer bir çözüm bulunmuyor. Şirketler ve bireysel kullanıcılar yeni cihaz ve teknolojileri benimsedikçe siber saldırılara karşı daha çok açık veriyor. Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet® (NASDAQ: FTNT), siber saldırganları motive eden değerli bilgileri etkin bir şekilde korumak için, öncelikle kişileri ve kurumları hedef alan farklı siber saldırı yöntemlerini anlamak gerektiğini öneriyor.

**Modern siber saldırılara dair işaretler**

Siber dolandırıcılar, bir ağa ya da cihaza ulaşmak, para sızdırmak veya değerli bilgileri çalmak için çok çeşitli taktik ve yöntemler uyguluyor. Günümüzün gelişen tehditlerini, kişilerin ve kurumların bu tehditlere karşı nasıl bir savunma yöntemi geliştirebileceklerini anlamak, siber suçluların kullandığı sosyal mühendislik taktiklerini bilmekten geçiyor.

Bunu akılda tutan kişiler ve kurumlar, kendilerini hedef alan siber saldırıların ortak noktalarını öğrenerek saldırıların etkisini azaltabilirler:

1. **Oltalama (phishing) yöntemi**

Siber saldırganlar, hem kurumsal hem de kişisel ağlara saldırı için en çok oltalama saldırılarını yöntem olarak kullanıyor. Bu saldırılar, hedefledikleri kullanıcının kimlik bilgilerini, kişisel verilerini, finansal bilgilerini ya da çalıştığı kurumun önemli bilgilerini elde etmeyi amaçlayan siber saldırganın, başka bir kişiden gelmiş gibi görünen e-posta, telefon görüşmesi, mesaj gibi bir iletişim yöntemini kullanmasıyla gerçekleştiriliyor. IBM’nin araştırmasına göre, hedefine ulaşan fidye yazılım sızıntılarının yüzde 59’unun oltalama yöntemi ile gerçekleştirildiği görülüyor. Fortinet, kullanıcıları bu saldırı yöntemini fark etmeleri için şu noktalara dikkat etmelerini öneriyor:

* **Gönderici ismini kontrol edin:** Sizden kişisel bilginizi paylaşmak ya da bir sitede oturum açmak gibi bir aksiyon almanızı isteyen bilmediğiniz bir kaynaktan gelen mesajlara temkinli yaklaşın. Çoğu şirket sizden e-posta ya da kısa mesaj yoluyla bilgilerinizi paylaşmanızı talep etmez. Birinden böyle bir talep geldiğinde, iddia ettiği kişi olmayabileceği düşünülerek bu durum kırmızı alarm olarak değerlendirilmelidir. Bu durumda göndericinin e-posta adresi veya telefon numarası kontrol edilmeli, bir tutarsızlık söz konusu ise göndericinin o olduğunu iddia ettiği kimlik, ilgili kişi veya kurumla karşılaştırılmalıdır.
* **Yazım hatalarına ve dil yanlışlarına dikkat edin:** Profesyonel kurumlar yazılı bir iletişimde bulunmadan önce içeriklerini gözden geçirirler. Ancak, siber suçlular çoğu kez bunu yapmaz.Eğer görünüşte güvenilir bir kaynaktan geldiğini düşündüğünüz, yazım ve noktalama yanlışları, dilbilgisi ve imla hataları olan bir mesaj alırsanız, bu mesajın bir oltalama saldırısı olma ihtimali çok yüksektir.
* **Sizi alarma geçirecek uyarı mesajlarına karşı sakin olun:** Eğer mesajın konusu ve tonu agresif ve endişe verici ise, oltalama saldırısı olma ihtimali çok yüksektir. E-postanızın “İstenmeyen e-postalar” klasöründe“Hesabınızdan para çekildi. Hemen bize ulaşın” diyen bir mesaj görebilirsiniz. Burada amaç sizi rahatsız etmek, paniğe kapılarak saldırganın istediklerini yapmanızı sağlamaktır. Paniğe kapılıp harekete geçmeden önce mesajın gönderildiği iddia edilen tarafla irtibata geçin.
1. **Hedef odaklı oltalama saldırıları (spear phishing)**

