COMODO
Creating Trust Online®

Comodo uyarıyor: Fidye yazılımı salgını geliyor

COMODO, 02.05.2016 - Siber güvenlikte dünya devi Comodo, internette salgına dönüşme olasılığı yüksek fidye yazılımlarına karşı atağa geçti. Comodo Başkan Yardımcısı Phillip Hallam-Baker, fidye yazılımlarının yaygınlaşmasında bitcoin ve taklitlerinin etkin olduğuna dikkat çekerken, "Bunlar kapanmadıkça salgın devam edecektir" mesajı verdi.

Comodo'da bilim baş danışmanlığı da yapan Baker, "Fidye yazılımları her yerde" başlıklı bir makale kaleme aldı. Makalesinde fidye yazılımlarının arkasındaki bilimsel mantığı mercek altına alan Baker, fidye yazılımlarının neredeyse tüm hackerların kazanç sağlayabileceği bir çalışma modeli olduğunu belirtti. Baker, herhangi bir şirketin bilgisayar sistemine kötü amaçlı bir yazılım gönderen fidyeci hackerın parayı bitcoin yoluyla almayı beklemesinin günümüz dünyasında çok doğal olduğunu anlatırken, işin bu aşamadan sonra çok daha çetrefilli bir duruma dönüştüğünü şöyle anlattı:

"İşte bu yüzden fidye yazılımları her boyuttaki şirketlerin karşı karşıya kaldığı bir numaralı BT güvenlik tehdidi konumundadır. Aslında para bir gerekçe değil, bu sistemi mümkün kılan unsurun ta kendisidir. Suçlarının para kazandırdığı siber suçlular yeni saldırılara karşı önlemleri yenmeye ve yeni hedefler geliştirmeye yatırım yapabilmektedirler."
Baker'ın makalesinde Amerikan Federal Araştırma Bürosu'nun (FBI) fidye yazılımlarıyla ilgili çarpıcı belirlemeleri de dikkat çekti. FBI'a göre ABD şirketleri geçen yıl içerisinde 25 milyon dolar fidye ödedi. 2016 sonunda bu rakamın 200 milyon dolardan fazla olmasını bekleyen FBI, fidye yazılımlarıyla başetmek için herkese 'internette güvenliğe dikkat' çağrısı yapıyor.

Jigsaw'a dikkat
Son dönemde internette büyük tehlike yaratan fidye yazılımlarının başında Jigsaw geliyor.
Jigsaw adındaki fidye yazılımı bir bilgisayardaki tüm dosyaları şifreleyerek, fidye ödenene kadar şirketleri köşeye sıkıştırıyor. Yazılım; fidye ödenene kadar saat başı birer birer değil, biner biner dosyaları silebiliyor. Şirketler, hackerlara yenilip ödeme yapana kadar bir hastanenin, bir bankanın ya da herhangi bir şirketin tüm kritik dosyaları ortadan kaybolabiliyor.

Comodo Antivirüs Laboratuvarları ekibi Jigsaw zararlısının sisteme girdikten sonra dosyaları şifrelemeye başladığını ve sonrasında da 24 saat içinde 150 dolar değerinde ödeme istendiğine dair bir fidye notu göndermeye başladığına dikkat çekiyor. Öyle ki bu fidye notunda ödeme yapılmayan her saat için bazı dosyaların tamamen silineceğine dair de bir tehdit notu yer alıyor. Bu tür tehditler ifade eden bir fidye zararlısının ilk kez görüldüğünü belirten Comodo ekibi; Jigsaw'la ilgili şu uyarıyı yapıyor:

"JIGSAW; uç nokta koruması, güvenli web gateway ve sızıntı tespiti teknolojilerini tek bir çatı altında toplayan güçlü, güvenilir, katmanlı güvenlik koruması bulunmayan BT altyapıları için yıkıma yol açabilir. Kötü amaçlı yazılımlara karşı şirketinizin çözümü yeni ortaya çıkan tehditlere karşı koyabilmeli; bilinen ve bilinmeyen (ve söz konusu tehditlerin kaynağı olan) dosyaları tanıyabilmeli; bilinmeyen dosyaları baştan güvenilmez olarak sınıflandırarak güvenli olduğu belirlenene kadar, tehdit önleme alanında tutabilmelidir. Bu adımların izlenmesi ile şirketlerdeki işleyiş durdurulmaksızın; şirketler gittikçe yayılan fidye yazılım saldırılarına karşı korunmuş olur."