Giriş Tarihi: 4.8.2016 09:37

Kripto çözüldü 150 bin FETÖ'cü kıskaçta

MİT, FETÖ'cülerin kullandığı Eagle ve ByLock isimli mesajlaşma uygulamasının şifresini kırdı. 100 milyondan fazla kriptolu mesajı çözdü. Uygulamaları kullanan 150 bin FETÖ'cüden 56 bininin kimliğini tespit etti

FETÖ'nün hain darbe girişimi öncesi ve sonrası kullandığı Eagle ve ByLock isimli uygulamalardaki hayalet mesajlarda yer alan darbe yazışmalarını Milli İstihbarat Teşkilatı (MİT) kriptosunu çözerek deşifre etti. SABAH Özel İstihbarat Bölümü'nün ulaştığı bilgilere göre kriptolu yazışmaları gerçekleştiren 56 bin FETÖ üyesinin kimliklerine ulaşıldı. Eagle ve ByLock üzerinden 150 bin kişinin yazıştığı, bu kişilerin kimliklerinin de en kısa sürede deşifre edileceği bildirildi. 15 Temmuz gecesi TBMM'yi, Özel Harekât Daire Başkanlığı'nı bombalayan, MİT'e, Genelkurmay'a helikopterle saldırı düzenleyen ve İstanbul ile Ankara'da sivil vatandaşları katleden darbecilerin nasıl ifade vermesi gerektiği anlatılan yazışmalarda yer alan "Nasıl ifade vermeliyiz" kısmında "Restleşmeden zemine göre duruş gösterilmelidir. Yerine göre dik duruş yerine göre alttan alma olabilir. Her kişi için sübjektif kriterler vardır. O esnada değerlendirilip karar verilmeli. Bu yüzden can güvenliği sorunu

yoksa mümkün olduğunca hiçbir iddiayı kabul etmemek kesin bir dille reddetmek lazım" deniliyor. Yazışmalar, FETÖ'nün darbe, terör ve iç işgal harekâtını örgüt olarak üstlenmesi anlamına geliyor.

ÜÇ KATMANLI ŞİFRELEME

MİT'in Siber Suçlarla Mücadele Başkanlığı'ndaki teknik uzmanların deşifre ettiği yazışmaların üç aşamalı olarak (kullanan şahıs, program ve server üzerinden) kriptolandığı, bir de üzerine VPN ile koruma sağlandığı tespit edildi. Uzmanlar "paranoyakça" şifrelenmiş yazışmaların içeriğinin açığa çıkarılmasının bir mucize olduğunu belirtti. FETÖ'nün gerçek hayattaki örgütlenmesi gibi yazışmalarda da hücre tipi yapılanmanın kullanıldığı ve bu sayede örgüt üyelerine ulaşılmasının engellenmeye çalışıldığı bildirildi. ByLock adlı kriptolu mesajlaşma uygulamasının şifreleri ilk olarak kış aylarında kırıldı. Uzmanlar sisteme girerken kullanılan VPN uygulamasının bilgilerini de ele geçirerek ByLock'u kullanan şahısların tespitini sağladı. Uygulamada kriptolu mesajlaşma ve mail iletişimine ait 100 milyonun üzerinde veri ele geçirildi, ele geçirilen şifreli dataların yüzde 90'nın kriptosu çözüldü ve içeriklerine ulaşıldı.

HAYALET İNSAN KONSEPTİ

ByLock uygulamasının verilerinin ele geçirildiğinin örgüt tarafından anlaşılmasının ardından Eagle adlı uygulamayı tersine mühendislik adı verilen yöntemle kullandı. Yine Eagle alt yapısı kullanılarak Line, Whatsapp ve Tango görünümlü uygulamaları üretip kullanmaya başladı. Bu uygulamaların sadece logo ve isimlerinin orijinal olduğu, Eagle'dan teknik açıdan herhangi bir farkının olmadığı, haberleşmenin yine kriptolu olarak sağlandığı tespit edildi. Eagle'da da üç katmanlı şifreleme tekniğinin kullanıldığı, uygulamada hayalet insan konseptinin oluşturulması amacıyla kullananların isim, soy isim, telefon bilgilerinin tutulmadığı, her kullanıcıya bir kod verildiği görüldü. MİT uygulamanın bir zaafı üzerinden sistem sunucularına gönderilen mesajları ve göndericilerini ele geçirdi. Ayrıca sistemin hatalı şifre girilmesi durumunda bütün verileri sildiği belirtildi. Eagle verilerinin kripto çözüm işlemleri yüzde 60 oranında tamamlandı.

FETÖ'CÜ OLDUĞUNUZU REDDEDİN

Deşifre edilen bir diğer darbe yazışmasında darbecilere "FETÖ üyesi olduğunuzu reddedin" talimatı veriliyor. Yazışmada "Diğer husus ifadede sorulan sorulara onların beklediği şekilde cevap vermek zorunda değiliz. Yani illa onların sorduğu soruya cevap vermek zorunda değiliz. Sakin olmaya çalışıp bir şeyler söyleyip gerçekte aleyhimize olan hiçbir şey söylemeyebiliriz. FETÖ'nün üyesi olduğunuz söylenirse bu üyelik reddedilmeli" deniliyor. Bir başka yazışmada ise "Darbe girişimiyle ilgili sorularda darbelere karşı demokratik bir duruş sergilenmeli. Darbeye ne direk ne de pasif destek olmadığımız belirtilmeli. Darbe ile ilgili atılan tweet, söylenen bir söz, karşı taraf kanıtlayamıyorsa reddedilmeli. Telefon programlarını yakalatmamışsak böyle bir şeyi kullanmadığımız açık bir şekilde söylenmeli" ifadeleri kullanılıyor.


SABAH