2.A.C.M.
2016/392 E.

BYLOCK TEKNİK RAPORUNU İNCELEME RAPORU

İÇİNDEKİLER

TANIMLAR VE KISALTMALAR

RAPOR:	Milli İstihbarat Teşkilatının hazırlamış olduğu "ByLock Uygulaması Teknik Raporu" [1]
Android:	Mobil cihazlar için geliştirilen açık kaynak kodlu işletim sistemi
Apk dosyası:	Androidişletim sisteminde kullanılan varsayılan paket dosyası formatıdır (Android Application Package).
AppStore:	Apple IOS işletim sistemleri için geliştirilmiş uygulamaların bulunduğuresmi mağaza.
BalticServers:	ByLock sunucularını barındırdığı iddia edilen Litvanya'da bir şirket.
Güvenlik duvarı:	Kurulduğu konumda gelen ve giden ağ trafiğini kontrol ederek bilgisayarımıza ya da bilgisayar ağınıza yetkisiz veya istemediğiniz kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.
Hack:	Sahibinin bilgisi ve izni olmadan, bir bilgiyi elde etmek, değiştirmek veya kullanılamaz duruma getirmek.
Hash fonksiyonu:	Farklı uzunluklu veri kümelerini, sabit uzunluklu veri kümelerine dönüştürentek yönlü algoritma veya alt programdır.Kriptografik özet fonksiyonu da denir.
Hosting:	Sunucu barındırma hizmeti.
IOS:	Apple tarafından mobil cihazlar için geliştirilmiş işletim sistemi.
IMEI numarası:	Uluslararası Mobil Cihaz Kodu (International Mobile Equipment Identity).

iptables:	Bir güvenlik duvarı yazılımı.
İstemci:	Sunucu bilgisayarın izni ve yetkilendirmesi ile verilen hizmeti kullanan cihaz, bilgisayar veya yazılım.
Log:	Bilişim sistemlerinde olayların ve hareketlerin özet kayıtları.
MAC adresi:	Bir bilgisayar ya da cihazın ağa erişimini sağlayan donanımın fiziksel adresi (kimliği).
Örneklem:	Bir araştırmada bütünü anlamak için bütünden seçilen araştırma tekniklerinin uygulanacağı grup.
PlayStore:	Android işletim sistemleri için geliştirilmiş uygulamaların bulunduğu resmi mağaza.
Sunucu:	Çeşitli amaçlar için kesintisiz hizmet veren, fiziksel ya da sanal bilgisayar veya bu bilgisayar üzerindeki hizmet yazılımı.
VPN:	Uzak bilgisayarlar arasında internet üzerinden sanal olarak yerel ağ kurulmasını sağlayan, genellikle şifreleme ile bağlantının güvenliğini sağlayan protokollerin genel adı (Virtual Private Network).

1. GİRİŞ

Son zamanlarda ByLock Uygulaması hakkında çok şey konuşuldu ve yazıldı. Binlerce kişinin tutuklanmasında en önemli unsur olarak kullanıldı. Özellikle yazılı-görsel basında ya da sosyal medyada yetkisiz ve bilgisizkişilerce açıklama yapıldı, kamuoyu ve adlî merciler etki altına alınmaya çalışıldı. Bu uygulamayı kullanmak suç olabilir miydi? Elde edilen listeler doğru ve güvenilir miydi? Listelerde manipülasyon yapılmış mıydı? En önemlisi elde etme yöntemi hukukî miydi?

Bu çalışmada, tartışılan bu konulara teknik ve hukukî açıklık getirilmeye çalışılmıştır. Üslup korunmaya çalışılmıştır. Tüm yargılara referans gösterilerek Kaynaklar bölümünde listelenmiştir.

Çalışmada, Milli İstihbarat Teşkilatı tarafından hazırlanan ByLock Uygulaması Teknik Raporu [1] çerçeve olarak kullanılmıştır.RAPOR'un, ByLock Listelerini güçlendirmesi açısından delil olarak dosyalara konulduğu düşünülmektedir. Mahkemelerce kesin bir şekilde güvenilir kabul edilmesine rağmenkaynak belirsiz ve çelişkiler barizdir.

Bu RAPOR'da beyan edilen ya da beyan edilmeyen teknik detaylardan ve örnek verilerden, basına yansıyan bilgilerden MİT'in yaptığı çalışma çözümlenmeye çalışılmış, çelişkiler belirtilmiştir..

2. BYLOCK UYGULAMASI

2.1. ByLock Nedir?

ByLock, 2014 Nisan ayından 2016'nın Şubat ayı sonlarına kadar hizmet veren anlık mesajlaşma uygulamasıdır. Google PlayStore ve Apple AppStore uygulama mağazalarından indirilebilen, hâlâ da apk dosyası şeklinde çeşitli açık depolarda bulunan tüm dünyaya açık bir uygulamadır [1]. Bir milyona varan indirme sayısına ulaşmıştır. İletişim, bütün anlık mesajlaşma uygulamalarında olduğu gibi uçtan uca şifreli olarak gerçekleştirilir. Uygulamaya üye olabilmek için hiçbir kısıtlama yada referans gereksinimi yoktur (Yandex mail [2] gibi). Kullanıcılar karşılıklı olarak birbirlerini eklemek suretiyle iletişime geçerler (Yahoo Messenger [3]gibi). Kullanıcılarına eposta, dosya transferi ve sesli iletişim imkânı vermektedir. Mesajlar üç günden sonra otomatik olarak silinir(SOMA Messenger'da teslim edilen mesajlar hemen kalıcı olarak siliniyor, teslim edilmeyen mesajlar da 7 günlük zaman aşımı süresinden sonra kalıcı olarak siliniyor [4]. Güvenlik kameraları ve uçaklardaki kara kutular gibi) [1].

Uygulama ile ilgili haklar Türk asıllı David Keynes adına kayıtlıdır [5].Uygulamanın kendisi yukarıda bahsedildiği gibi hâlâ temin edilebilmekte fakat uygulama sunucusu erişilebilir durumda değildir.Uygulama sunucusu hizmet verdiği dönemde Litvanya'da bulunmaktaydı [1].

2.2. Kronoloji

Tablo 1 deki tarihler ve olaylar farklı kaynaklardan alındığı için tutarsızlık olabilir. Fikir vermesi açısından burada yer verilmiştir.

Tablo 1 ByLock uygulaması ile ilgili önemli tarihler.

