Giriş Tarihi: 7.10.2016 18:24 Son Güncelleme: 7.10.2016 18:29

ByLock'un kripto sistemleri çözülüyor

AA

Bilişim Uzmanı Füsun Nebil, Fetullahçı Terör Örgütü (FETÖ) mensuplarının kriptolu iletişim sağladığı iddia edilen ByLock programı ile ilgili, "215 bin kişinin kullandığı tespit edilen anlık mesajlaşma sistemi ByLock, tahminlerimize göre sanal mağazadan indirilmiyor. Kriptolu yazışılıyor. Mesajı gönderen ve alan anahtar giriyor ve bu anahtarlar tutuyorsa iletişim başlıyor." dedi.

Nebil, AA muhabirine yaptığı açıklamada, ByLock ile ilgili bilgisinin yalnızca basından okudukları kadar olduğunu ancak bilişim teknolojilerini bildiği için konuya ilişkin çeşitli değerlendirmeler yapabileceğini söyledi.

Bir uygulama sistemi üzerinde bulunan kriptolu mesajlaşma programı Bylock ile Kasım 2014'ten bu yana 18 milyonun üzerinde mesajın yayınlandığının daha önce kamuoyuna açıklandığını anımsatan Nebil, yine basına yansıyan rakamlara göre bu sistemi kullanan 215 bin dolayında hesabın bulunduğunu aktardı.

Nebil, "215 bin kişinin kullandığı tespit edilen anlık mesajlaşma sistemi ByLock, tahminlerimize göre sanal mağazadan indirilmiyor. Kriptolu yazışılıyor. Mesajı gönderen ve alan anahtar giriyor ve bu

anahtarlar tutuyorsa iletişim başlıyor." dedi.

Bir mesajlaşma uygulaması geliştirildiğinde öncelikle bunun reklamının yapılacağına işaret eden Nebil, "15 Temmuz öncesine baktığımız zaman, ne yabancı basında ne de Türkiye'de ByLock'un ne olduğu konusunda en ufak bir reklam, haber, bilgi yok. Biz bilişim uzmanları da bu olaylara kadar öyle bir mesajlaşma sistemini duymamıştık. Bu da bu mesajlaşma sisteminin özel bir amacı olduğunu gösteriyor." diye konuştu.

- "GİZLİ BİR UYGULAMA GÖRÜNTÜSÜ VERİYOR"

Kullanıcılarının ne şekilde haberleştiğini ancak tahminler üzerinden anlatabileceğinin altını çizen Nebil, şöyle konuştu:

"İstihbarat yetkililerinin, 17-25 Aralık sürecinde bu yapılanmanın ByLock üzerinden haberleştiğini tespit ettiğine dair haberler var. O dönemde yazılımın işletildiği sunuculara sızılmış ve hem hesaplar hem de mesajlar bu sunucudan indirilmiş. Şu anda yapılan tespitler, bu bilgilerin çözümlenmesi ile ilgili gözüküyor.

Ben ByLock'ta sistemin teke tek görüşmeler şeklinde olduğunu ve kullanıcıların birbirini bir rehber üzerinde görmediklerini ancak davet usulu ile iletişime geçtiklerini tahmin ediyorum. Görselerdi birbirlerine 'key' yani anahtar vermek zorunda kalmazlardı. Yani ancak birbirinin anahtarlarını bilen insanların kullanacağı gizli bir uygulama görüntüsü veriyor."

Nebil, "İnternet üzerinde kimin ne yaptığını ancak IP adresi ile bulabilirsiniz. Burada da indirilen bilgilerde, hesapların hangi IP adresi üzerinden bağlandığı tespit ediliyor. Bu IP adresinin hangi operatör tarafından, hangi kullanıcıya verildiği de biliniyor. Böylece o IP'den hareketle ilgili kişi tespit edilmiş oluyor". bilgilerini paylaştı.

Mobil telefonlar üzerinden yapılan haberleşmelerde bu tespitin son derece kolay olduğunu belirten Nebil, şöyle devam etti:

"Eğer wi-fi üzerinden ByLock kullanımı bir kurumdan (yani otel, kafe ya da şirket) ise 2007 yılında yürürlüğe giren 5651 sayılı İnternet Kanunu nedeniyle buralarda kullanım yapanlar kayıt altında. Loglar tutuluyor. Dolayısıyla da ilgili kişinin bulunma olasılığı yüksek. Eğer loglar tutulmuyorsa, zaten

ilgili kurum ve yetkili kişi bundan sorumlu tutulur.

Ama bu bir ev ise ve 2-3 komşu kendi aralarında wi-fi paylaşımı yapıyorlarsa, bu durumda hangi komşunun kullandığı anlaşılamaz. Böyle 1-2 olay da biliniyor. Dolayısıyla bugün ByLock için bahsedilen listelerden turuncu olanlar bu bölüme giriyor. Wi-fi paylaşımı, hele bilmediğiniz insanlarla paylaşım her halükarda tehlikeli. Diğer insanların ne yaptığını bilmiyorsanız, bu çocuk pornosu olabilir, banka dolandırıcılığı bile olabilir ya da burada olduğu gibi ByLock gibi bir konu gündeme gelebilir."

