Giriş Tarihi: 17.12.2017

FETÖ'nün kripto ağı bir bir çözülüyor

Erkam ÇOBAN

İhanet şebekesinin ByLock'tan sonra "Turquoise" adlı ağ üzerinde haberleştiği saptandı. "ByLock" serverındaki IP'lerde yapılan haberleşme programının şifreleri özel ekiplerce çözülüyor

FETÖ soruşturmalarında en önemli delil olan örgütün kriptolu haberleşme programı ByLock ile ilgili istihbarat birimlerinin hazırladığı rapora SABAH ulaştı. Raporda, FETÖ'nün 2015 yılından itibaren ByLock'un bağlı olduğu serverdaki aynı IP adresleri üzerinden işlem sağlayan Turquoise isimli haberleşme programına geçtiği tespit edildi. İstihbarat birimlerinin bu programın şifrelerini çözmek için üzerinde çalıştığı öğrenildi. FETÖ üyeliği için tek başına delil olan, örgüt üyelerine talimatların aktarıldığı ve FETÖ'nün tüm hassas ağlarını gün yüzüne çıkaran şifreli haberleşme programı ByLock, ile ilgili istihbarat birimlerinin hazırladığı raporda şunlara yer verildi:

PARMAK İZLİ GÜVENLİK ÖZELLİĞİ: Örgüt mensuplarının önemli gördüğü mesajları ekstra güvenlik önlemi olarak sisteme eklenen cihaz kullanıcısının parmak izinin

kullanılmasına da olanak sağlamaktadır. Programı cihazlarına indirenlerin, programı kullanmaya başlamadan önce bir defaya mahsus kullanıcı hesabı oluşturmaları gerekmektedir. Bütün kullanıcı adları birbirinden farklıdır. Bir kişinin aldığı kullanıcı adının uygulama başkasına vermez. Kullanıcı adı ve şifresinden oluşan kullanıcı hesabı internet üzerinden cihazın donanım kimliğiyle birlikte Bylock sunucusuna kaydedilir.

VERİLER İŞTE BÖYLE ŞİFRELENDİ: ByLock'da diğer mesajlaşma uygulamalarındaki gibi rehber senkronizasyonu yapılmaz ve rehber uygulamaya kopyalanmaz. Kullanıcı iletişim kurmak istediği kişiyi, o kişinin kullanıcı adıyla ve karşılıklı bilinen şifreler ile uygulamanın rehberine kendisi ekler. ByLock'ta veri alışverişinde gönderilecek mesaj veya ses öncelikle sunucu tarafından verilen bir anahtar yardımıyla şifrelenir.

İSTİHBARAT ÖĞRENİNCE VPN'YE GEÇİLDİ: İstihbarat birimlerinin bu programı öğrendiğini fark eden FETÖ, 17 Kasım 2014'te Türkiye'den gelen IP'lere engelleme getirilerek Türkiye'den bağlanan kullanıcılar ByLock'a VPN ile bağlanmaya zorlandı. ByLock'un 24 Aralık 2014 tarihli 1.1.7 sürümünün; renkleri, uygulama simgesi, buton ve menü görünümlerinin değiştirilmesi suretiyle 2015 yılında "Turquoise" programını kullanıma soktu. Turquoise, ByLock gibi Google Play Store ile Apple Store üzerinden yayınlanmadı.

AYNI ÇEKİRDEK YAZILIM

Turquoise, örgüt üyelerinin cihazlarına "Uygulama Paylaş" isimli özel bir uygulama üzerinden gönderildi veya Bluetoooth, Flash Bellek gibi araçlarla birebir yüklendi. ByLock gibi örgütün geniş tabanına yaygınlaştırılmayan program, örgütün önemli gördüğü kişilere ByLock'u sildirerek Turquoise yüklemelerini sağladı.

AYNI KULLANICI ADI KULLANILMIYOR: ByLock'un çekirdek yazılımı değiştirilmeden Turquoise'da kullanıldı. Turquoise da, ByLock gibi Litvanya'da bulunan aynı IP adreslerini kullandı. ByLock ve Turquise'ın kaynak dosyaları da birebir aynıdır. Ayrıca ByLock'tan alınan bir kullanıcı adının Turquoise'dan alınmaya çalışılması durumunda alınmaya çalışılan kullanıcının var olduğu uyarısını veriyor.