Tarih	Olay
03 Aralık 2013	ByLock'u tasarlayan 'Tilki' lakaplı kişi, bu tarihte programı AppStore'a koyabilmek için David Keynes'in kredi kartını kullandı, kullanım hakkı bu isim üzerine kaydedildi[5].
12 Mart 2014	İlk ByLock kullanıcısının (id=1) erişim tarihi [6].
Nisan 2014	İlk ByLock kullanıcılarının erişirim tarihleri [6].
Nisan 2014	46.166.160.137 IP adresi ile hizmet sunuyor. (Tarih okunamadı. Sunucu işletim sistemi Ubuntu 14.04, releasedate: 17.04.2014) [1].
Mart 2014	ByLock, Mart 2014'ten sonra Apple Store ve Google Play adlı online mağazalarda kullanıma açıldı [5].
24 Ağustos 2014	ByLock geliştiricisi tarafından 46.166.164.176/29 aralığında 8 IP kiralandı ama hiçbir yönlendirme yapılmadı[1].
07 Eylül 2014	ByLock, AppStore'dan kaldırıldı [5].
15 Kasım 2014	"bylockapp.wordpress.com" adresli web sayfasında, Ortadoğu'dan gelen bazı IP adreslerinin uygulamaya erişiminin engellendiği duyurulmuştur[1].
15 Kasım 2014	Bu tarihten önceki erişim log kayıtları, yönetici tarafından veri tabanından silindi [1].
17 Kasım 2014	Ortadoğu IP'lerinin sunuculara erişimi engellendi. Türkiye kullanıcıları VPN kullanmak zorunda bırakıldı [1].
19 Ocak 2015	6437 ID'liByLock sunucusu için fatura kesildi (Dönem 08/02/2015-08/03/2015) [1].
1 Eylül 2015 - 9 Ekim 2016	Bu tarihleri arasında 46.166.160.137 adresinin bylock.net alan adı ile kullanıldığı bulgusuna ulaşılmıştır [1].
Aralık 2015 – Ocak 2016	MİT, sistemde ne varsa bu tarihlerde alıyor [6].
11 Aralık 2015	Uygulama loglarındaki ilk verinin tarihi [1].
Ocak 2016	Bu tarihten itibaren ByLock'un kullanım dışı oldu [5].
Şubat 2016	Bu tarihe kadar sunucu giderleri için PaySera ödeme sistemi ile ödemeler yapıldı [1].
1 Mart 2016	Bu tarihte ByLock hizmet vermeyi tamamen durdurdu [7].

Mayıs 2016	MİT, Mayıs ayı sonlarına doğru ByLock kayıtlarından saptayabildiği 40 bin kadar isimden devlet kurumlarında çalışanları, kendi kurumlarına bildirmeye başladı [6].
17.06.2016	David Keynes'in Türkiye'ye son giriş tarihi [5].
07 Ağustos 2016	David Keynes'in Türkiye'den çıkış yaptığı tarih [5].
10 Eylül 2016	TÜBİTAK eski yöneticilerinden Mesut Yılmazer, gözaltına alındı [8].
11 Eylül 2016	TÜBİTAK eski yöneticilerinden Mesut Yılmazer, ByLock'u yazan ekipte yer aldığı kuşkusuyla çıkarıldığı mahkemede tutuklandı [6].
12 Ekim 2016	David Keynes, Hürriyet Gazetesinden İsmail Saymaz ile iletişime geçti [5].
16 Ekim 2016	Hürriyett Gazetesinden İsmail Saymaz, David Keynes ileABD'de röportaj yaptı [5].
04 Mart 2017	MİT'in ByLock Uygulaması Teknik Rapor'u internete düştü [9].

3. MİT'in BYLOCK RAPORU'ndaki ÇELİŞKİLER

3.1. Kriptosuz Haberleşme Uygulaması Olur mu?

RAPOR'da çokça (45 adet) "*kripto*" kelimesi veya ekli versiyonları, (67 adet) "*şifre*" kelimesi veya ekli versiyonları ile (21 adet) "*parola*" kelimesi veya ekli versiyonları zikredilmiştir. Uygulama kullanıcılarını daha sırlı hale getirip, gizlenen her bilginin suç unsuru teşkil ettiği algısı oluşturulmaya çalışılmıştır.

İletişimde araya girme yöntemlerinin en ilkeli belki de telefon kablosuna toplu iğne ile paralel atmaktır. Böylece iki kişi sabit telefon ile görüşürken aradaki bu üçüncü kişi tüm konuşulanlara vakıf olur. Bu hack yöntemi, günümüzde "*man in themiddle (ortadaki adam)*" olarak adlandırılır. Gelişen teknoloji ile birlikte artan iletişim araçları, amatör ya da profesyonel birçok kişinin araya girmesine engel olmak ve iletişimin güvenliğini sağlamak üzere donatılmış veya programlanmıştır.

Gerek yerel ağda gerekse uluslararası bilgisayar ağı internette, iki cihaz haberleşirken geçen paketleri *ortadaki adam*'ların ele geçirmesi mümkündür. İletişimin güvenliği, bu paketler üçüncü kişilere ulaşsa dahi anlamsız olması, çözülememesi için paketlerin uçtan uca şifrelenmesiyle sağlanır. Bu şifreleme işlemi çeşitli katmanlarda, çeşitli kriptografi algoritmalarıyla yapılabilir. Günümüzde internet ortak ağını kullanan bütün haberleşme uygulamalarında uçtan uca şifreleme (kripto) bir seçenek değil, standart bir özelliktir. Dolayısıyla bir haberleşme uygulamasına *kriptolu haberleşme uygulaması* demek, *direksiyonlu otomobil* demek kadar saçmadır [9].

3.2. Kullanıcı Şifrelerini Çözmek Yıllar Alır

RAPOR'da "*Ek-11 Çözümlenen Şifrelere İlişkin İstatistiki Veriler başlığıyla*",

"*215.092 adet kriptografik MD5 özetinden yaklaşık %85'i çözülenmiş olup en sık görülen 50 şifreye aşağıda yer verilmiştir*" denilmektedir [Sayfa 85]. Ayrıca uzun şifre örneklerine de yer verilmektedir [Sayfa 88].

"*3.6.2.15 'user' tablosu*" başlığı altında;

"*'user' tablosunda, Kullanıcı Adı, kullanıcı şifresi (md5 kriptografik özeti), ...gibi bilgilerin tutulduğu görülmüştür.*" denilmektedir [Sayfa 51].

"*'user' tablosunda toplam 215.092 kayıt bulunmakta olup, uygulama kullanıcılarının kullandıkları parolalar kriptolu bir şekilde saklanmıştır. Gerçekleştirilen çalışmalar neticesinde 184.298 şahsa ait parola bilgisi çözümlenmiştir.*" denilmektedir [Sayfa 52]. Buradaki şahıstan kastın user tablosundaki *kullanıcı* olduğu anlaşılmaktadır.

Kullanıcı şifrelerini veri tabanında kriptografik özet şeklinde saklamak sıkça rastlanan bir yöntemdir. Hatta bunun aksi ciddi bir güvenlik açığıdır. Şifredeki tek bir değişiklik bile tüm kriptografik özeti değiştirir. Buna kelebek etkisi denir. Ayrıca bu özet fonksiyonları tek yönlüdür, geriye dönük çalışmaz. Yani şifreden özet üretmek çok kısa zaman alırken, üretilmiş özeti tekrar şifreye dönüştürmek imkânsızdır. MD5 veya benzeri algoritmalar ile özetlenmiş bir şifreyi çözmek için, mümkün olan bütün şifre kombinasyonları tek tek fonksiyondan geçirilerek karşılaştırılır. Bu şifre deneyerek çözmeye çalışma işlemine brute force denir.