Oltalama saldırıları toplu olarak ve fark edilmesi genellikle kolay içerikler olarak gönderilirken, hedef odaklı oltalama saldırıları daha net hedefler belirler ve daha sofistike bir yapıya sahiptirler. Hedef odaklı oltalama saldırılarını kullanan saldırganlar kurbanları hakkında kapsamlı bir araştırma yürüterek saldırılarının başarı şansını artırmak için kurbanlarının çalıştığı kurum, iş arkadaşları ve ilgi alanlarını öğrenmek için mesai harcarlar. Hedef odaklı saldırılara karşı etkili bir şekilde korunmak için şunlara dikkat edilmesi önem arz ediyor:

* **E-posta doğrulama hizmeti kullanın:** E-posta doğrulama hizmetleri aldığınız e-postaları gönderen kaynağın Administrative Management Domain (ADMD)’deki kimliklerle kullanılan e-posta adresinin eşleşip eşleşmediğini teyit eder.
* **Bilgilerinizi paylaşırken tedbirli olun:** Her ne kadar basit gibi görünse de, kullanıcılar biraz daha dikkat ederek kendi bilgilerini kendileri paylaşmazsa, oltalama saldırıları etkin bir yöntem olmaktan çıkacaktır.
* **Güvenlik hijyenine özen gösterin:** En temel güvenlik hijyeni uygulamalarının hayata geçirilmesi, cihazlara zararlı yazılım bulaştırmayı, bilgilere ve kurumların ağına erişmeyi amaçlayan saldırganların en yaygın saldırı vektörlerini kullanmalarına engel olur. Basit, günlük alışkanlıkları değiştirerek saldırıların bir cihazı veya bir ağı tamamen ele geçirmelerini önlemede büyük bir yol kat edilebilir.
1. **Tuzak donanım saldırıları**

Adından da anlaşılacağı üzere, bu yöntemi kullanan saldırganlar, kurbanlarını virüsü cihazlarına indirmeye veya kişisel bilgilerini girmeye yöneltecek bir “tuzakla” kandırmayı amaçlar. Bu saldırılar, ücretsiz anti-virüs yazılımı, kullanıcıların indirebileceği filmler ya da kurbanın bulduğunda cihazına takması için üzerinde “Kurumsal Maaş Bilgileri” yazan ve kurbanın ofisine bırakılan bir usb flaş bellekle somut bir tuzak olarak kurgulanabilir. Bu yöntem çok farklı şekillerde uygulansa da, nihai amaç her zaman aynıdır: Kullanıcıların zararlı bir şeyi cihazlarına yüklemesi için onları tuzağa düşürmek. Kişilerin kendilerini ve çalıştıkları kurumları bu tür tuzaklardan koruyabilmesi için bazı sinyallere karşı uyanık olmaları gerekiyor:

* **“Bedava” tekliflerden uzak durun:** Eğer bir şey “gerçek olamayacak kadar iyi” ise muhtemelen gerçek değildir. Pek çok siber saldırgan, kurbanlarını ücretsiz indirmeler, bedava kargo gönderimleri, bedava üyelik vb. kullanarak kandırmayı amaçlar. Kullanıcıların bu tarz “fırsatlarla” karşılaştıklarında kaynağı kontrol etmeleri ve her türlü anlaşmanın dipnot kısımlarını okumaları gerekiyor. Aynı zamanda bu teklifi sunan kaynaktan teyit alınması öneriliyor.
* **Bilmediğiniz flaş bellekleri veya hard diskleri cihazlarınıza takmayın:** Tuzak donanım saldırıları dijital olarak yapılabileceği gibi zararlı yazılımları cihazlarınıza yüklemek için fiziki sürücülerle de yapılabiliyor. Bu durumda, size ait olmayan sürücüleri cihazınıza takmamaya özen göstermeniz gerekiyor.
1. **Teknik destek dolandırıcılığı**

