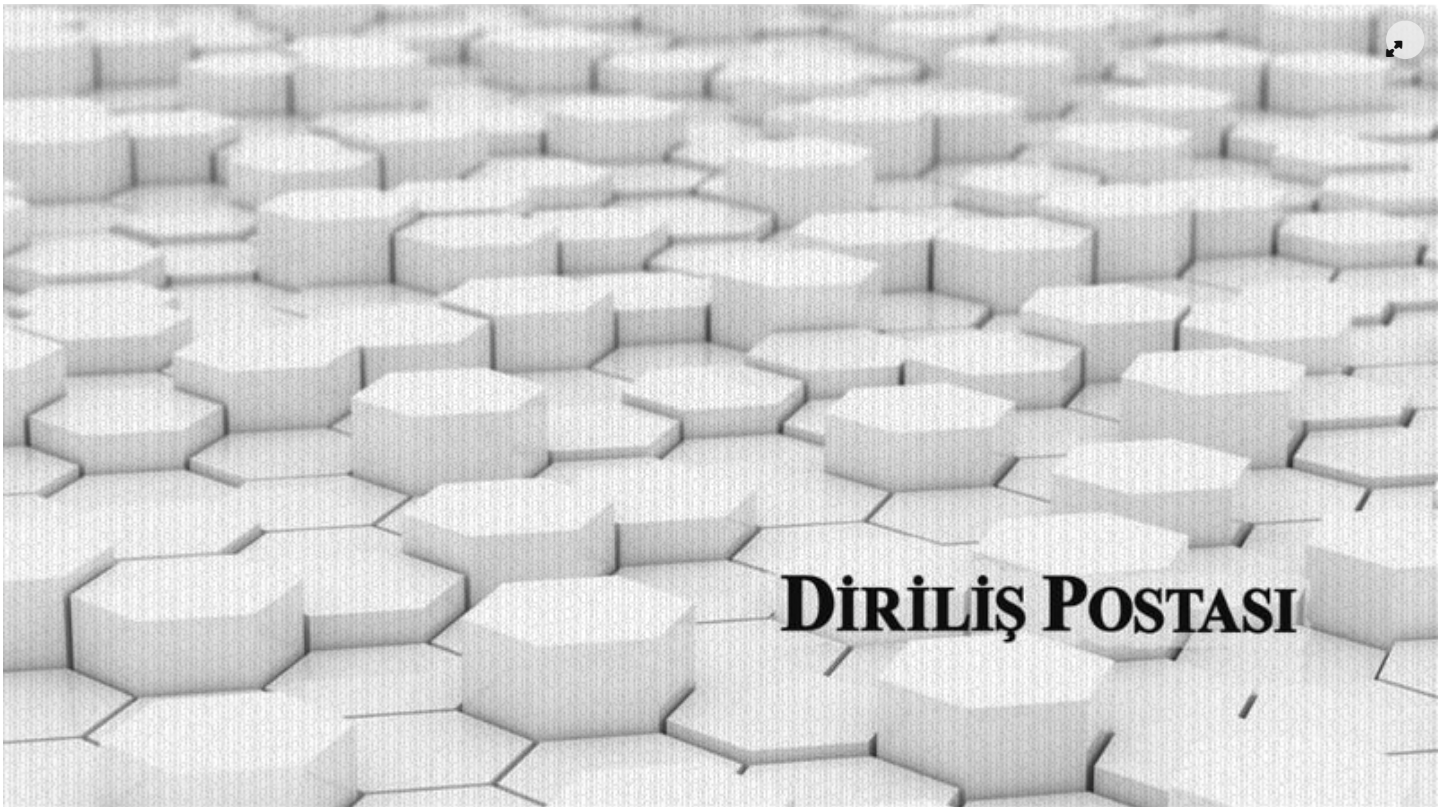
DİRİLİŞ POSTASI

Adem Büyük Polonya'da forma giyecek

21 Oca 2017 - 11:07 - Gündem G: 22 Oca 2021 - 16:15

'ByLock' programıyla ilgili kapsamlı ilk iddianame

Fetullahçı Terör Örgütünün (FETÖ) haberleşme programı "Bylock" kullandıkları tespit edilen Bankacılık Düzenleme ve Denetleme Kurulu (BDDK) çalışanı 26...