Kullanıcı, büyük harf, küçük harf, rakam ve özel karakterlerden oluşan "`Yahaf1z99.`" şeklindeki 10 karakter uzunluğunda bir şifre seçtiğini düşünelim (bu şifrenin sık kullanılan bir şifre olmadığını ve sözlüklerde bulunmadığını varsayıyoruz). Bu şifre veri tabanındaki user tablosunda "`8bc2bef73dfcc580357cc72a012a6295`" şeklinde MD5 kriptografik özeti ile saklanacaktır [10]. Bu anlamsız özet metninden şifreye ulaşmak için 10 karakterli bütün alternatifleri tek tek MD5 fonksiyonundan geçirmek gerekiyor. Alternatif 10 karakterli şifre kombinasyonu7.423.084.163.014.967.000adet olup bu kadar şifrenin 8 çekirdekli i7 işlemcili bir bilgisayardaki çözüm süresi yaklaşık 26871 yıl olarak hesaplanıyor. Bu şifre 11 karakterli olsaydı çözüm süresi aynı bilgisayarda 2 milyon yıldan uzun sürecekti [11].Birkaç örnek Tablo 2'de yazılmıştır.

Tablo 2 Bazı örnek şifreleri çözmek için gerekli süre ve deneme sayıları.

Örnek Şifre	MD5 Kriptografik Özeti	Kombinasyon Sayısı	Çözme Süresi
9874523488	1077e73a9daab6d695 a6e09f7070a2ea	11.111.111.110	21 dakika
Haf1z.	e555244fea5dd4efd0 924776e26a2acf	211.164.779.826	7 saat
Yahaf1z99.	8bc2bef73dfcc58035 7cc72a012a6295	7.423.084.163.014.967.000	27 bin yıl
#Yahaf1z99.	c2bf111534f94d8399 dc04052075458f	571.577.480.552.152.400.000	2 milyon yıl

Sık kullanılan olarak bilinmeyen, sözlüklerde olmayan,karmaşık ve uzun binlerce şifrenin çözümü için Milli İstihbarat Teşkilatı'nın bu özelliklerdeki bilgisayarlardan milyonlarcasını aynı anda kullanması gerekir. Yani, RAPOR'da geçen zor şifrelerin şifre deneme yöntemi (brute force) ile çözülmesi imkânsızlığı ortadadır.

3.3. ByLock Sunucularının Elde Edilme Yöntemi Usulsüz mü?

RAPOR'da "*3.1 Dayanak ve Yöntem*" başlığı altında;

"*1.11.1983 Tarihli ve 2937 Sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6 ncı maddesinin (d) bendinde; Milli İstihbarat Teşkilatının görevlerini yerine getirirken; gizli çalışma usul, prensip ve tekniklerini kullanabileceği (i) bendinde ise Milli İstihbarat Teşkilatı 'dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak' yetkisiyle donatılmış bulunmaktadır.*" denilmektedir [Sayfa 12].Kanunda, burası, 6'ncı maddeni (i) bendi değil, 4'üncü maddenin (i) bendi olarak geçiyor [12].

Dayanak olarak kullanılan "*kanunî yetki*" de belirtildiği gibi üretilen bilgi ve analizler "*istihbarî*"dir. İstihbarî bilgi delil yerine kullanılamaz, haricen delillendirilmesi gereklidir [Ek-1] [Ek-2].

"*Söz konusu kanunî yetkiye müsteniden Teşkilata özgü teknik istihbarat usul, araç ve yöntemleri kullanılmak suretiyle ByLock uygulamasına ait sunucular üzerindeki veriler ile uygulama sunucusunun ve IP adreslerinin satın alındığı e-posta adreslerinin içerikleri başta olmak üzere muhtelif veriler elde edilmiştir.*" denilmektedir [Sayfa 12].

RAPOR'un başka hiçbir yerinde ByLock sunucularının veya üzerindeki verilerin elde edilme yönteminden söz edilmemiştir. "*Devletin teknik istihbarat faaliyetlerine ilişkin imkân ve kabiliyetlerin açığa çıkarılmaması ve istihbarata karşı koyma amacıyla, verilerin temin edilmesine ilişkin hassas yöntem, usul ve araçlara yer verilmemiştir.*" gibi bir gerekçeyle konu kapatılmıştır [Sayfa 12].

Ancak; 100 binden fazla kişinin "ByLock listesinde bulunmak" ("ByLock kullanmak" değil) suçuna istinaden zan altında bırakılması, gözaltına alınması, aylarca tutuklu bulunması, hatta hüküm giymesi, başka bir deyişle hürriyetten mahrum bırakılması ile sonuçlanan böyle önemli bir bilginin/listenin kaynağı sorgulanmalıdır. Hukuksuz elde edilen delil, delil değildir [Anayasa 38, CMK 206].

Sunucuyu elde etmek için, erişim bilgilerine sahip bir kişiye işkence mi yapılmıştır? Yoksa BalticServers sunucuları bir devlet kurumumuz tarafından hacklenmek suretiyle uluslararası bir suç mu işlenmiştir [6] [13]? Ya da BalticServers veri merkezindeki(datacenter) server ve storagelarözel bir operasyonla mı elde edilmiştir [14]? Veyahut BalticServers şirketi satın alınmış, sonra dabir mahkeme kararı ilesunucular MİT'e mi teslim edilmiştir? Hadi sunucu elde edildi diyelim. Çalışmaya başlamadan öncesunucu ve/veya yedekleri ham imajları ya da veri tabanı dosyaları,hash kodları ile korumaya alınmış mıdır? Belki de sunucular hiçbir zaman elde edilememiştir de, eldeki bazı bulanık bilgiler kullanılarak tüm bu (sözde) sunucu bilgileri laboratuvar ortamlarında üretilmiştir. Belki de tüm bu liste çalışmaları, bir şekilde fişlenen kişileri kamuoyu ve mahkeme nezdinde suçlu göstermek için uydurma argümanlardır.

Bu sunucuların elde edilme yöntemi usulsüz mü ki,RAPOR'da paylaşılmadı? Bu gizemin giderilmesi, raporu hazırlayan teknik heyetin(ya da personelin) sorumluluğunda olmasa bile Milli İstihbarat Teşkilatının sorumluluğundadır. Kaldı ki, teknik heyetin(ya da persone-

lin) teknik olmayan birçok konu hakkında da RAPOR'da yorum yaptığı görülmektedir. Gizem giderilse bile -mahkeme kararı olmadığı müddetçe- listenin istihbarî olduğu gerçeğini değiştirmez ve delil niteliği yoktur. Tarafsız heyetlerce teyide muhtaçtır. Bununla birlikte, sunucunun elde edildiği iddiası ile ilgili olarak RAPOR'da tam ikna edici bilgi mevcut değildir.

3.4. ByLock İstisna Bir Uygulama mı?

RAPOR'da "*2.4 ByLock Uygulamasını Global ve Ticari Anlık Mesajlaşma (Instant Messaging - IM) Uygulamalarından Ayıran Farklılıklar*" başlığı altında;

"*Anlık mesajlaşma uygulamalarının çoğu, kullanıcılara kolay kullanım özelliği sunmaktadır. ByLock uygulamasında ise, uygulamayı kullanan şahıs, iletişim kurmak istediği şahsa ait 'Kullanıcı Adı' bilgisine sahip değilse, bu kişi ile iletişim kuramamaktadır.*" denilmektedir [Sayfa 11].