FBI, sadece 2017’de 11 bin teknik destek dolandırıcılığı bildirimi aldığını duyurdu. Bu dolandırıcılıkların toplamda 15 milyon dolarlık zarara yol açtığı bildirildi. Adından da anlaşılacağı üzere, saldırganlar kendilerine, kurbanın çalıştığı kurumun ya da bağımsız bir servisin teknik destek çalışanı süsü vererek kişisel bilgilere erişmeyi amaçlıyor. Diğer saldırı yöntemleri gibi, burada da saldırının başarılı olup olmaması kurbanın sosyal mühendislik saldırısının tuzağına düşüp düşmemesine bağlı. Bunu akılda tutarak, bu saldırıyı açık eden bazı kırmızı alarm niteliğindeki uyarılara dikkat etmek gerekiyor:

* **İstenmeyen mesajlara dikkat edin:** Teknik destek uzmanları genellikle bilgisayarınızdaki sorunları çözmek ve cihazınızı kontrol etmek için size ulaşmaz.Yazılım ve donanım geliştiriciler çözümlerinin ne durumda olduğunu asla takip etmez ve güvenlik desteği için sizi aramaz. Eğer herhangi bir teknik destek çalışanı veya şirketi size açılır pencere reklamı, sizin talebiniz dışında gönderilen bir e-posta veya beklemediğiniz bir telefon görüşmesi aracılığıyla ulaşmayı deniyorsa muhtemelen bir dolandırıcılıkla karşı karşıyasınız demektir. Gerçek ve meşru şirketler ürün ve çözümlerini güncellemek için belirli sürelerde yama ve güncellemeler yayınlar veya çözümün doğrudan kendisinde bulunan yöntemlerle sorunları çözer.
* **Bilmediğiniz kaynaklardan yükleme yapmayın:** Doğrudan bildiğiniz ve güvendiğiniz bir kaynaktan olmadığı sürece, cihazınıza zararlı yazılımlar bulaştırma riski taşıyacağı için internetten herhangi bir şey indirmekten kaçının. Tuzak donanım saldırılarında olduğu gibi, siber suçlular, kullanıcıların bilgisayarlarına zararlı yazılımlar bulaştıran “ücretsiz güvenlik taraması” veya “bilgisayar temizliği” önererek kurbanlarını kandırmayı amaçlar.
* **Cihazınıza uzaktan erişim taleplerine temkinli yaklaşın:** Uzaktan erişim, teknik destek ekiplerinin bilgisayarınızdaki bir sorun çözmek için cihazın yönetimini uzaktan devralmasına izin verir. Ancak, aynı teknoloji cihazınızdaki kişisel bilgilerinizin kolayca ele geçirilmesi için de kullanılabilir. Eğer kaynağından emin olmadığınız bir uzaktan erişim talebi alırsanız, bu talebi asla kabul etmeyin.
1. **Mobil cihaz güvenliği**

Mobil cihazlar da giderek siber saldırganların öncelikli hedefi haline geliyor. Veri elde etmeye çalışan sahte uygulamalar veya zararlı yazılımlar özellikle Android işletim sistemli cihazlar için yaygınlaşıyor.

* **Gerçek uygulama ve güncelleme gibi görünen zararlı yazılımlara dikkat edin:** Üçüncü taraf uygulama mağazalarındaki sahte uygulama sayısı her geçen gün artıyor. Ayrıca, uygulamaları ve cihazları istismar eden kripto-gasp yazılımları gibi eklenti ve güncellemeler de artıyor. Bunlara ek olarak, gereksiz izin taleplerinde bulunan uygulamalara karşı da dikkatli olmak gerekiyor (cihaz Yöneticisi ve kötü amaçlı SMS’ler gibi).
* **Güvenli WiFi ağlarını kullanın: Ücretsiz WiFi ağlarına temkinli yaklaşın.** Ücretsiz WiFi erişimi sunan kamuya açık alanlar ve mağazalar iki nokta arasındaki bağlantıyı izinsiz izleyen saldırganlar için en uygun lokasyonlardır. Bu saldırılarda, saldırganlar WiFi hizmetlerinin kullanılabileceğini duyurur ve ardından bu ağı veri ele geçirmek için kullanırlar. Herkese açık bir WiFi ağı kullandığınızda, VPN bağlantılarını kullanın ve kritik işlemlerinizi gerçekleştirmekten kaçının. Pek çok mobil uygulama tanıdığı ağlara otomatik olarak bağlanacak şekilde programlanmıştır. Bundan faydalanan siber saldırganlar, kullanıcıların herhangi bir kullanıcı bilgisi girmeden otomatik olarak cihazlarını bu ağlara bağlamasını sağlamak için “Ev Ağı” gibi genel ağ adları kullanırlar.
1. **Nesnelerin İnterneti cihazları**