Fetullahçı Terör Örgütünün (**FETÖ**) haberleşme programı "**Bylock**" kullandıkları tespit edilen Bankacılık Düzenleme ve Denetleme Kurulu (**BDDK**) çalışanı 26 şüpheli hakkında hazırlanan iddianamede, şifreli haberleşme programı "Bylock" ile ilgili şu ana kadar yapılan çalışma ve analizlerle ilgili en kapsamlı bilgiler yer aldı. Buna göre şu ana kadar ulaşılan 215 bin 92 kullanıcıdan, parolası çözümlenebilen kullanıcı sayısının 184 bin 298 olduğu belirtildi.

İstanbul Cumhuriyet Başsavcılığınca hazırlanan iddianamede, BDDK Destek Hizmetleri Daire Başkanlığının, "FETÖ/PDY ile bağlantılı oldukları gerekçesiyle 38 kurum çalışanının açığa alındığı ve bunlardan 33'ünün ByLock programını kullandıkları" yönündeki 26 Ağustos 2016 tarihli raporun gönderildiği İstanbul Cumhuriyet Başsavcılığı Terör ve Örgütlü Suçlar Bürosunun, haklarında daha önce işlem yapılmayan 26 şüpheli hakkında "FETÖ/PDY üyesi olma" isnadıyla soruşturma başlattığı hatırlatıldı.

“Başka ülkelerde kayıtlı mobil telefon hatları kullanıyorlar”

FETÖ ile ilgili diğer iddianamelerde olduğu gibi, örgütün genel değerlendirmesi, işleyişi, hukuki nitelendirilmesi, amacı, paralel devlet kurma çabaları, hiyerarşik, zihinsel, mali, sosyal ve kültürel yapısı ile yönetim modeli, istihbarat ağı, kullandığı yöntemler ve gelir kaynaklarının başlıklar halinde anlatıldığı iddianamede, delil olarak değerlendirilen ByLock programının teknik analizi yapıldı.

Örgüt üyelerinin acil durumlarda görüşülmesi gereken bir konuyla ilgili, birinci derecede yüz yüze haberleşme yöntemini kullandığı, mecbur kalınmadıkça telefonla görüşme yapılmadığı belirtilen iddianamede, örgütün en önemli haberleşme aracının da mobil telefonlar olduğuna vurgu yapıldı.

İddianamede, terör örgütü mensuplarının kendi adlarına kayıtlı olmayan mobil telefon hatları temin edip, bunları belirli aralıklarla cihazlarıyla birlikte değiştirmelerinin bile legal olduğunu iddia ettikleri faaliyetlerinin illegal olduğunu ve bunları gizlemeye çalıştıklarını ortaya koymak açısından önemli bir veri olduğu kaydedildi.

Örgütün üst düzey “abi” ve “ablaları”nın, sadece hangi ülkeye ait olduğunun görülebildiği başka ülkelerde kayıtlı mobil telefon hatları kullandıkları, yurt dışındaki okullarla irtibat için ise kiralık hatlar vasıtasıyla şifreli IP telefon kullandıkları anlatılan iddianamede, mobil veri ile iletişime imkan tanıyan Skype, Tango, ByLock, Kakaotalk, WhatsApp ve benzeri programların da düşük maliyetli olması ve mesajlaşmaların şifrelenerek korunması sebebiyle sık tercih edilen haberleşme yöntem ve aracı olduğu ifade edildi.