"*Anlık mesajlaşma uygulamaları, kullanıcılarına hızlı iletişim imkânı sunar. ByLock uygulamasını kullanan bir şahıs uygulamayı telefonuna indirdiğinde, rehberindeki diğer şahısların uygulamayı kullanıp kullanmadığını görememekte, şahıslar ile doğrudan iletişime geçememektedir.*" denilmektedir [Sayfa 11].

Bu tarz ifadeler ile bir taraftan kullanıcı adı girilerek iletişime geçilen, başka anlık mesajlaşma uygulaması bulunmadığı yönünde algı oluşturulmaya çalışılırken, diğer taraftan 'çoğu' kelimesini kullanarak ByLock'un bir istisna olmadığı kabul edilmiştir. Nitekim Yahoo Messenger, tıpkı ByLock gibi kullanıcı adı bilinmek suretiyle arkadaş eklemeye imkân vermekte olup, rehberdeki kişileri otomatik ekleme özelliğine sahip değildir [3].

"*Anlık mesajlaşma uygulamalarında, şahıslar sosyal çevresiyle günlük ve çoğunlukla rutine dair iletişime geçmektedir. ByLock uygulamasındaki iletişim ağı ve içerikler incelendiğinde ise, örgütsel amaç ve temalı bir kullanım görülmektedir.*" denilmektedir [Sayfa 11].

Burada da uygulamaların kullanım amacı konusunda yanlış genelleme yapılmıştır. WhatsApp anlık mesajlaşma uygulamasında, günlük iletişimden ziyade sadece iş için kullanılan özel gruplar (sohbet odaları) oluşturulduğu bilinmektedir. Örneğin okul müdürleri, oluşturdukları gruplar ile mesleki paylaşımlar yapmaktadır. Bununla beraber, incelenen ByLock içeriklerinin kaç tanesinin örgütsel amaç ve temalı, kaç tanesinin günlük rutine dair iletişim-

den ibaret olduğundan bahsedilmemiştir.Sadece rutine dair iletişim yapan kullanıcıların listeden çıkarılıp çıkarılmayacağı merak konusudur?

3.5. Anonimlik

RAPOR'da "*2.4 ByLock Uygulamasını Global ve Ticari Anlık Mesajlaşma (Instant Messaging - IM) Uygulamalarından Ayıran Farklılıklar*" başlığı altında;

"*Anlık mesajlaşma uygulamalarının çoğu, reklam vb. servisler ile uygulamanın olabildiğince çok kullanıcı tarafından kullanılmasını sağlamak suretiyle uygulamanın marka değerini ve kazancını arttırmayı hedeflemektedir. ByLock uygulamasında ise daha fazla kullanıcıya ulaşmak ve ticari bir değer haline gelmek yerine 'anonimlik' temelinde belirli bir kullanıcı sayısını aşmamak istendiği anlaşılmaktadır.*" denilmektedir [Sayfa 11].

RAPOR'da da bahsedildiği gibi bylockapp.wordpress.com, Google PlayStore ve Apple AppStore gibi ortamlarda uygulama hakkında bilgi bulunduğuna göre, geliştiricinin uygulamayı gizlemek gibi bir niyetinin olmadığı anlaşılmaktadır. Tüm kaynak kodlar ve veri tabanı ele geçirilmiş ve/veya çözülmüş olmasına rağmen, uygulama kodunda ya da kullanıcı tablosunda belirli bir sayıya ulaştığında kullanıcı kaydını reddeden bir koda rastlanmamış anlaşılan ki; geliştiricinin anonimlik tercihi "*belirli bir kullanıcı sayısını aşmamak*" şeklinde yorumlanmış.

Yazılımcılar ya da web tasarımcıları kendi kimliklerini ve/veya iletişim bilgilerini whois sorgusundan gizlemek için rumuz kullanmaları bilinen bir gerçektir. Hatta domain hizmeti veren firmalar bu seçeneği müşterilerine ücretli ya da ücretsiz sunmaktadır. Örneğin Godaddy firması faturalandırma aşamasında "*Keep my personal info public*" ve "*Make my domain private for €7.99/yr!*" seçeneklerinden birini seçmelerini zorunlu kılmaktadır [15].

Anonimlik, sadece yazılımcılar ya da web tasarımcılarının tercihi değildir. Örneğin bir ürün satın aldığının ortaya çıkması durumunda utanacağını düşünen bir kişinin kimliğini gizlemek için anonimlik sağlayan ödeme yöntemlerini kullanmasından daha doğal ne olabilir?

Hatta, RAPOR yazar(lar)ı da anonimlik tercihinde bulunmuş ki hiçbir yerde isim ve unvanları ile iş tecrübeleri geçmiyor.

Ayrıca, uygulamanın kayıtlı sahibi Türk asıllı David Keynes, hakkında soruşturma açılması ve ifadesine başvurulması halinde, ByLock geliştiricisinin kimlik bilgilerini verebileceğini, bu kişinin Türkiye'de yaşadığını söylüyor [5]. Bir gazetecinin ulaşabildiği kişiye, MİT ya da güvenlik güçleri ulaşamamış mıdır?

3.6. İndirme ve Kullanma Karmaşası

RAPOR'da "*3.3 ByLock Uygulamasına İlişkin Açık Kaynak Tespitleri*" başlığı altında;

"*Tüm çalışmalarda bilinçli veya bilinçsiz 'indirme' değil kullanma durumu irdelenmiştir. Dolayısıyla, muhtelif indirme rakamlarından ziyade, anılan uygulamaya 'kayıt olmuş' kullanıcıların esas alınması gerekmektedir.*" denilmektedir [Sayfa 15-16].

"İndirme"nin önemli olmadığı, "kullanma" durumunun önemli olduğu vurgulanmış ve *kullanmak = uygulamaya kayıt olmak* şeklinde bir tanım yapılmıştır.

Ancak *kullanmak* fiili iyi tanımlı değildir. Üzerinde düşünülmesi gereken bir konudur. Bir uygulamayı kullanmak o uygulamaya kayıt olmaktan ibaret değildir. Örneğin ByLock için *kullanmak* kelimesi "*uygulama üzerinden en az bir kez mesaj atmış ve/veya almış, ya da en az bir başarılı sesli görüşme yapmış olmak*" şeklinde tanımlanabilir.

RAPOR'da;

Uygulamaya Kayıt Olan Kullanıcı Sayısı	=215.092
En Az 1 Kez Mesaj Atmış ve/veya Almış Şahıs Sayısı	=60.473
Uygulamayı Sadece Sesli iletişim için Kullanan Şahıs Sayısı	=46.799

şeklindeistatistik verilmiştir [Sayfa 56]. (Tablonun gidişatından buradaki "*şahıs*" kelimesi ile "*kullanıcı*" kastedildiği düşünülmektedir.)

Yukarıdaki örnek tanıma göre ByLock *kullanan*kullanıcı sayısı 107.272 olarak bulunur. Bu durumda bile,birden fazla kullanıcı hesabına sahip olanlar ile (exception ya da call_history tablosu incelenerek) hiç başarılı sesli görüşme yapamayanlar sayıdan düşülmelidir.

