**BASIN BÜLTENİ**

**BugBounter, güvenlik açığı arayan siber saldırganların kullandığı 4 yöntemi paylaşıyor**

**COVID-19 pandemisi ile dijitalleşen şirketlerin sistemlerindeki açıklar, hacker’lar için yeni fırsatlar yaratıyor. Her ne kadar kurumların iç güvenlik ekipleri siber saldırganlara karşı durmaksızın mücadele ediyor olsa da güvenlik stratejileri hacker’ların gelişen yöntemlerine göre düzenlendiğinde daha etkili oluyor. Bu yüzden BugBounter, siber saldırganların tercih ettiği 4 güncel yönteme dair bilgi veriyor.**

Geleneksel süreçlerin dijital dünyaya entegre edildiği günümüzde siber güvenlik ekiplerinin hacker’lara karşı verdiği savaş gün geçtikçe büyüyor. Siber güvenlik uzmanlarının aksine belli kurallar veya sistem çerçevesinde çalışma zorunluluğu bulunmayan siber saldırganlar, kendilerine has birtakım süreçleri takip ediyor. Şirketlerin güvenlik açıklarını bulma ihtiyacını platforma kayıtlı yüzlerce bağımsız araştırmacıdan oluşan güvenilir toplulukla hızlı, hesaplı ve etkin bir şekilde çözen BugBounter.com da teknoloji ekiplerinin elini güçlendirmek için hacker’ların kullandığı yöntemleri aktarıyor.

**Saldırganlar, siber güvenliğin en düşük seviyede olduğu yerleri arıyor**

Siber saldırganlar, ele geçirebilecekleri cazip bir hedef belirledikten sonra güvenlik açığı bulmak için birçok farklı tekniği bir arada kullanıyor. Bazı hedefler saldırganlara daha hızlı zafer kazandırabilirken, bazıları için daha fazla zaman harcaması gerekebiliyor. Bu yüzden bazı saldırganlar denenmiş ve başarı kazandırdığı ispatlanmış yöntemleri kullansa bile yaratıcı hacker’lar uzmanların tahmin edemediği yöntemler üzerinden sistemlere sızmanın yollarını buluyor. Şirket içi güvenlik ekiplerinin etkili savunma stratejileri geliştirirken savundukları sistemde hacker’lar için en cazip bölümleri tespit etmesi çok önemli.

Öte yandan bir saldırganın yazılımda hata ararken kullandığı bakış açısı, güvenlik uzmanlarının değerli varlıkları nasıl koruyacağını belirlemesine yardımcı olabiliyor. Saldırganların en yaygın şekilde kullandığı dört yöntem ise şöyle:

**Bilinen Zafiyet ve Açıkların (CVE) Benzerlerini Bulma**

Güvenlik ekiplerine ulaşan uyarı kadar siber saldırganlar da güvenlik açığı bilgileriyle karşılaşıyor. Fakat bunların sadece ufak bir kısmı amaçları için önem taşıyor. Bu yüzden saldırganlar ilk aşamada hedef aldıkları sistemde son dönemlerde en çok rastlanan güvenlik açıklarını kontrol ediyor. Bu noktada herkes tarafından bilinen yaygın açıklar, kodlarda gizlenen benzer hataları keşfetmek için referans noktası haline geliyor.

**Çözümlenmemiş Sorunları İçeren Yazılımcı Notları**

Kaynak kodunu okuyan saldırganlar, aradıkları güvenlik açığını burada bulabiliyor. Genellikle en kolay ulaşabilen güvenlik açıkları, uygulamaların geliştirme sürecinde yazılım ekibinin birbirleri için bıraktıkları notlar üzerinden tespit edilebiliyor. Buna rağmen yazılımcılar da teslim tarihlerine yetişebilmek için bu notları göz ardı edip odağını sistemin başka bir alanına kaydırabiliyor. Bir kodu incelerken yazılımcılar tarafından bırakılan "FIXME" (beni onar) veya "RBF" (remove before flight, canlıya almadan önce kaldır) etiketlerini gören siber saldırganlar, aradıkları açığı bu şekilde kolayca bulmuş oluyor. Bu yüzden standart etiketler ve kaldırılmamış notlar sistemin ele geçirilmesinde önemli rol oynayabiliyor.