“17-25 Aralık sürecinden sonra ByLock kullanımına başlandı”

Örgüt lideriyle çoğunlukla en sağlıklı haberleşme yöntemi olarak kabul edilen canlı kuryeyle haberleşildiği, talimat almak veya faaliyetler hakkında bilgi vermek amacıyla ABD’nin Pensilvanya eyaletine gidilerek örgüt lideriyle yüz yüze görüşüldüğü ve talimatların bizzat liderlerinden alındığı anlatılan iddianamede, “Casusluk şebekesi gibi hareket eden ve gizliliğe büyük önem veren FETÖ, özellikle 17-25 Aralık sürecinden sonra suç faaliyeti içinde olmanın bilinciyle muhtemel telefon dinlemelerine karşı, o güne kadar örgüt içi iletişimde kullandığı programlar terk edilerek, örgüt tarafından geliştirilen kriptolu haberleşme programı ByLock’u kullanmaya başlamıştır.” ifadesine yer verildi.

İddianamede, FETÖ elebaşı Fethullah Gülen’in, “Tüm üyeler ByLock programı üzerinden görüşmeler yapsın, normal telefonla görüşme yapanlar hizmete ihanet etmiş olur” şeklindeki talimatının ByLock programının örgüt için ne anlama geldiğini göstermesi bakımından önemli olduğu vurgulanarak, örgüt üyelerinin Gülen’in bu talimatıyla, özel bir server üzerinden yalnızca örgüttekilerin kullanabileceği, özel bir yazılım olarak üretilen, üyelerin deşifre olmadan kendi aralarındaki iletişimi sağlama amaçlı, ByLock isimli kriptolu program üzerinden haberleşmeye başladıklarının anlaşıldığı dile getirildi.

ByLock programının kurulum dosyası olmadan, haricen ya da internet üzerinden temininin mümkün olmadığı, programa erişimi örgüt üyelerinin birbirlerine kurulum dosyasını dijital ortamda vererek sağladığı ve bu özelliği nedeniyle de programın örgüte aidiyeti kesin olan bir program olduğu aktarılan iddianamede, bunun da ByLock programına, FETÖ/PDY içerisinde faaliyet göstermeyen bir kişinin ulaşmasının mümkün olmadığını gösterdiğine işaret edildi.

“Genellikle ABD üzerinden bağlantı gerçekleşmektedir”

ByLock programının, Bluetooth, flashbellek vb. ile kurulum dosyasını telefona kopyalamayla başlayan

özde bir mesajlaşma programı olduğuna yer verilen iddianamede, giriş şifresi oluşturulduktan sonra sisteme Türkiye haricinden başka bir ülkenin serverı üzerinden bağlantı sağlanabildiği ve bu bağlantının genellikle ABD üzerinden gerçekleştiği belirtildi.

İddianamede, ByLock'un sunucusunun Litvanya'da olduğu, program üzerinden gönderilen mesajların, alıcı tarafından silinmemiş ise 24 saat içerisinde, sistem tarafından otomatik olarak silindiği, göndericinin mesajı gönderdikten sonra telefonundan silmesi ve alıcının mesajı okuması durumunda sistemin mesajı otomatik olarak sildiği, gelen mesajlardan telefonların özelliklerine göre ekran görüntüsü ve kopyasının alınabildiği anlatıldı.

Programın önce İngilizce yazılım olarak, daha sonra da Türkçe yazılım güncellemesi yapılarak "Turquoise" ismiyle tüm Türkiye'deki örgüt mensuplarının hizmetine sunulduğu, örgüt tarafından programın Türkçe- İngilizce versiyonlarının kullanıldığı ifade edilen iddianamede, şunlar kaydedildi:

"ByLock ve Turquoise isimli versiyonlar başta App Store ve Play Store olmak üzere hiçbir mağazada satışa sunulmamakta, örgüt üyeleri dışında temini mümkün olmamaktadır. Program kullanılmaya başlandıktan sonra başta örgütün elebaşısı Fetullah Gülen olmak üzere örgütün üst yöneticilerinin emir ve talimatlarının, bölge imamlarına, bölge imamları vasıtasıyla il ve ilçe imam, abi ve diğer sorumlulara, onların aracılığıyla da tüm diğer örgüt mensuplarına ulaştırıldığı bilinmektedir.