Bu arada, RAPOR'da sesli görüşme içerikleri ile ilgili hiçbir veri ve çalışmadan söz edilmemiştir.İçerik çalışması sadece mesaj/mail trafiği olan 60.473 kullanıcı ile ilgilidir. Dolayısıyla basına yansıyan 122.000 kişilik güncel ByLock listesindeki[16] kişilerin en azından

61.527 si hakkında kesinlikle içerik çalışması yoktur. Bu konu daha sonra ayrıntılı olarak ele alınacaktır.

Ayrıca RAPOR'da indirmenin masum olduğu ve irdelenmemesi gerektiği söylenmesine karşın, teknik incelemelerde cihazlarında ByLock izine rastlanan şahısların –listelerde olmasa bile- aylardır tutuklu bulunduğu ve bunun somut delil sayıldığı bir gerçektir.

3.7. Sunucu Analizleri

RAPOR'da "*3.4.2.1 Statik Analiz*" başlığı altında;

"*Uygulamanın kaynak kodları içerisinde, Türkçe "Dosya", "Posta" ve "Sesli Arama " şeklinde ifadelerin bulunduğu görülmüştür (Ek-5).*" denilmiştir [Sayfa 18].

Kaynak kodlardaki Türkçe ifadelerle ilgili RAPOR'un değişik yerlerinde de vurgular yapılmıştır. Ancak David Keynes gibi Türk kökenli birinin de aralarında bulunduğu bir ekibin Türkçe değişken isimleri kullanılmış olmasında ne gibi bir gariplik olduğu, hangi sonuçlara ulaşmanın hedeflendiği anlaşılamamıştır.

RAPOR'da "*Uygulama Sunucusuna Ortadoğu IP Adreslerinden Erişimin Engellenmesi*" başlığı altında;

```
root@hst-46-166-160-137:~#
iptables -N LOGGING
iptables -A INPUT -s 5.2.80.0/21 -j LOGGING
```

şeklinde bir konsol çıktısı verilmeye çalışmıştır [Sayfa 26].

Ancak RAPOR'un başka yerinde "`select * fromaction;`" gibi çıktıyı veren komut yazılırken, burada hangi komut ile böyle bir çıktı alındığı belirtilmemiştir. Çalışan bir gevenlik duvarındaki (firewall) kurallar olduğu kuşkuludur. Yönetici komut geçmişinde (history) bulunması bir şey ifade etmez.

3.8. Sesli İletişim İçeriği Yok

RAPOR'da "*3.6.2.3 'call_history' tablosu*" başlığı altında;

"Userid eşleştirilmesi yapılabilen şahıslara ait elde edilen çağrı hareketlerine ilişkin kayıtlardan, kimlerin, ne zaman ByLock uygulaması üzerinden sesli iletişim kurduğunun tespiti yapılabilmektedir." denilmektedir [Sayfa 30].

Tablo alan isimlerinden ve sonuç cümlesinden anlaşılacağı üzere sesli görüşmelerde içerik kaydı yoktur.

3.9. Anlık Mesaj İçerikleri

RAPOR'da *"3.6.2.4 'chat' tablosu"* başlığı altında;

"Elde edilen 17.169.632 adet mesajlaşma içeriğinin tamamı kriptolu olarak veri tabanında saklanmakta olup, gerçekleştirilen çalışmalar neticesinde 15.520.552 adet mesajlaşmaya ait içerikler çözümlenmiştir. Mesajların çözümlenme işlemi devam etmektedir." denilmektedir [Sayfa 31].

Örnek Mesaj İçerikleri Verinin Tam Bir Örneklemi

RAPOR'daki örnek mesajlar, içerikler dikkate alınmadan oturum oturum ayrılarak aşağıdaki özet tabloda (Tablo 3) birleştirilmiştir [Sayfa 32-37].

Tablo 3 RAPOR'daki örnek mesajlardan oluşturulmuş özet tablo.

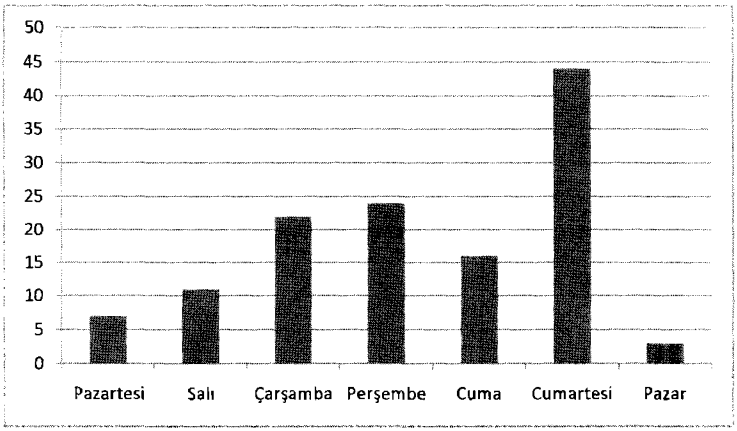
Kaynak	Gönderenin Kullanıcı IDsi	Alıcının Kullanıcı IDsi	Oturumda Gönderilen Mesaj Sayısı	Oturumda Gönderilen İlk Mesajın Gönderme Zamanı	Oturumda Gönderilen Son Mesajın Gönderme Zamanı
Örnek-1	363824	344436	1	12.12.2015 19:21:27	
Örnek-2	73605	201087	26	23.01.2016 22:29:42	23.01.2016 22:46:46
Örnek-3	56827	2637	1	20.12.2015 21:58:24	
Örnek-3	56827	2637	10	23.12.2015 20:50:50	23.12.2015 20:54:35
Örnek-3	56827	2637	2	02.01.2016 07:13:24	02.01.2016 07:13:59
Örnek-3	56827	2637	1	16.01.2016 23:20:52	
Örnek-3	56827	2637	3	26.01.2016 12:14:24	26.01.2016 12:15:11
Örnek-3	56827	2637	14	31.10.2015 19:06:28	31.10.2015 19:11:51
Örnek-4	222716	277794	2	04.02.2016 23:31:07	04.02.2016 23:45:12
Örnek-4	222716	277794	2	17.02.2016 02:20:18	17.02.2016 02:20:52
Örnek-4	222716	277794	2	22.11.2015 11:40:32	22.11.2015 11:41:05
Örnek-4	277794	222716	1	26.01.2016 22:41:01	
Örnek-4	277794	222716	4	04.02.2016 23:45:04	04.02.2016 23:46:53
Örnek-4	277794	222716	1	10.02.2016 00:28:00	

Örnek-4	277794	222716	4	17.02.2016 02:16:36	17.02.2016 02:24:04
Örnek-5	4380	49	2	16.12.2015 18:45:52	16.12.2015 18:52:00
Örnek-5	4380	49	2	26.12.2015 19:29:09	26.12.2016 19:34:10
Örnek-5	4380	49	3	31.12.2015 00:19:38	31.12.2015 01:36:29
Örnek-5	4380	49	4	01.01.2016 08:07:26	01.01.2016 08:35:45
Örnek-5	4380	49	5	04.01.2016 19:00:47	04.01.2016 19:09:15
Örnek-5	4380	49	6	07.01.2016 08:29:32	07.01.2016 08:34:48
Örnek-5	4380	49	9	08.01.2016 01:34:59	08.01.2016 01:48:21
Örnek-5	4380	49	3	22.01.2016 03:30:13	22.01.2016 18:45:53
Örnek-6	1382	8605	3	03.11.2015 14:08:48	03.11.2015 14:11:01
Örnek-6	1382	8605	9	12.11.2015 14:53:58	12.11.2015 16:44:57
Örnek-6	1382	8605	2	02.12.2015 14:31:59	02.12.2015 14:33:37
Örnek-6	1382	8605	1	09.12.2015 17:15:49	
Örnek-6	8605	1382	4	15.12.2015 12:26:42	15.12.2015 22:42:22

