COMODO
Creating Trust Online®

Hackerler Amazon müşterilerine de saldırıyor

COMODO 15.06.2016 – İnternet ortamındaki zararlı yazılımlara karşı güçlü bir mücadele yürüten Comodo, fidye yazılımlarla ilgili çalışmalarını derinleştirdi. Comodo uzmanları; fidye yazılımcılarının ünlü alışveriş sitesi Amazon uzantılı elektronik mesajlarla da hırsızlık yaptığını belirledi.

Comodo Tehdit Araştırmaları Laboratuvarları (CTRL) internet ortamındaki herkesin amazon.com uzantılı elektronik mesajlara dikkat etmesi gerektiğini duyurdu. Öyle ki; e-mail hesaplarında Amazon.com'dan gelmiş gibi gösterilen sahte bir e-mail'le hırsızlık yapılıyor. Bu siber hırsızlık e-mail'leri, kullanıcılara Amazon.com çıkışlı gibi gösterilen auto-shipping@amazon.com adresiyle gönderiliyor. Bu e-mailin gövde bölümünün olmadığı bildirilse de, e-mailin konusu "Amazon.com siparişiniz yola çıktı (#kod)" şeklinde belirtiliyor. Virüslü mesajlar ise mailde Microsoft Word dosyaları biçiminde gönderilmiş olan ekleri kapsıyor.

Comodo uzmanları, bu dosyaları analiz ettiğinde kopyaların yerine yalnızca makro kodların olduğunu belirledi. Bu dosyaların içeriğini çalıştırmaları yönünde yönlendirilen ve şüphelenmeyen alıcılar ise bu yolu izlediğinde, makro kodları çalıştırılıyor. Böylece çalıştırılabilir bir dosyanın internetten indirilerek çalıştırılması sağlanıyor. Çalışan bu dosyanın dokümanlar, resimler, ses dosyaları, veri tabanı dosyaları gibi kullanıcı dosyalarını tarayıp şifreleyen bir Ransomware fidye yazılımı olduğu tespit edildi. Bu süreç sırasında orijinal dosyalar silinerek bulundukları klasörde **"%hashvariable%locky"** adıyla şifrelenmiş dosyalarla değiştiriliyor.

Peki; siber suçlular bundan nasıl kazanç sağlıyor? Fidye yazılımının yüklenmesi sonucunda, kullanıcıların verileri rehin tutuluyor. Şifrelenen dosyalarla, kullanıcıların orijinal dosyaları geri almak için fidye ödemeleri gerektiğine dair uyarılar ve yönergeler bulunan bmp dosyaları oluşturuluyor. Kullanıcılara fidyeyi nasıl ödeyebilecekleri anlatılırken, bu uyarılar ve yönergeler masaüstü arka planı olarak ayarlanıyor. Ayrıca, aynı uyarıları ve yönergeleri içeren bir html dosyası da şifrelenmiş dosyalar barındıran tüm klasörlere yerleştiriliyor. Bu son saldırı yalnızca güvenlik önlemlerinin güçlendirilmesi için çağrıyı güçlendiriyor. Siber suçlular kendilerini engelleme çabalarına uyum sağlarken yeni ve daha sinsi kötü amaçlı yazılım türleri yaratmaya devam ediyorlar. Comodo'nun, gelişmiş sürekli tehditlerle başa çıkacak çözümlerinin olduğu unutulmalı. Comodo, küçük veya büyük tüm şirketler için özel tasarlanan birçok çözüm sunuyor.