Örgütün 15 Temmuz 2016 günü yapmış olduğu silahlı kalkışma-darbe teşebbüsü eyleminin hemen akabinde, 'ByLock silinsin, telefonlar formatlansın' talimatını vermesi, soruşturmalar kapsamında yakalanan tüm örgüt mensuplarının telefonlarını ya formatlattıklarının ya da yeniledikleri tespit edilmesi, ByLock programının FETÖ/PDY'ye aidiyetini, programı kullananın da örgüte mensubiyetini gösteren en önemli karinedir."

"Google'da 'ByLock' aramaları 7-13 Eylül 2014 aralığında tavan yaptı"

İddianamede, ByLock ve uygulama sunucularının ayrıntılı teknik çalışmalara tabi tutulduğu, bu çalışmalarda uygulamanın teknik tasarımına, mimarisine, işleyişine, aynı işlevi gören uygulamalarla benzer ve farklı yönlerine, kullanıcı profiline ilişkin hususların değerlendirildiğine vurgu yapılarak, "Google Play'de 2014 yılının başlarında kullanıma sunulan ve 2016 yılının ilk aylarına kadar çeşitli versiyonlarla kullanımda bulunan ByLock uygulamasında, kriptolu anlık mesajlaşma, kriptolu sesli görüşme, grup mesajlaşmaları, dosya paylaşımı, e-posta iletişimi, arkadaş ekleme özellikleri mevcuttur. Uygulama üzerinden telefon numarası veya ad-soyad ilgileriyle arama yapılarak kullanıcı ve telefon rehberindeki kişilerin de otomatik olarak eklenmesine imkan bulunmamaktadır. Kullanıcıların birbirleriyle ByLock uygulaması üzerinden iletisime geçebilmeleri için tarafların birbirlerinin 'kullanıcı adı/kodu' bilgilerini bilmeleri ve her iki tarafın diğerini arkadaş olarak eklemesi gerekmektedir." denildi.

Darbeye teşebbüs tarihi olan 15 Temmuz 2016'dan öncesine dair ByLock uygulamasına ilişkin açık kaynaklarda yürütülen araştırmalar sonucunda, uygulamanın Google Play ve Apple Store uygulama marketlerinden yayından kaldırıldığı ve uygulama kurulum dosyalarına erisimin devam ettiğinin tespit edildiği aktarılan iddianamede, 17 Aralık 2013 ve 17 Şubat 2016 tarihleri arasında 'ByLock' anahtar kelimesi kullanılarak yapılan Google aramalarına göre, aramaların 7-13 Eylül 2014 tarih aralığında tavan yaptığı, 2015 yılının başlarında inişe geçtiği ve sonraki süreçte de tekrar yükselişe geçmediğinin belirlendiği anlatıldı.

"Bylock'un indirilmesi değil, kullanılma durumu irdelendi"

İddianamede, ByLock uygulamasıyla ilgili Türkiye dışında Fransa, İngiltere ve ABD'de de arama yapılmasına rağmen aramaların neredeyse tamamının Türkiye kaynaklı olduğu, diğer ülkelerden yapılan aramaların da örgütün yabancı ülkelerdeki üyeleri veya Türk kullanıcılar tarafından VPN bağlantısı ile gerçekleştirildiğinin değerlendirildiği kaydedilerek, şu bilgilere yer verildi:

"İndirme sayılarının, uygulama sunucusu üzerinde olduğu görülen 215 bin 92 adet kullanıcı sayısıyla uyumsuz olmadığı değerlendirilmektedir. Nitekim tüm çalışmalarda, bilinçli veya bilinçsiz indirme değil, kullanma durumu irdelenmiştir. Dolayısıyla, muhtelif indirme rakamlarından ziyade, uygulamaya kayıt olmuş kullanıcıların esas alınması gerekmektedir. Twitter'da, 15 Temmuz 2016 tarihi öncesinde ByLock uygulamasına ilişkin paylaşımlarda bulunan kullanıcıların büyük çoğunluğunun, FETÖ/PDY lehine paylaşımlarda bulunduğu görülmüştür. Bu durum, kimliği tespit edilebilen hesap kullanıcılarının örgüte müzahir şahıslar olduklarının, kamuoyuna yansımasında önce uygulamayı bildiklerinin ve yaygın şekilde kullandıklarının göstergesi olarak değerlendirilmiştir."