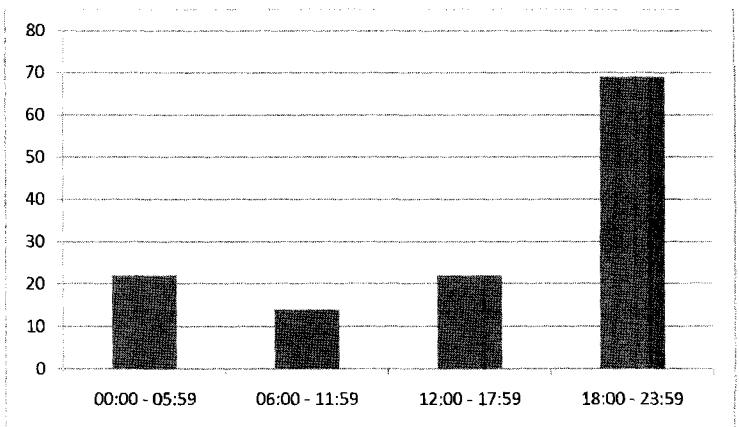
Örnek mesajlar 8 farklı kullanıcının gönderdiği toplamda 127 adet içerikten ibarettir. Gönderme zamanına göre sınıflandırıldığında örnek içeriklerin 31 Ekim 2015 ile 17 Şubat 2016 tarihleri arasında gönderildiği görülmüştür. Ayrıca örnek mesajların eldeki tüm verinin örneklemini teşkil etmesi için bu 110 günlük zamana düzgünce dağıtıldığı düşünülmektedir. Bununla beraber örnek mesajların haftalık ve günlük dağılımı da düşünceyi destekler niteliktedir. Haftanın her günü, günün her saati için örnek mesaj mevcuttur. Bu dağılım, aşağıdaki Tablo 4, Şekil 1 ve Şekil 2'de açıkça görülmektedir.

Tablo 4 RAPOR'daki örnek mesajların günlere göre dağılımı.

Ekim 2015	**Kasım 2015**	**Aralık 2015**	**Ocak 2016**	**Şubat 2016**
31 Ekim	3 Kasım	2 Aralık	1 Ocak	4 Şubat
	12 Kasım	9 Aralık	2 Ocak	10 Şubat
	22 Kasım	12 Aralık	4 Ocak	17 Şubat
		15 Aralık	7 Ocak	
		16 Aralık	8 Ocak	
		20 Aralık	16 Ocak	
		23 Aralık	22 Ocak	
		26 Aralık	23 Ocak	
		31 Aralık	26 Ocak	



Şekil 1 RAPOR'daki örnek mesajların haftanın günlerine göre dağılımı.



Şekil 2 RAPOR'daki örnek mesajların gün içerisindeki dağılımı.

İçerikler 110 Günlük: Kasım 2015 – Şubat 2016

Buradan hareketle chat tablosundaki 17.169.632 içerik kaydının, en az bir mesaj almış ve/veya göndermiş olan 60.473 kullanıcısı sayısına bölündüğünde ortalama mesaj sayısı 284 olarak bulunur.Uygulamanın faaliyette kaldığı süre boyunca kullanıcı başına günlük ortalama

1 mesaj bile gönderilmemiş demektir. Haftanın her günü, günün her saati mesaj gönderebilen bir kullanıcı profili ileRAPOR'da"*kullanıcıların örgütsel mahiyetteki haberleşme ihtiyaçlarının, başka herhangi bir haberleşme aracına ihtiyaç duyulmadan gerçekleştirildiği*" iddiası göz önünde bulundurulduğunda, kullanıcı başına günlük ortalama 1 mesaj bile atılmamış olması, chat tablosundaki kayıtların büyük bir bölümün silindiğini veya elde edilemediğini göstermektedir. Bu kayıtların son 110 günlük devrede atılmış olan mesajlar olduğu kabul edildiğinde bile, kullanıcı başına günlük 3 mesaj düşmemesi, içeriklerin oldukça eksik olduğu anlamına gelmektedir.

Hürriyet Gazetesinden Murat Yetkin, "*MİT 2015 Aralık ve 2016 Ocak'ta hafızada ne varsa alıp sistemden çıkıyor.*" diyor [6]. Yine sosyal medyada yayılan ve şüpheliye sunulan içerikler de bu tarihler arasında gönderilmiş [17]. Ayrıca medyanın konu ile ilgili refleksi göz önüne alındığında, önemli mesajların tarih tarih servis edilmesi beklenirdi [18].

Bu profilde kullanıcılara sahip uygulamanın mesaj sayısı belki de bir milyarın üzerinde olmalıydı. Üç günden eski mesajların silinmesi güvenlik ya da anonimlik gerekçesinden çok sunucudaki disk alanını koruma gayreti de olabilir. Üç günden eski mesajlar otomatik silinmesine rağmen 110 günlük zaman dilimine ait verilere erişme yöntemine de açıklık getirilmelidir. Aksi takdirde 17 milyondan fazla içerik kaydının tamamınınson üç günlük mesajlar olduğu ya da kullanıcıların uygulamayı pek de kullanmadıkları düşünülebilir.

Örnek mesajların bu kadar özenle 110 gün içerisinden (31 Ekim 2015 - 17 Şubat 2016 tarihleri arasından) seçilmesinden anlaşılıyor ki, önceki tarihlere ait kayıtlara asla ulaşılmadı.(Buradaki tarihler *civar* olarak değerlendirilmedir.) Veri mevcut olsaydı, örneğin 7 Haziran 2015 genel seçimleri değerlendirme mesajları RAPOR'da veya medyada örnek olarak verilirdi kanaatindeyiz.

Bu arada çözülmüş örnek mesajların -anlık iletişim olmasına rağmen- gönderme zamanı ile alma zamanı arasındaki zaman farkının tam 6 saat olması da ilgi çekici başka bir çelişkidir.

