COMODO
Creating Trust Online®

Comodo: Microsoft Windows güncellemelerine dikkat

COMODO, 20.09.2016 – İnternetteki zararlı yazılımlarla mücadelesini sürdüren Comodo, Microsoft Windows güncellemesi kılığında yeni bir fidye yazılımı konusunda uyarıyor. Fantom isimli yazılım; Microsoft Windows güncellemesi kılığına girerek kullanıcıların yazılımı indirmesini sağlıyor ve veri güvenliğini ihlal ediyor.

Fantom zararlı yazılımını araştırmacı Jakub Kraustek keşfetti. Bildiğimiz gibi hackerların sistemleri bloke etmesini ve kullanıcıların dosyalarını şifrelemesini, böylece dosyaların açılamamasını veya kullanılamamasını sağlayan zararlı yazılımlara fidye yazılımı deniyor. Fidye yazılımları aynı zamanda uygulamaların çalışmasını engelliyor. Böylece bundan etkilenen kişiler, sistemlerini tekrar çalıştırmak veya dosya ve uygulamaları açmak-kullanmak için hackerlara fidye ödemek zorunda kalıyorlar. Son günlerde fidye yazılımı saldırılarının sayısı da gittikçe artıyor; son aylarda **fidye yazılımı** saldırılarına maruz kalan birçok kurum var.

Fantom Nasıl İşler…

Fantom, açık kaynak fidye yazılımı projesi EDA2'ye dayanarak geliştirilmiş bir fidye yazılımı ve sahte bir Windows Güncellemesi Ekranı göstererek ortaya çıkıyor. Bu güncelleme ekranı size Windows'un yeni ve kritik bir güncelleme kurduğunu düşündürüyor. Fidye yazılımının dosya özelliklerinde bile bunun Microsoft'tan geldiği belirtiliyor ve dosya tanımlaması olarak 'Kritik Güncelleme' ibaresi yer alıyor.

Bunun gerçekten bir Windows güncellemesi olduğuna inandırıldığınız için, olasılıkla çalıştırıyorsunuz. Fidye yazılımı böylece WindowsUpdate.exe isimli bir başka gömülü programı çıkarıyor ve çalıştırıyor, sonra da sahte bir Windows Güncellemesi ekranı beliriyor. Bu ekran, tüm aktif pencerelerin üzerini kaplıyor ve açık olan herhangi bir uygulamaya geçemiyorsunuz. Bu güncelleme ekranında görünen yüzde, size Windows güncellemesinin devam ettiğini düşündürüyor ama aslında yüzde arttıkça dosyalarınız şifreleniyor. İsterseniz Ctrl+F4 tuş kombinasyonuyla bu ekranı kapatabiliyorsunuz ama dosyalar arka planda şifrelenmeye devam ediyor.

Diğer EDA-2 temelli fidye yazılımları gibi Fantom da rastgele bir AES-128 anahtarı oluşturuyor ve bunu RSA kullanarak şifreliyor. Sonra bu, zararlı yazılımcıların Kumanda ve Kontrol sunucusuna yükleniyor. Bu dosyalar AES-128 şifreleme protokolü kullanılarak şifrelenip şifrelenen her dosyaya .fantom uzantısı ekleniyor. Fantom'un şifrelediği dosyaların bulunduğu klasörlerde ayrıca DECRYPT_YOUR_FILES.HTML isminde bir fidye notu oluşturuluyor. Şifreleme tamamlandığında Fantom iki ortak iş dosyası açıp çalıştırıyor ve bu dosyalar, gölge kopyalarını ve daha önce gelmiş olan sahte güncelleme ekranını siliyor.

COMODO
Creating Trust Online®

Ve sonunda DECRYPT_YOUR_FILES.HTML ismindeki fidye notu geliyor. Burada verilerinizi kurtarmak için onlardan parola satın almanız gerektiği söyleniyor. Ödeme talimatları için fantomd12@yandex.ru veya fantom12@techemail.com adresine e-posta göndermeniz isteniyor. Aynı zamanda dosyalarınızı kurtarmaya çalışmamanız, aksi takdirde verilerinizi tamamen yok edebileceğiniz konusunda uyarılıyorsunuz.

Hackerlar fidye yazılımları ile saldırıda bulunurken birçok farklı yöntem kullanıyor ama Fantom'da kullanılan strateji, akıllıca. Saldırganlar, kurumsal kullanıcılar da dahil olmak üzere birçok kullanıcının tanıdığı ve hatta güvendiği bir ekranı taklit ediyorlar; insanları gerçek bir Windows güncellemesi yaptıklarına inandırmak ve bu şekilde Fantom'u indirmelerini sağlamak nispeten kolay. Bu, genel anlamda zararlı yazılımlar ve özellikle de fidye yazılımları açısından tehlikeli bir trende işaret ediyor olabilir.