ByLock'un bir süredir FETÖ mensubu olmaya dair en önemli kanıt sayıldığına işaret eden Nebil, "Sunucusunun Litvanya'da bulunduğu söyleniyor. ByLock ile ilgili basında 15 Temmuz öncesinde bilgi yok." dedi.

Nebil, ByLock yazılımı yüklemelerinin bir kısmının bluetooth üzerinden olduğunun tahmin edildiğini belirtti.

- "BYLOCK KULLANAN HERKESİN İZİNE ULAŞMAK MÜMKÜN"

Türki·ye Bi·li·şi·m Derneği· Yöneti·m Kurulu Başkanı İlker Tabak da ByLock'un, Türkiye'de kullanımı yaygın olan WhatsApp, Viber gibi bir haberleşme ve mesajlaşma programı olduğunu söyledi.

Kullanıcıların cep telefonlarına kolay bir şekilde ByLock programını yükleyebildiklerini belirten Tabak, yüklemek için kişinin, "programın nereden yükleneceği" bilgisine sahip olması gerektiğini aktardı.

Programın bir web sitesi üzerinden indirilebilecek şekilde planlanmış olabileceğini ifade eden Tabak, FETÖ'nün haberleşme ağı olarak bilinen ByLock gibi herhangi başka bir programın da şu anda kullanılabiliyor olabileceğini ifade etti.

Cep telefonuna indirilen ve kullanılan uygulamaların tespitinin yapılabildiğini dile getiren Tabak, "Programı kim indirdi, hangi numaralı telefon bunu indirdi diye bu yazılımın, programın kaynağındaki sunucu bilgisayarlarda bir arşiv tutuluyordur. Ayrıca indirilen telefona erişilirse orada yapılacak bir incelemede 'hangi uygulamaların yüklendiği, yüklendikten sonra ne kadar süreyle çalıştırıldığı, ne zaman bilgisayardan ya da telefondan kaldırıldığı' gibi birtakım bilgiler de o cihazların içinde bulunabilir. Derin incelemelerle ByLock kullanan herkesi·n i·zi·ne ulaşmak mümkün." şeklinde konuştu.

Tabak, bu tür programların iletişim kanallarında kullandığı birtakım kapılar ve şifreler olduğunu belirterek, "Dolayısıyla uygulamada özel bir şifre kullanıldı mı, kullanılmadı mı diye bakılarak bir analiz yapılıp, sonuca ulaşılabilir." dedi.

Cep telefonlarının seri numaralarından da ByLock kullanıcılarının tespitinin mümkün olabileceğine dikkat çeken Tabak, şöyle devam etti:

"Bir bilgi bir yerde paylaşıldığında veya iz bıraktığında buna erişmek mümkün. Yapılan görüşmeler silinse bile, diyelim ki silindi, bunlar sonuçta birtakım sunucuların belleklerinde, disklerinde saklanan bilgiler ve her ihtimale karşı yedeği alınıyor. Bizler de gerektiğinde yedekleme yapıyoruz. Aldığınız yedekleri temizlemezseniz, oradan bile bu geçmişe dönük bilgilere ulaşılabilir. Ayrıca derin analizlerle, çalışmalarla 'Bu disklerde daha önce neler vardı, neler yoktu' bilgisi çıkabilir."

Vatandaşlara da güvenlik uyarısında bulunan Tabak, "Vatandaşlarımız birçok uygulamayı indirdiği zaman, verisinin, bilgisinin paylaşılmasını da kabul ediyor. Programlar indirilirken 'İzin ver' diye bir buton var. Bunların çoğu okunmadan kabul ediliyor. Öyle olunca bunlar çeşitli dolandırıcılık yöntemlerine de alet olabiliyor. Burada toplanan veriler bir şekilde başkalarının eline geçebiliyor. Olabildiğince lisanslı ürün kullanmak gerekli." ifadelerini kullandı.

- FETÖ MENSUPLARININ DEŞİFRE EDİLMESİNDE REFERANS OLDU

FETÖ'nün 15 Temmuz'daki darbe girişiminin ardından başlatılan soruşturmalar sırasında, bir şüphelinin cep telefonunda bulunan ByLock programının, soruşturmanın derinleştirilmesiyle FETÖ mensupları tarafından haberleşmede kulanılan kripto bir yazılım olduğu ortaya çıkmıştı.

2014 aralık ayından önce bir oyun programının mesajlaşma ara yüzü olarak kullanılan uygulamanın, bu tarihten sonra FETÖ'nün Ar-Ge bölümü tarafından güvenlik katmanları eklenerek Türkçeleştirildiği ve örgüt içi haberleşmede kullanılmaya başlandığı belirlenmişti. Milli İstihbarat Teşkilatı (MİT) uzmanları tarafından şifreleri kırılan ByLock uygulaması, FETÖ'nün darbe girişimine

ilişkin soruşturmada, örgüt mensuplarının deşifre edilmesinde en önemli referanslardan biri oldu.