Comodo'dan "Sauron" uyarısı

"Devletlerin bilgisayarlarına karşı 5 yıldır casusluk yapıyor"

COMODO, 06.09.2016 – İnternetteki zararlı yazılımlarla mücadelesini sürdüren Comodo, devletlerin bilgisayarlarına karşı 5 yıldır casusluk yapan Sauron Projesi'nin yarattığı tehdide dikkat çekti. Diğer zararlı yazılımların aksine arkasında iz bırakmayan, farklı kimliklere bürünmeyi başaran bu yazılım, araştırmacıları şaşırtmayı da sürdürüyor. Öyle ki araştırmacılar, bu yazılımın arkasında bir devletin desteklediği bir grubun olma ihtimalini de değerlendiriyor.

Sauron Projesi; beş yıldan uzun bir süredir devlet bilgisayarlarını ve büyük kuruluşlara ait bilgisayarları izleyen zararlı yazılımın ismi. Bu yazılımı tespit eden araştırmacılar, yazılımın kaynak kodunda Tolkien'in yazdığı "Yüzüklerin Efendisi" kitabının baş anti-kahramanı Sauron'a yapılan göndermeden dolayı yazılıma Sauron Projesi adını verdiler.

Sauron Projesi'nin, ilk kez, geçen Eylül ayında ismi açıklanmayan bir devletin bilgisayar ağında, ağa bağlı olan cihazlardan birindeki zararlı aktivitelerin araştırıldığı sırada tespit edildiği belirtiliyor. Daha sonra yapılan araştırmalar, bu zararlı yazılımın birçok başka ağda da mevcut olduğunu gösterdi. Sauron Projesi en az 30 kurumun ağlarında tespit edildi. Bu kurumlar arasında askeri, finansal ve haberleşme kurumları gibi stratejik kurumlar da bulunuyor. Sauron Prıojesi'nin Çin'de bir havayolu şirketinde, Belçika'daki bir büyükelçilikte ve İsveç'te ismi belirlenemeyen bir kurumda tespit edildiği söyleniyor.

Araştırmacılar Sauron Projesi üzerinde çalışırken, bir Windows parola filtresi olduğunu iddia eden tuhaf bir çalıştırılabilir dosyanın varlığını tespit ettiler. Şöyle ki; bir kullanıcı giriş yapmak istediğinde veya bir parola girdiğinde, exe dosyası çalışmaya başlıyor. Zararlı yazılım; parola, şifreleme anahtarı, yapılandırma dosyaları ve log depolarını çalmak için kullanılabiliyor ve daha sonra tüm bunlar doğrudan korsanların eline geçiyor. Sauron Projesi; bir sonraki adım olarak; klavye dinleme yöntemiyle, bilgisayar korsanlarının bir sistem veya ağı ele geçirmelerini sağlayacak bir arka kapı yaratıyor.

Araştırmacıları şaşırtıyor

Sauron Projesi tespit edilmesi neredeyse imkansız bir zararlı yazılım olmanın yanısıra diğer bilindik zararlı yazılımlardan farklı olarak değişik ağlarda farklı görünümler sergiliyor. Bu zararlı yazılım; diğer zararlı yazılımların aksine arkasında iz de bırakmıyor. Bu yüzden de zararlı yazılımın etkilediği diğer alanları tespit etmek de çok güçleşiyor.

Sauron Projesi'nin yaratıcıları, zararlı yazılımdan etkilenen iki alanın birbirine benzememesini ve aynı yazılım yapaylıklarını ortaya çıkarmamasını da sağladılar. Ayrıca bu yazılım, farklı kimliklere de bürünmeyi başarıyor. Örneğin; Microsoft tarafından çıkarılan dosyaların adlarına benzer dosya adları taşıyabiliyor. Bilgisayar korsanına verileri gönderme yöntemi de

her zaman aynı olmuyor. Bu da; sürekli örüntüler bulmaya çalışan araştırmacıları şaşkınlığa düşürüyor.

Güvenlik duvarlarını aşıyor

Sauron Projesi çok karmaşık bir yapı sergileyen bir zararlı yazılım olmasının yanısıra en kapsamlı güvenlik duvarlarından bazılarını da aşabiliyor. Bu zararlı yazılım; hava boşluğuyla korunan (air-gapped) ve internete bağlı olmayan, bu yüzden de alışagelmiş zararlı yazılımların erişimine kapalı olan sistemleri de etkileyebiliyor. Sauron Projesi, burada ise normal veri depolama araçları gibi görünen fakat birkaç yüz Mbs'lik gizli bir bölme içeren, özel olarak hazırlanmış USB belleklerle sistemlere sızıyor. Bu belleklerde depolanan bir sanal dosya sistemiyle air-gap korumasına sahip sistemlerden veri aktarımı mümkün hale getiriliyor. Araştırmacılar, bu çok karmaşık saldırının bazı bilinmeyen ve henüz keşfedilmemiş sıfırıncı-gün güvenlik açıklarının kullanılması yoluyla gerçekleştirildiğini düşünüyor. Fakat, bu sıfırıncı gün güvenlik açığı boyutu henüz bir spekülasyondan ibaret ve teyit edilmiş değil.

Sauron Projesi çok karmaşık bir zararlı yazılım ve halen bu zararlı yazılımın analiz süreci devam ediyor. Araştırmacılar; bir devletin desteklediği bir grubun bu zararlı yazılımın arkasında olabileceği ihtimalini de değerlendiriyor.