3.10. Log Tablosu

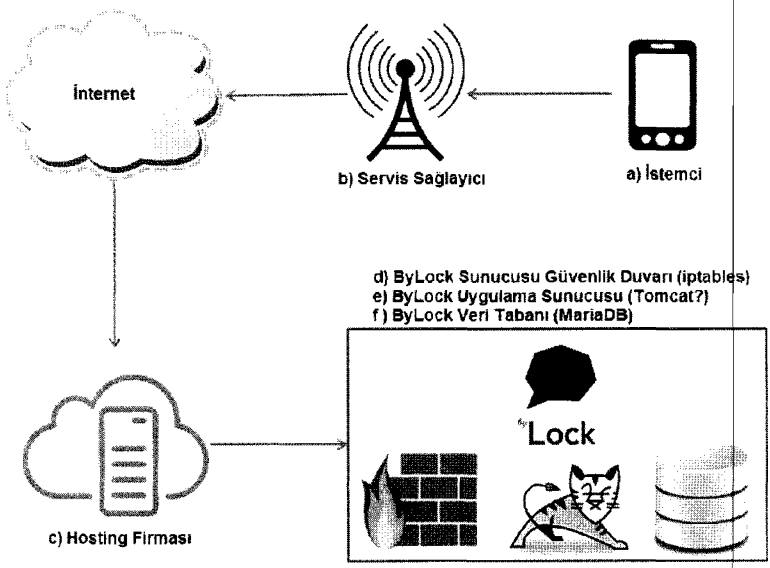
Log tutma, bilişim dünyasında çok yaygın bir işlemdir. Log kayıtları büyük bir okuldaki ziyaretçi kayıt defterine benzetilebilir. Nizamiyedeki güvenlik görevlisi okula giren kişi-

lerin kısaca kimlik bilgilerini, kim için geldiği gibi bilgileri kayıt defterine yazar. Okulun farklı bölümlerinde, güvenliğin sıkı olduğu birimlerde başka bir deftere kayıt tutulabilir.

A operatöründeki bir abonenin B operatöründeki başka bir abone ile görüştüğünü düşünelim. Bu görüşme özet bilgileri aşağıdaki sırayla farklı farklı yerlerde tekrar tekrar loglanır.

- Arayan abonenin cep telefonunda aranan numaralara *numara, arama zamanı, arama süresi* gibi bilgiler.
- A operatörü baz istasyonu ve sunucularında *arayan numara, aranan numara, arama zamanı, arama süresi, karşı operatör* gibi bilgiler.
- B operatörü sunucuları ve baz istasyonunda *arayan numara, aranan numara, arama zamanı, arama süresi, arayanın operatörü* gibi bilgiler.
- Aranan abonenin cep telefonunda gelen aramalara *arayan numara, arama zamanı, arama süresi* gibi bilgiler.

Benzer şekilde bir ByLock mobil uygulaması ile ByLock web uygulamasına arasındaki trafik farklı seviyelerde loglanabilir. İnternet paketlerinin geçtiği her durakta, en azından paketlerin başlık (özet) bilgileri kaydedebilir ve kaydedilir. Hatta ByLock sunucusunda olduğu gibi sadece bir sunucu üzerinde bile farklı farklı log kayıtları olabilir(Şekil 3). RAPOR'da bahsedilen log tablosu veri tabanındaki log tablosudur. Yani en içteki log kayıtlarıdır.



Şekil 3 Bir istemcinin ByLock sunucusuna erişirken izlediği temsili yol.

RAPOR'da "*3.6.2.11 'log' tablosu*" başlığı altında;

"*Uygulamaya giriş işlemi olan 'Login' ile uygulamaya kayıt olma işlemi olan 'Register' işlemlerinde, kullanıcılara ait IP adres bilgilerinin de 'log' tablosuna kayıt edildiği görülmüştür. Bu veriler şahıs tespit işlemlerinde kullanılmıştır. Log tablosu uygulamayı kullanan şahısların sunucuda bırakmış oldukları izler olarak görülmektedir.*" denilmektedir [Sayfa 42-43].

RAPOR'daki tanımama göre uygulamayı kullanan şahıslardan kasıt kullanıcı hesabına sahip olanlardır. Bu tanımın doğru olmadığından daha önce bahsedilmişti. Bir uygulamaya kayıt olmak ve sadece giriş yapmak o uygulamayı kullanmak anlamına gelmez.

Aralık 2015 Öncesi Log Kayıtları Yok

Örnek loglar incelendiğinde gecenin bir yarısında 12 saniye içerisinde 50 log kaydedilmiş olduğu görülecektir. Kaba bir hesapla ByLock sunucusunun hizmet verdiği toplam

sürede yüz milyonlarca log kaydının tutulmuş olması gerekirdi. RAPOR'da mesaj sayısı, mail sayısı, kullanıcı sayısı, çözümlenen mesaj, mail, parola sayısı net olarak verilmesine rağmen log tablosundaki satır sayısından hiç söz edilmemektedir.

Veri tabanı log tablosundaki örnek log kayıtları verilirken "`select * from log2 limit 50;`" komutu kullanılmış. Sıralama istenmemiş. Bu durum da veri tabanı "id" alanına göre sıralama yapmış. İlk loglama, 11.12.2015 00:27:49 da yapılmış. Buradan 11.12.2015 tarihinden önceki logların sistemde olmadığı sonucu çıkarılabilir.

Basında yer alan bir ekran görüntüsünde, user tablosundaki ilk 26 kullanıcının sisteme son giriş tarihlerinin de bulunduğu bir liste bulunmaktadır [6]. Bu listedeki en yeni tarihin 22.12.2015 olduğu görülmüştür. Bu durum inceleme çalışmalarının bu tarihler civarında yapıldığının bir göstergesidir.

Bu arada neden log tablosunda değil de log2 tablosunda sorgu yapıldığı belirtilmemiş. Log tablosundaki kayıtlar filtrelenerek log2 tablosuna mı yazılmış, varsa bu filtre hangi kritere göre yapılmış belirtilmemiş.

IP'lerin Tamamına Yakını Yurtdışı Kaynaklı

Şahıs tespit işlemlerinde kullanıldığı iddiası olmasına rağmen RAPOR'un başka hiçbir yerinde loglardaki IP'lerden T.C. Kimlik numarasına sahip şahıslara nasıl gidildiği ile en ufak bir bilgi bulunmamaktadır. Veri tabanı log tablosundaki IP'lerden kimlik tespiti yapılmasının imkânsıza çok yakın olduğu kanaatindeyiz.

Türkiye IP'leri 17.11.2014 tarihinde sunucu seviyesinde bloklandığı için (kullanıcılar iddia edildiği gibi VPN kullanmak zorunda bırakıldığı için) bu tarihten sonra uygulamaya erişenlerin gerçek IP'lerine log tablosundan erişmek mümkün değildir.

Bu log tablosunda örnek olarak verilen ilk 50 IP'nin yer (location) bilgisi tek tek sorgulandığında 49 tanesinin yurt dışı kaynaklı olduğu görülmüştür (Tablo 5) [19] [20]. Bu durumda; Türkiye IP'lenin engellenmesi sonucu *kullanıcılarının VPN kullanmaya zorlanması* tezinin doğruluğu kabul edilse bile, log kayıtlarındaki IP'lerden kimlik tespitinin imkânsıza yakın (%2) olduğu sonucunu çıkarmamıza neden olur.

Burada, *bu IP'ler şimdi yurt dışı kaynaklı görünse bile erişim zamanında Türkiye kaynaklı olamaz mı?*sorusu akla gelebilir. Ancak gerçek IP'ler servis sağlayıcılara tahsis edildiğinden, farklı tarihlerdeki sorgularda şehir değişse bile genelde ülke değişmez.

