**BASIN BÜLTENİ**

**Siber saldırılar finans sektörünü etkilemeye devam ediyor**

**Financial Industry Regulatory Authority (FINRA), aracılık yapan firmaları devam etmekte olan oltalama saldırılarına karşı uyarıyor.**

Şirketlerin güvenlik açıklarını bulma ihtiyacını platforma kayıtlı yüzlerce bağımsız araştırmacıdan oluşan güvenilir toplulukla hızlı, hesaplı ve etkin bir şekilde çözen BugBounter, Amerika’daki aracı işlemlerini gözeten ve kâr amacı gütmeyen bir kuruluş olan FINRA’nın (Financial Industry Regulatory Authority) finans dünyasının önemli bir parçası olan aracılara yönelik oltalama saldırısı uyarısını paylaşıyor.

Sosyal mühendislik yöntemleri arasında ilk sıralarda yer alan oltalama saldırıları, kişinin cihazının yasal kaynaklar tarafından oluşturulmuş bir içeriğe benzetilen e-posta ya da web sitesi üzerinden ele geçirilmesini hedefliyor. Başarıyla gerçekleşen bir oltalama saldırısının ardından ele geçirilen bilgisayardaki tüm dosyalar ve o bilgisayardan gönderilen tüm e-postalar risk taşımaya başlıyor.

Konuyla ilgili görüşlerini belirten BugBounter Kurucu Ortağı Murat Lostar, şunları söyledi: “Business e-mail compromise ya da kısaca BEC olarak adlandırılan bu saldırı yönteminde ele geçirilmiş bir bilgisayarda açık bir e-posta adresi üzerinden kullanıcının haberi olmadan şirketin diğer çalışanlarına e-posta gönderiliyor. E-postayı alan kişi, gönderen kişiyi tanıdığını düşünerek içindeki bağlantıya tıklıyor ve zararlı bir siteye yönlendirildiği için o cihaz da ele geçiriliyor. Ya da finans dünyası tarafından baktığımızda para transferleri farklı hesaplara yönlendirilebiliyor. FBI’ın 2020 Şubat’ta yayınladığı rakamlara göre 2019’da BEC saldırıları yüzünden yaşanan kayıp 1,7 milyar dolar seviyesini [geçti](securityweek.com/bec-losses-surpassed-17-billion-2019-fbi). Yapılan araştırmalar dünyanın dört bir yanındaki en az 150 şirket bu saldırılardan etkilendiğini ve toplamda 15 milyar doların, gitmesi gereken hesaba ulaşmadığını ortaya koyuyor. Öte yandan [Microsoft Security Intelligence](https://twitter.com/MsftSecIntel/status/1356649995710025728) da BEC saldırılarındaki yaşanan artışa dikkat çekiyor. Bu yüzden çalışanların bir e-posta geldiği zaman doğruluğundan emin olması gerekiyor. Kurumların da sistemlerini düzenli olarak denetletmesi gerekiyor. Bu noktada ödül avcılığı programları sayesinde şirketler uygun maliyetle uzun süre şirketlerini devamlı olarak kontrol ettirebiliyor. BugBounter gibi bir platforma sahip şirketle birlikte ilerlediklerinde ise ödül avcılığı programının kalitesi ve alınan verim önemli derecede artıyor.”

**İlgili Kişiler:**

Önder Kalkancı - Marjinal Porter Novelli

0533 927 23 95

[onderk@marjinal.com.tr](mailto:onderk@marjinal.com.tr)

Sezin Bulum - Marjinal Porter Novelli

0537 465 82 25

[sezinb@marjinal.com.tr](mailto:sezinb@marjinal.com.tr)

**BugBounter hakkında**

Bağımsız araştırmacıların niteliksel ve niceliksel açık keşfetme gücünü doğrulama süreçlerinden geçirerek sunan BugBounter, hacklenmeyen bir dünya vizyonuyla siber güvenlik uzmanlarından oluşan bir ekosistem kurmaktadır. Şirketlerin kendilerini siber saldırılara karşı güçlendirmesini sağlayan BugBounter, tüm süreci hem firmalar hem de araştırmacılar için demokratikleştiren tek platformun geliştiricisidir. <https://bugbounter.com/>