Nesnelerin interneti cihazları giderek yaygınlaşan bir diğer saldırı vektörü olarak biliniyor. Çoğu nesnelerin interneti cihazının kolayca istismar edilebilmesi, kesintisiz internet bağlantısına sahip olması ve güçlü GPU işlemciler kullanması bu cihazların kripto-para madenciliği ve DDoS saldırıları için uygun bir hedef olmasını sağlıyor. Fortinet, bu cihazları hedef alan saldırılara karşı kullanıcılara şu önerilerde bulunuyor:

* **Kimlik bilgilerinizi güncelleyin:** En yaygın saldırı stratejisi, herhangi bir nesnelerin interneti cihazının ön tanımlı kullanıcı adı ve şifresini kullanarak cihaza bağlanmaya çalışmaktır. Sık sık yönlendirme cihazlarınızın, akıllı TVlerinizin ve ev eğlence sistemlerinizin şifrelerini değiştirin.
* **Akıllı arabalar:** Giderek daha çok cihaz birbirine bağlandıkça, güvenlik zafiyetleri de aynı oranda artıyor. Akıllı arabalar gibi cihazlar, sahip oldukları kullanıcı verileri, telefon numaraları ve hatta ödeme bilgileriyle saldırganlar için cazip hedefler olarak dikkat çekiyor. Bu cihazların ele geçirilmesi hem sürücüleri hem de yolcuları çeşitli risklerle karşı karşıya bırakıyor. Akıllı bir araba aldığınızda, dikkatlice inceleyin, ön tanımlı güvenlik ayarlarını değiştirin ve bilmediğiniz kaynaklardan uygulama kurulumu yapmaktan kaçının. Ayrıca, özellikle aracınızdaki ağa arayüz bağlantısıyla bağlanan Bluetooth bağlantılı cihazların güvenlik ve kimlik bilgilerini gözden geçirin.

Siber saldırılar bu ortak uyarılara dikkat etmeyen herkesi etkileyebilir. Kullanıcılar bir ağa bağlı cihazlar kullanmaya devam ettikçe, siber dolandırıcıların tuzağına düşme riskleri de artacak. Kullanıclar, günümüzde kendilerini hedef alan en yaygın siber dolandırıcılık yöntemlerinin farkında olarak ve bu yöntemlerin verdiği sinyallere dikkat ederek, kişisel verilerini ve ağa bağlandıkları bilgileri koruyabiliyor.

**İlgili Kişi:**
Eray Çoşan Akkuş
Marjinal Porter Novelli
0 533 927 23 97
erayc@marjinal.com.tr

**Fortinet Hakkında**
Fortinet (NASDAQ: FTNT) dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün artan sanal saldırılara karşı müşterilerine akıllı ve sorunsuz koruma sağlar, sınırların ortadan kalktığı ağların artan performans ihtiyaçlarını karşılar. Ağlardaki uygulamaların, bulut sistemlerinin ve mobil cihazların karşılaştığı en kritik güvenlik sorunlarına karşı performanstan ödün vermeden güvenlik sunan tek çözüm sadece Fortinet'in Security Fabric mimarisidir. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 360 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Daha fazla bilgi için: [http://www.fortinet.com](http://www.fortinet.com/), [Fortinet Blog](https://blog.fortinet.com/) sayfası veya [FortiGuard Labs](https://fortiguard.com/).