COMODO
Creating Trust Online®

Comodo: Hacker saldırıları her saniye olabilir

COMODO, 25.10.2016 - Başkanlık için geri sayımın sürdüğü Amerika'nın siber saldırıların hedefi olması ve bu saldırıların tüm dünyayı etkilemesi, akıllı ürünler tasarlayan ve üreten şirketlerin siber güvenliğe öncelik vermesinin ne kadar hayati önemde olduğunu da ortaya koydu. Öyle ki; Gartner'ın yaptığı bir araştırmaya göre günümüzde her gün 5.5 milyon yeni nesne (telefon, saat, bilgisayar, araba gibi) internete bağlanıyor ve bu sayı 2020'de 20.8 milyarı bulacak. Güvenlikten taviz verilmesi durumunda ise insanları hayata bağlayan sistemlerin tamamen çöküşü gözlenecek.

Comodo, "Nesnelerin internetinin" artık günlük hayatın bir parçası olduğuna dikkat çekiyor. İnternet bugün hayatımızın her alanına yayılmış durumda. İnternet bağlantısı yoluyla daha iyi işlevler sunan akıllı arabalarımız ve tıbbi aletlerimiz var; kol saatlerimiz, mutfak ekipmanlarımız, akıllı evlerimiz, giyilebilir teknoloji ürünlerimiz… Comodo, "Ama bir noktayı unutmayalım; hayat daha akıllı hale geldikçe gizli riskler de artıyor" uyarısı yapıyor.

Peki; ne yapmak gerekiyor? "Daha akıllı olmalıyız" diyen Comodo'nun "Güvenliğe öncelik vermeliyiz" başlığı altında dikkat çektiği konular şöyle:

*Özellikle farklı sebeplerden ötürü güvenlik özelliklerinden taviz verebilecek ürünleri tasarlama ve üretme aşamasında, -nesnelerin interneti-nin karşımıza çıkaracağı zorlukları anlamalıyız. Örneğin; düşük maliyetli bileşenlerle düşük maliyetli cihazlar üretme iddiasında olan şirketler güvenlikten taviz vermek zorunda kalabilir.

*Eğer bir cihazda kullanılan yazılım dili iyi planlanmamışsa bu da güvenliği tehlikeye sokabilir. Bu nedenle güncelleştirme döngüleri ve cihaz yaşam döngüleri uzadıkça güvenlik zafiyetleri artabilir. Hackerler cihazların güncel olmamasından istifade ederek yazılımdaki güvenlik zafiyetlerini kullanıp verileri çalabilir veya kullanıcı davranışlarının kontrolünü ele geçirebilirler. Zaman zaman akıllı cihaz üreticileri de sistem performansını geliştirmek için ciddi sonuçları olabilecek SSL şifreleme ve kimlik doğrulama gibi güvenlik özelliklerinden taviz verebilir.

*Tüm bu nedenlerden ötürü; güvenlik, tasarım sürecinin temel bir parçası olarak yer almalıdır. Bu, sonradan bir anti-virüs yazılımı veya bir anti zararlı yazalım ürünü eklemekten daha iyi olacaktır. Bir cihaz tasarlanırken güvenlik de maliyet, performans ve diğer buna benzer faktörlerle birlikte değerlendirilmelidir.

COMODO
Creating Trust Online®

*Bu yüzden tüm –nesnelerin interneti-cihazı araştırmacıları ve üreticileri için güvenlik risklerini belirlemek ve bunların üzerine eğilmek, bu riskleri takip etmek, zafiyetleri aramak ve bunları onarmak bir zorunluluk haline geliyor.

*Geliştirme aşamasında, saldırı yüzeyinin artmasına yol açabilecek gereksiz işlevlerin kaldırılması gerekir. Cihaza bir de iyi ve güvenli bir güncelleme mekanizması yerleştirilmelidir. Bu şekilde, iyi bir liderlik ve kurumlardaki güvenlik uzmanlarının tam desteği ile güvenliğe ilişkin yüksek standartlar korunabilir ve biz ancak o zaman –nesnelerin interneti-teknolojisinden tam anlamıyla faydalanabiliriz.

Çözüm 'Comodo'yla mümkün

Bu noktada hacker saldırılarının arttığını vurgulayan Comodo, son yaşanan DDoS saldırılarında zararlı yazılım bulaşmış olan uç noktalara dikkat çekiyor. Zararlı yazılım bulaşmış ve uzaktan yönetim altında tutularak saldırı gerçekleştirmek için kullanılabilecek internete bağlı bir bilgisayar olarak tanımlanan zombi bilgisayarlar, birden fazla botnet makineleri ile eşgüdümlü botnet saldırısı düzenleyebilirler. Saniyede dört yeni zararlının üretildiği günümüzde bunu ancak sıfırıcı gün ataklarını önleyebilen "yeni nesil" uç nokta güvenlik çözümler ile yapmak mümkündür. Comodo Gelişmiş Uç Nokta Koruma çözümü yeni nesil, katmanlı ve default deny teknolojisi kullanılarak hazırlandı. Bu platform kötü amaçlı yazılımlar, casus yazılımlar, Trojan'lar ve çalıştırılabilir diğer zararlı programların yol açtığı bilinmeyen salıdırılar ile sıfırıncı gün saldırılarını engelliyor ve izole ediyor. Böylece; bu saldırıları, uç noktara karşı etkisiz kılıyor.

Gelişmiş Uç Nokta Güvenlik Çözümünün yanı sıra Comodo patent başvurusu yapılmış ödüllü SecureBox ürününün kullanılması ile tam koruma sağlamak mümkün. Bu teknoloji sayesinde uygulamalar, bilgisayarda korunaklı ve tamamen fonksiyonel bir bölüme yerleştiriliyor. Kritik önemdeki uygulamaları, bir uç noktada daha önce yerleşmiş olan zararlı yazılımlardan ayıran ve onları koruyan COMODO SecureBox, şirketler için önemli olan kritik uygulama ve verilerin çalınmasını engelliyor. Bu noktada Comodo, "Gerekli önlemleri alın, hacker saldırılarından korunun" mesajına dikkat çekiyor.