“Proxy” Tabanlı Oltalama Saldırıları Yeniden Yükselişte

medium.com/cyberwise/proxy-tabanlı-oltalama-saldırıları-yeniden-yükselişte-139a9eb8ee79

Cyberwise August 24, 2023

--

Özet

· Potansiyel kurbanın gerçek sayfa ile iletişimi “reverse proxy” teknolojisi kullanılarak sağlanmaktadır.

· Gerçek sayfa yüklendiğinden, çok adımlı doğrulama şemaları etkisizleşebilmektedir. MFA doğrulama talepleri reverse proxy aracılığı ile gerçek sisteme yönlendirilmektedir.

· “**EvilProxy**” gibi illegal servisler tehdit aktörlerine para karşılığında hazır teknik altyapı sağlamaktadır.

· Tehdit aktörleri otomasyonlar yardımıyla kalıcılık ve veri sızdırma amaçlarını hızlıca gerçekleştirebilmektedir.

· Bulut ortamında tutulan ve erişilebilen pek çok veri herkese açık paylaşımlar ile sızdırılabilmektedir.

· Bu tip saldırılar yeni olmamakla birlikte alt yapıyı para karşılığı sunan servislerin ortaya çıkmasıyla bu ve buna benzer saldırıların yaygınlığında artış gözlemlenmiştir.

Son zamanlarda gözlemlenen oltalama amaçlı e-postalarda, tehdit aktörlerinin, oluşturdukları vekil sunuculardan faydalandıkları gözlemlenmiştir. Bu yaklaşımda tehdit aktörü, kurban ile gerçek erişim sayfaları arasındaki trafiği izleyip, modifiye ederek erişim ve bilgi sızıntısı hedeflerine ulaşabilmektedir. Konsept, MitM (man-in-the-middle) konseptine benzerliğiyle dikkat çekmektedir. Gerçek sayfa ile aynı zamanlı iletişim gerçekleştiğinden çoklu kimlik doğrulama gibi önlemler de etkisiz kalabilmektedir. Bu saldırılarda aktörlerin, yük dengeleme sistemlerinde de kullanılan reverse proxy teknolojilerini kendi saldırılarında kullanmaya başladığı görülmektedir.

Örnek Oltalama e-postası
göre, güvenliği ihlal edilmiş kullanıcıların kurumlardaki rolleri yaygın olarak Üst Düzey Yönetici, Finans Direktörü ve Yönetici Yardımcısı rolleridir. Tehdit aktörleri, diğer düzeydeki çalışanlara da ilgi gösterdikleri ve çabalarını finansal varlıklara veya hassas bilgilere erişimi olan personele odakladıkları gözlemlenmiştir.

Role göre güvenlik ihlal yayılımı (ProofPoint Araştırması)
Bu yöntemden faydalanan tehdit aktörleri, otomasyon tekniklerini kullanarak hızlı ve kitlesel saldırılar gerçekleştirme kabiliyetine ulaşabilmektedirler. Ek olarak saldırıyı gerçekleştirmek üzere gerekebilecek hedef bilgilerini, teknik altyapıyı ve oltalama amaçlı e-posta servisleri başka tehdit aktörleri tarafından pazarlanan servisleri kullanmak yoluyla elde edebilmektedirler. Bu servislerden bazıları oltalama kurbanının, organizasyondaki yerine göre önem seviyesini de ilişkilendirebilmekte ve servis kullanıcısını yönlendirebilmektedir.

Oltalama amaçlı saldırılarda, kullanılan altyapılar genellikle başka kurbanların altyapılarından oluşmaktadır. Bu durum saldırı sonrası yapılan çalışmalarda geriye takibi ve tehdit aktörünün kimliğinin tespitini zorlaştırabilmektedir. Ek olarak inceleme yapan kişilerin veya güvenlik amaçlı yazılımların işini zorlaştırmak üzere ek güvenlik önlemleri aldıkları bilinmektedir. Aşağıdaki metinler “” isimli servisin öneri metodlarından alınmıştır.

Öneriler

· Personel için farkındalık eğitimlerinin ve gerçekçi tatbikatların gerçekleştirilmesi,

· Saldırı öncesi önlem ve saldırı sonrası tespit amaçlı veri akışı için siber tehdit istihbaratı sağlanması,

· Uygulama ayar ve kural değişikliklerinin takibi, (Kullanılıyorsa bulut ortamında bulunan servisler ihmal edilmeyerek)

· Uygulama erişim günlüklerinin takibi (Kullanılıyorsa bulut ortamında bulunan servisler ihmal edilmeyerek)

· Data Loss Prevention (DLP) entegrasyonu sağlanması,

· Servisler için konum, zaman, internet servis sağlayıcı ve rol tabanlı erişim yönetimi ve kısıtlamalarının gerçekleştirilmesi,

· E-posta güvenliği için DMARC-SPF-DKIM Mekanizmalarının doğru biçimde yapılandırılması ve

· E-posta güvenliğini sıkılaştırma amaçlı aşağıdaki bağlantıda yer alan kılavuz incelenebilir.

Diyagram: EvilProxy Saldırılarının Yaşam Akışı