BİR KARELİK TUZAK: “QUISHING” VE FİNANSAL SUÇ PERSPEKTİFİ

I. QR Kodların Yaygınlaşması ve Artan Risk Alanı

QR kodlar, son yıllarda restoran menülerinden ödeme işlemlerine, internet sitelerine hızlı erişimden bilgi paylaşımına kadar gündelik yaşamın birçok alanında yaygın şekilde kullanılmaktadır. Özellikle mobil cihazlar aracılığıyla kolaylıkla taranabilmeleri ve kullanıcıya hızlı erişim imkânı sunmaları, bu teknolojinin erişilebilirliğini ve kullanım sıklığını önemli ölçüde artırmıştır. Bununla birlikte, QR kodlar aracılığıyla yönlendirilen içeriklerin kullanıcı tarafından tarama öncesinde açık ve şeffaf biçimde görülememesi, güvenlik ve veri gizliliği bakımından belirli riskler doğurmaktadır. Fiziksel veya dijital ortamlarda karşılaşılan bir QR kodun taranması, kullanıcının farkında olmaksızın kötü amaçlı bir internet sitesine yönlendirilmesine veya kişisel verilerini paylaşmaya sevk edilmesine yol açabilmektedir.

QR kodların özellikle ödeme süreçleri, kampanyalar ve hesap doğrulama gibi finansal işlem temelli kullanım alanlarında yaygınlaşması, bu teknolojinin yalnızca bir erişim aracı olmaktan çıkıp potansiyel bir finansal suistimal vektörüne dönüşmesine neden olmuştur. Bu çerçevede, QR kodlar üzerinden gerçekleştirilen özel bir oltalama yöntemi olan “*quishing*”, kişisel ve finansal verilerin ele geçirilmesi suretiyle dolandırıcılık ve yetkisiz işlem risklerini tetikleyebilen bir finansal suç başlığı olarak dikkat çekmektedir.

II. “*Quishing*”in Tanımı ve İşleyiş Mekanizması

“*Quishing*” terimi, “QR” (*Quick Response*) ve “*phishing*” (*oltalama*) kelimelerinin birleşiminden oluşmakta olup sahte veya sonradan değiştirilmiş QR kodlar aracılığıyla kullanıcıların kötü amaçlı içeriklere yönlendirilmesini ifade etmektedir. Bu saldırı türünde tehdit aktörleri, kullanıcıyı meşru ve güvenilir olduğu izlenimi verilen bir QR kodu taramaya teşvik etmekte; ardından sahte giriş sayfalarına, zararlı yazılım içeren dosyalara veya sahte ödeme arayüzlerine yönlendirme gerçekleştirmektedir.

Teknik açıdan bakıldığında, QR kodları statik ve dinamik olmak üzere ikiye ayrılmaktadır. Statik QR kodlarda içerik sabitken, dinamik QR kodlarda kodun görsel yapısı değişmeden yönlendirilen içerik güncellenebilmektedir. Bu esneklik, meşru kullanım açısından avantaj sağlamakla birlikte, dinamik QR kodların arka planda bir yönlendirme adresi üzerinden çalışması, görselde herhangi bir değişiklik olmaksızın içeriğin kötü amaçlı bir kaynağa dönüştürülmesine imkân tanıyabilmektedir. Bu durum, “*quishing*” saldırılarının tespitini güçleştiren önemli unsurlardan biridir.

III. “*Quishing*” Saldırılarının İşleyişi ve Tespit Göstergeleri

“*Quishing*” saldırıları, kullanıcıda zararsız veya gerekli bir QR kodla etkileşimde bulunduğu algısını oluşturmaya dayanmaktadır. Saldırganlar, bilinen internet sitelerini taklit eden sahte giriş sayfalarına yönlendiren bağlantılar, sahte ödeme süreçleri veya zararlı yazılım içeren dosyalar barındıran QR kodlar oluşturabilmektedir. Bu kodlar fiziksel ortamlara yerleştirilebildiği gibi, e-posta veya mesajlaşma kanalları aracılığıyla görsel unsur şeklinde de iletilebilmektedir. QR kodun görsel formatta gönderilmesi, bağlantının bazı güvenlik filtreleri tarafından doğrudan analiz edilmesini zorlaştırabilmektedir.

Tespit bakımından dikkat çekebilecek göstergelere örnek olarak; kamuya açık alanlarda sonradan yapıştırılmış izlenimi veren veya bulunduğu yüzeyle uyumsuz görünen QR kodlar, kaynağı belirsiz kampanya veya ödeme yönlendirmeleri, beklenmeyen göndericilerden gelen ve aciliyet duygusu yaratan iletiler, tarama sonrası kimlik doğrulama veya ödeme bilgisi talep eden şüpheli sayfalar, temsil ettiği iddia edilen kurumla uyuşmayan alan adları veya beklenmeyen dosya indirme talepleri verilebilir.

QR kodların görsel olarak büyük ölçüde benzerlik göstermesi ve yönlendirme adresinin tarama öncesinde kullanıcı tarafından açıkça görülememesi ise riskin ilk aşamada fark edilmesini güçleştiren temel unsurlardan biridir.

IV. “*Quishing*”in Finansal Suç Ekosistemindeki Yeri

“*Quishing*”, yalnızca bir siber güvenlik zafiyeti değil, finansal suçların işlenmesinde kullanılabilecek işlevsel bir araç niteliği taşımaktadır. Sahte giriş sayfaları üzerinden ele geçirilen kimlik doğrulama bilgileri, kart verileri veya hesap erişim bilgileri; dolandırıcılık, hesap ele geçirme ve yetkisiz ödeme işlemleri gibi doğrudan finansal kayba yol açabilecek eylemlere zemin hazırlayabilmektedir. Özellikle ödeme süreçlerine veya teslimat, kampanya ve hesap güvenliği gibi temalara dayandırılan senaryolar, kullanıcıların finansal işlem yapmaya daha yatkın olduğu anları hedef alabilmektedir.

QR kodların hem fiziksel hem dijital ortamlarda yaygın kullanım alanına sahip olması, bu yöntemi sosyal mühendislik temelli finansal suçlar bakımından etkili bir yönlendirme vektörü hâline getirmektedir. Görsel olarak güven veren bir karekodun arkasında gizlenen yönlendirme altyapısı, suç gelirinin elde edilmesine veya finansal verilerin ele geçirilmesine aracılık edebilmektedir. Bu yönüyle quishing, dijital ödeme alışkanlıklarının arttığı ve mobil cihazların finansal işlemlerde merkezi rol üstlendiği bir ortamda, finansal suç risk haritasında giderek daha görünür hâle gelen bir başlık olarak değerlendirilmektedir.

Bu risklere karşı bireylerin; kamuya açık alanlardaki QR kodlara temkinli yaklaşmaları, tarama sonrası yönlendirilen bağlantıyı dikkatle incelemeleri, kişisel ve finansal bilgilerini paylaşmadan önce internet sitesinin doğruluğunu teyit etmeleri ve mümkünse adresi manuel olarak tarayıcıya girmeleri önem taşımaktadır. Ayrıca cihaz güncellemelerinin yapılması ve çok faktörlü kimlik doğrulama kullanılması gibi temel güvenlik önlemleri de riskin azaltılmasına katkı sağlayacaktır.