"ByLock bilgisine 15 Temmuz'dan önce Ekşisözlük'te de rastlanılmadı"

ByLock uygulamasının, 15 Temmuz'dan önce, belirli sayıda olmak üzere, Twitter dışındaki çok az platformda yer aldığı, Eksisözlük, Uludagsözlük ve İncisözlük gibi güncel konuların ve kavramların yoğun olarak paylaşılıp tartışıldığı platformlarda uygulamayla ilgili herhangi bir bilgiye rastlanılmadığına dikkat çekilen iddianamede, "Toplumda ve hatta teknik konularla ilgili insanlar arasından bilinirliği yok denebilecek seviyedeyken, istatistikler göz önünde bulundurulduğunda, diğer ülkelere kıyasla Türkiye'den kullanım değerlerinin açık, farklı, yüksek olması, (diğer tüm ülkelerin toplamından çok daha fazla) uygulamanın amacı hakkında fikir veren en önemli unsurlar arasında görülmektedir." değerlendirmesinde bulunuldu.

İdidanamede, iki kullanıcı arasında iletilen verilerin kriptografik algoritması kullanılarak şifrelendiğinin belirlendiği, kriptografik algoritmanın bir tür açık anahtarlı/asimetrik şifreleme algoritması olduğu ve biri gizli diğeri açık olmak kaydıyla iki adet anahtar kullanarak şifreleme yaptığı ifade edilirken, şöyle devam edildi:

"Uygulama sunucusunu yöneten şahsın, uygulamanın hizmet sunucuyu ve IP adreslerini kiralama yöntemi ile temin ettiği, söz konusu hizmetlere ait bedelleri aylık ve üç aylık aralıklarla ödediği, bu işlemleri **** adlı elektronik posta adresi üzerinden gerçekleştirdiği tespit edilmiştir. Bahsi geçen sunucunun, Litvanya'da hizmet veren 'Baltic Servers' isimli firmanın kiraladığı sunuculardan biri olduğu görülmüştür."

Uygulama sunucusu yöneticisinin, uygulamayı kullananların tespitini nispeten zorlaştırmak amacıyla 8 adet ilave IP adresi kiraladığı ve 15 Kasım 2014'te uygulama için açtığı bir web sayfasında, Ortadoğu'dan gelen bazı IP adreslerinin uygulamaya erişimini engellediğini duyurduğu anlatılan iddianamede, "Uygulama sunucularına yönelik yürütülen teknik incelemeler neticesinde elde edilen bilgilerle, şahsın engelleme işlemini 17 Kasım 2014 tarihinde yaptığı, fakat 15 Kasım 2014 tarihinden önceki erişim log kayıtlarını veri tabanından sildiği tespit edilmiştir. Engelleme işlemine konu IP adreslerinin tamamına yakınının Türkiye IP adresleri aralığında olduğu, dolayısıyla şahsın, açıklamalarında, 'Ortadoğu' derken aslında özellikle Türkiye'den gelen bağlantıları engellemeye yönelik bir çalışmada bulunduğu anlaşılmıştır. Bu yöntemle uygulamayı kullananların tespitinin önüne geçilmesini amaçlayan kurgusal başka bir tedbir alındığı değerlendirilmektedir." denildi.