**Destek forumlarında “SOS” uyarıları**

Şirketlerin BT ekipleri kurumsal e-posta adreslerini kullanarak herkesin erişimine açık bir destek forumunda soru yayınlayabiliyor. Siber saldırganlar da bunları yakından takip ediyor. Ele geçirmesi kolay cihazları belirliyor, destek forumlarını araştırıyor ve çevrimiçi olarak yayınlanan ve hatalar içeren ürün yazılımı güncellemelerini bulabiliyor. Bu hatalar arasında kimlik doğrulamayı atlamanıza izin veren hatalar, sistem yöneticisi olmayı gerektirmeyen kod yolları ve dosya sızıntıları gibi sorunlar yer alabiliyor. Saldırganlar, bir istismara yol açabilecek bilgileri bulmak için güvenlik duvarlarını incelemenin dışında siber güvenlik ekibinde yer alan üyelerin paylaşımlarını takip edebiliyor.

**Spearfuzzing: Hedefe odaklı saldırılar**

Fuzzing, hataları bulurken daha fazla zaman alan ve yeterli başarıyı sunmayan bir yöntem. Fuzzing, bir ağdaki açıkları bulmak için kolay bir yol gibi görünebiliyor ancak saldırganlar canlıya alınmış bir sisteme karşı fuzzing saldırısı yaptığında, neredeyse her sefer sistem yöneticilerine uyarı gidiyor. Bu yüzden spearfuzzing adı verilen daha gelişmiş bir yöntem tercih edilebiliyor. Spearfuzzing’in fuzzing’den tek farkı ise sürece bir çalışanın dahil edilmesi. Saldırılabilecek alanı önceden belirlemek için çalışanların bilgisi kullanıldığında siber saldırganlar harcadıkları zamanın büyük bir kısmını geri kazanabiliyor.

Güvenlik uzmanlarının sürekli olarak saldırganların izinsiz girişlerini engellemeye odaklandığını belirten Arif Gürdenli, “Siber saldırganlar güvenlik uzmanları gibi düşünmüyor ve harcadıkları zamana, çabaya ve kaynağa odaklanıyor. Saldırganlara karşı savunma geliştiren kurumların ilk aşamada hacker’ların mantığına uyum sağlaması ve bir hedefi cazip kılan şeyin ne olduğunu anlaması gerekiyor. Güvenliği ihlal edilmiş bir yazılımın yaratabileceği sorunu anlayan ekipler, sistemin en kritik alanlarındaki koruma katmanını artırarak sistemlerini daha iyi savunabiliyor. Farkında olunmayan açıkları en hızlı şekilde belirlemenin yolu ise bug bounty (ödül avcılığı) programlarını test süreçlerine dahil ederek çok sayıda yeteneğin gücünden yararlanmak. Bu yaklaşım sayesinde güvenlik uzmanları açıkların yerlerini hızla tespit edebiliyor ve gerçekten zarar verebilecek açıkları ortadan kaldırabiliyor. Hacker’ların bakış açısını anlamak, kurumların alışılmış yolların ötesinde dayanıklılığa sahip olmasını, katmanlı bir erken uyarı ve savunma stratejisi oluşturmasını ve siber saldırganları sistemlerinden uzak tutmasını sağlıyor” dedi.

**İlgili Kişiler:**

Önder Kalkancı - Marjinal Porter Novelli

0533 927 23 95

onderk@marjinal.com.tr

Sezin Bulum - Marjinal Porter Novelli

0537 465 82 25

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/