Comodo uyarıyor: TeslaCrypt'e dikkat

COMODO, 31 Mart 2016 – Comodo; internet ortamındaki zararlı yazılımlar konusundaki uyarılarını sürdürüyor. Comodo ekibi; TeslaCrypt fidye yazılımının yeniden ortaya çıkarak internet kullanıcılarını tehdit ettiğini belirledi. Bu tehdide karşı en etkin koruma yolu da Comodo ürünlerini kullanmaktan geçiyor.

Zararlı yazılımlar konusundaki araştırmalarını kesintisiz sürdüren Comodo ekibinin son tespitlerine göre; geçen yıl ortaya çıkan, kötü üne sahip olmasına karşın çabucak yaygınlaşan TeslaCrypt fidye yazılımı kendisine karşı oluşturulan güvenlik duvarını yeniden aşmaya başladı. Öyle ki; TeslaCrypt geliştiricileri kendi hatalarını düzeltti ve zayıf yönlerini kapattı, böylelikle TeslaCrypt fidye yazılımını yenilemiş oldular. (3.01) Comodo ekibi de, ilk sürümlerine göre daha fazla bilgi sızdırılmasına olanak tanıyan ve ele geçirdiği her bir bilgisayarı TeslaCrypt botnet noktasına çeviren bu yeni sürümün daha tehlikeli olduğuna dikkat çekiyor. Comodo'nun tespitlerine göre bu sürümle sözkonusu olan tehlike şöyle:

"RSA 4096 şifrelemesi ve yeni sürümde özel anahtarın (dosyalarınıza erişmek için kullanmanız gereken kod), söz konusu makinelerden alınarak host sunucuya taşınması ile bu sürümü kırmak, basitçe, imkânsız."

Comodo'nun avantajı da tam bu noktada devreye giriyor. Comodo'nun Default Deny Platformu ile tüm kötü amaçlı yazılım türleri engellenerek ve bilinmeyen dosyalara (kötü amaçlı yazılım olma ihtimali söz konusu olan) ilişkin tehditler otomatik olarak önlenerek, TeslaCrypt ve Cryptolocker gibi tüm fidye yazılımlarının önüne geçiliyor.Yani, sözkonusu kötü amaçlı yazılım oldukça tehlikeli olsa bile, Comodo'nun sağladığı korumayla, bu durum bir sorun olmaktan çıkıyor. Comodo tehdit önleme sisteminin özelliği; sistemin tüm bilinmeyen dosyaları (iyi veya kötü) tehdit önleme alanı içinde çalıştırması. Bu sırada bulut tabanlı karar hizmeti olan Valkyrie ile dosyalara ilişkin karar so derece hızlı şekilde alınabiliyor. Dosyanın iyi amaçlı olduğuna karar verildiğinde, dosya tehdit önleme alanından çıkarılıyor. Dosyanın kötü amaçlı olduğuna karar verildiğinde ise; zararlı yazılımın "işe yaraması" için erişmesi gereken kaynaklara ve altyapıya erişimi engelleniyor ve sisteminiz korunmuş oluyor.

Comodo'nun farkı

Comodo Kurumsal Ürünler Başkan Yardımcısı John Peterson, zararlı yazılımlara karşı geleneksel çözümler ile Comodo'nun çözümleri arasındaki farkı şöyle anlattı:

"Uç noktalarda kötü amaçlı yazılımların izole edilmesine yönelik geleneksel çözümler default-allow ve sanallaştırma, ya da sandbox teknolojisini kullanmaktadır; bu ise ilk

makinenin ele geçirilmesine olanak tanımaktadır. Comodo'nun yaklaşımı ise bundan tamamen farklıdır; Comodo, patent bekleyen tehdit önleme teknolojisini kötü amaçlı yazılım sorununa uygulayarak iyi, kötü veya bilinmeyen tüm çalıştırılabilir dosyaların güvenli bir alanda çalıştırılmasına olanak sağlar. Comodo daha sonra her bir çalıştırılabilir dosyayı analiz ederek ya geçişine izin verir (iyi dosya), ya da siler (kötü dosya); böylece performans etkilenmez ve daha da önemlisi, uç nokta ve ağ her daim korunur ve güvenli kalır."

Comodo korunmasından yararlanmanız için yapmanız gereken ise şöyle:

- Kötü amaçlı yazılımların farklı türlerine ilişkin ayrıntılı bilgi almak için, Comodo'nun kötü amaçlı yazılım arama motorunu ziyaret edin: https://file-intelligence.comodo.com/

- Şirketinizin BT ortamını phishing, kötü amaçlı yazılım, casus yazılım saldırıları veya siber saldırılardan korumak için, Comodo güvenlik uzmanları ile irtibat kurun: https://tr.comodo.com/contact/

TeslaCrypt ne yapmıştı?

TeslaCrypt fidye yazılımı geçen yıl oraya çıktığında; internetde salgın bir hastalık gibi yayılarak; bilgisayarlara bulaşıp dosyaları kilitleyerek fidye talebinde bulunarak büyük hasara yol açmıştı. Daha sonra, endüstri bu duruma, ters mühendislik yoluyla zekice üretilmiş, virüse maruz kalan kullanıcıların kilitli dosyalara yeniden erişebilmek için ödeme yapmaktan kaçınmalarını sağlayan çözümler ile yanıt vermişti.