"1 milyon 218 bin 784 çağrı, 17 milyon 169 bin 632 mesajlaşma"

İddianamede, uygulama sunucusu yöneticisinin gerçekleştirdiği IP engellemesinin, Türkiye'deki kullanıcılarının uygulamaya erişimlerini engellemekten ziyade, kullanıcıların VPN kullanılması sonucunda gerçek IP adresleri ile sunucuya bağlanmalarının tespit edilmesini önlemeyi amaçladığı sonucuna varıldığı anlatılarak, yürütülen çalışmalar sonucunda ByLock uygulama sunucusundaki veri tabanı dosyaları, sunucu yöneticisi tarafından girilen komutlar ve sunucuda çalışan yazılım dosyalarının elde edildiği belirtildi.

İddianamede, ByLock uygulaması üzerinde yapılan çalışmalar sonucu, bütün çağrı hareketleri, mesajlaşma, mailleşme ve rehber bilgileri tablolarına ilişkin elde edilen şu verilere de yer verildi:

"Uygulamaya kayıt olan kullanıcı sayısı 215 bin 92, parolası çözümlenebilen kullanıcı sayısı (çözümleme işlemi devam etmektedir) 184 bin 298, oluşturulmuş toplam grup sayısı 31 bin 886, toplam mesaj içeriği (gönderilen ve alınan bütün mesajlar) 17 milyon 169 bin 632, çözümlenen mesaj içeriği (çözümleme işlemi devam etmektedir) 15 milyon 520 bin 552, verilerdeki toplam e-posta içeriği 3 milyon 158 bin 388, çözümlenen e-posta içeriği (çözümleme işlemi devam etmektedir) 2 milyon 293 bin 518, an az bir kez mesaj atmış ve/veya almış şahıs sayısı 60 bin 473, sesli görüşmeyi kullanan şahıs sayısı 78 bin 165, sadece sesli iletişim için kullanan şahıs sayısı 46 bin 799."

"Global uygulama maskesiyle FETÖ hizmetine sunuldu"

Uygulamayı geliştiren ve kullanıma sunan şahsın, daha önce yaptığı işlere ilişkin referansları ile erişilebilir iletişim bilgilerinin bulunmadığı, sektördeki geçmişinin belirsizlik arz ettiği, kullanıcı sayısını artırmayı, ticari değer haline gelmeyi hedeflemediği ve uygulamanın tanıtılmasına yönelik girişimlerinin olmadığı vurgulanan iddianamede, şunlar kaydedildi:

"Kullanıcı adlarının, grup isimlerinin ve çözümlenen şifrelerin ve içeriklerin büyük çoğunluğunun Türkçe ifadelerden oluşması, uygulama sunucusu yöneticisinin gerçekleştirdiği engellemelerin tamamına yakının Türkiye IP adreslerine yönelik olması, Türkiye'de kullanıcıların uygulamaya erişiminin, VPN vasıtasıyla gerçekleştirilmesine zorlanması, Google üzerinden gerçekleştirilen aramaların neredeyse tamamının Türkiye'deki kullanıcılar tarafından gerçekleştirilmesi, ülkedeki IP adreslerinden erişimin engellendiği tarih itibariyle uygulamaya yönelik Google aramalarında büyük bir artış olması, uygulamayla ilişkili internet kaynaklı yayınların çoğunlukla sahte hesaplar üzerinden FETÖ/PDY lehine paylaşımlarda bulunulması, 200 bini aşkın kullanıcı kitlesine sahip ByLock'un 15 Temmuz darbe girişimi öncesinde ne Türk kamuoyu ne de yabancılar tarafından bilinmemesi/tanınmaması hususları birlikte değerlendirildiğinde, bu uygulamanın global bir uygulama maskesi altında, FETÖ/PDY mensuplarının kullanımına sunulduğu anlaşılmıştır."

"38 haneye varan parolalar kullanmışlar"

İddianamede, ByLock uygulamasını kullanan örgüt mensuplarının kendilerini gizlemek amacıyla çok uzun haneli parolalar belirlediğine de işaret edilen iddianamede, şöyle denildi:

"Örneğin çözümü tamamlanan veriler arasında 38 haneye varan parolaların yer aldığı ve çözümü tamamlanan parolaların yarısından fazlasının 9 hane ve üzerinde karakter içerdiği, belirli bir tarihten sonra uygulamanın Android market veya Apple Store'dan indirilmesi yerine, kullanıcıların cihazlarına manuel olarak yüklendiği, uygulamaya kayıt esnasında gerçek isimlerin 'kullanıcı adı' olarak belirlenmediği, haberleşme içeriklerinde ve uygulamadaki arkadaş listelerinde kişilerin gerçek bilgileri yerine örgüt içerisindeki kod adlarına yer verildiği görülmüştür. Elde edilen ve çözümleme işlemleri tamamlanan mesajlaşma içeriklerinin tamamına yakınının FETÖ/PDY unsurlarına ait örgütsel temas ve

faaliyetleri içerdiği ve örgüte ait jargonla örtüştüğü görülmüştür.

FETÖ/PDY unsurlarınca gerçekleştirilen 15 Temmuz 2016 askeri darbe girişimi sonrasında adli kontrol işlemlerine (gözaltı, tutuklama, yakalama vb.) tabi tutulan örgüt mensuplarının ifadelerinden, 2014 yılının başlangıcında FETÖ/PDY örgüt üyeleri tarafından örgütsel haberleşme aracı olarak kullanıldığı anlaşılmıştır. İzah edilen durumların hepsi birlikte değerlendirildiğinde, ByLock uygulamasının, global bir uygulama görüntüsü altında münhasıran FETÖ/PDY silahlı terör örgütü mensuplarının kullanımına sunulduğu sonucuna varılmaktadır."

Şüphelilerin eylemleri

İddianamede, bu programı kullandıkları tespit edilen BDDK görevlisi şüphelilerin eylemlerine de yer verildi.

Kurumda başkan müşaviri olarak görev yapan tutuklu şüphelilerden Murat Türker'in, FETÖ/PDY mensupları arasında haberleşmeyi sağlamak, örgüt lider ve yöneticilerinin emir ve talimatlarını aktarmak için geliştirip kullandığı, kriptolu haberleşme programı ByLock'u adına kayıtlı hat üzerinden 12 Ağustos 2014 tarihinde indirdiği ve yoğun kullanım karşılığı turuncu renk grubuyla kullandığı belirtildi.

İddianamede, örgütle bağlantılı olduğu gerekçesiyle kurumundan ihraç edilen ve bu gerekçeyle hakkında suç ihbarı yapılan şüpheli Türker'in örgüt lider ve yöneticilerinden söz konusu program üzerinden emir ve talimat alarak süreklilik ve etkinlik arz edecek şekilde örgütün hiyerarşik yapısı içerisinde yer almak suretiyle üzerine atılı, "silahlı terör örgütü üyeliği" suçunu gerçekleştirdiği dile getirildi.

Diğer şüphelilerin de örgüt yöneticilerinin emir ve talimatlarını aktarmak için bu programı çeşitli tarihlerde telefonlarına indirdikleri ve örgütün hiyerarşik yapısı içinde aynı suçu işledikleri belirtilen iddianamede, ifadesi alınamayan firari 5 şüpheli haricinde BDDK görevlisi tutuklu 21 şüphelinin, ifadelerinde ByLock programını telefonlarına indirip kullanmadıkları ve örgütle bir ilgilerinin olmadığı yönünde beyanlarda bulunduğu kaydedildi.

 # 15 Temmuz

21 Oca 2017 - 11:07 - Gündem

TAKİP ET

Sitemizdeki dış bağlantılar referans amaçlıdır, dış bağlantıların içeriklerinden kuruluşumuz sorumlu değildir

Kuruluş Hakkında

Künye Bilgileri

Yayın İlkeleri

Haber İhbar
Reklam Ver

İletişim

Veri Politikası Kullanım Şartları

+90 (212) 550 90 05

daktilo