Yine de emin olmak için bir çalışma daha yaptık: Log tablosundaki ilk 50 IP ile RAPOR'da Ek-10 olarak verilen "*Uygulama Sunucusundaki Engellenen IP Adresleri Listesi*"ndeki [Sayfa 79-84] IP'ler ile karşılaştırdık. Engelleme listesinde 735 adet networkte toplam 16.362.240adet IP vardır. Örneğin aşağıdaki IP adresinin engellenen IP blok ile uyuşmaması gibi.

Engellenen Network:	188.132.128.0/17	**10111100100001001**
IP Adresi:	188.166.68.163	**10111100101001100**100010010100011

Bu karşılaştırma sonucundalog tablosundaki örnek IP'lerin hiç birinin, engelleme listesindeki networklere ait olmadığı bulgusuna ulaştık [Ek-6]. Yani sunucu seviyesindeki IP bloklama işlemi doğru çalışmış, ve engellenen Türkiye IP'lerinin hiç birisini uygulamaya ulaştırmamış. Hatta yer sorgusundaki tek Türkiye IP'si (85.203.19.87) blok listesindeki ağlara ait olmadığı için uygulama tarafından loglanmış. Yani bu, bloklama yapan kişinin gözden kaçırdığı en az bir IP bloğu olduğu anlamına gelmektedir. *İmkânsıza yakın*dan kastımız budur.

Sadece 50 adet IP den böyle bir kanaat oluşmasının sebebi ise, RAPOR'un birçok yerinde verilen örnek verilen tam anlamıyla bir örneklem oluşturduğun açık olmasıdır. Ayrıca kanaati düşürecek veriye rastlanmamıştır.

*Kimlik tespiti log kayıtlarındaki IP'ler kullanılarak yapıldığı*iddiasında ısrar edildiğinde de ByLock uygulamasının küresel olduğu (%98 Türkiye dışı) sonucuna ulaşılır ki*belirli bir grup için özel olarak geliştirildiği* iddiası RAPOR içinde çürür.

Tablo 5 Uygulama loglarındaki IP'lerin yer bilgileri.

IP ADDRESS	COUNTRY	REGION	CITY
63.141.217.112	United States	California	Torrance
109.237.27.253	United Kingdom	England	Manchester
46.165.250.77	Germany	Hamburg	Hamburg
95.90.236.57	Germany	Berlin	Berlin
41.237.216.23	Egypt		
212.71.237.37	United Kingdom	England	London
50.118.197.80	United States	California	San Jose
107.181.822.187	United States	Georgia	Atlanta
69.31.50.104	United States	Illinois	Chicago
105.196.74.28	Egypt		
188.165.245.164	France		Roubaix
188.226.164.216	Netherlands		Amsterdam
119.81.230.144	Singapore		
46.101.201.244	Germany	Hessen	Frankfurt
50.118.197.55	United States	California	San Jose
176.58.115.86	United Kingdom	Scotland	Galloway
85.159.214.107	United Kingdom	Scotland	Galloway
209.95.44.197	United States	Utah	Providence
68.80.188.144	United States	Pennsylvania	Philadelphia
192.95.46.78	Canada	Quebec	Montreal
78.214.29.62	France		Paris
37.187.57.151	France		Roubaix
151.236.221.64	United Kingdom		Telford
37.107.3.107	SaudiArabia		Riyadh
192.95.25.76	Canada	Quebec	Montreal
107.182.226.40	United States	Illinois	ElkGrove
69.31.50.186	United States	Illinois	Chicago
206.190.151.208	United States	Utah	Providence
165.14.184.166	Japan		
95.211.206.221	Netherlands		Amsterdam
178.32.117.4	France		Roubaix
216.185.39.178	United States	Ohio	Columbus
107.182.229.11	United States	Illinois	ElkGrove
66.228.57.54	United States	New Jersey	Absecon
37.139.12.233	Netherlands		Amsterdam
46.101.10.91	United Kingdom	England	London
168.235.80.45	United States	Georgia	Smarr
46.165.250.77	Germany	Hamburg	Hamburg
104.238.169.118	United Kingdom	England	London
107.182.228.69	United States	Illinois	ElkGrove
188.166.68.163	Netherlands		Amsterdam
188.166.42.118	Netherlands		Amsterdam
178.62.37.116	United Kingdom	England	London
188.165.28.83	Lithuania		Vilnius
209.95.35.113	United States	Utah	Providence
50.115.126.118	United States	Utah	Providence
37.187.56.223	France		Roubaix
85.203.19.87	**Turkey**		Istanbul
107.191.108.233	United States	Georgia	Smarr
107.162.226.87	United States	California	Belmont

Uygulama Loglarından Kimlik Tespiti Sorunları

Bir şekilde elde edilen Türkiye IP'lerinin kullanıcıT.C. Kimlik Numaralarına dönüştürülmesinde de sıkıntılar var. Tahmini iş akışı aşağıdaki gibidir:

Log tablosundaki IP'ler ve erişim tarihleri Login ve Register actionları göz önünde bulundurularak veri tabanından çıkarılır.

Bu IP'lerin Türkiye'de hizmet veren ve otoriteye bağlı servis sağlayıcılarının IP bloklarında olanları ayrı ayrı söz konusu servis sağlayıcıya gönderip, kendi IP tahsis logları ile karşılaştırarak tam o zamanda hangi IP hangi müşteriye verilmiş tespiti istenir. Servis sağlayıcılardan telefon ya da hizmet numarası, T.C. kimlik numarası, IMEI numarası gibi müşteri bilgileri alınır. Bu noktada şu konu önemlidir: IP tahsis logları en az 6 ay en fazla 2 yıl süreyle saklanır. Söz konusu log kaydının tarihi ile otoritenin talep tarihi arasında iki yıldan uzun süre varsa servis sağlayıcının bu bilgileri vermesi hukukî değildir [5651 sayılı kanun]. Bir diğer önemli husus da sucunun zaman dilimi ve saat ayarı ile her bir servis sağlayıcının zaman dilimi ve saat ayarı erişimin gerçekleştiği zaman için senkron olma zorunluluğudur. Servis sağlayıcılar müşterilerine dinamik IP dağıttığından IP tahsisleri anlık olarak değişebilir. Dakikalık hatta saniyelik şaşma, kimlik tespitinde hataya neden olur. %100 kesinlik mümkün değildir. Anlık görüşmelerdeki gönderme ve alma zamanları arasındaki saat farkının hep 6 olması, zaman dilimi ve saat ayarı konusunda sorun olduğunun bir belirtisidir.

Elde edilen bu kimlik bilgileri hâlâ gerçek kullanıcıları göstermiyor olabilir. Komşusunun kablosuz ağ şifresini bilen gerçek bir ByLock kullanıcı listesinde bulunmazken, akıllı bir cihazı bile bulunmayan komşu, Liste'den kurtulamayacaktır. Servis sağlayıcıda abonenin lehine bir bilgi tutulmamaktadır [21]. Maalesef bu durumu mağdurun kendisinin ortaya çıkarması istenecektir. Kablosuz ağ şifresi kırma işlemi, ilköğretim-lise çağındaki gençlerin bile ilgisini çekmekte, bu işe özel yazılım/donanım kolayca temin edilebilmektedir. Aynı durum telefonun internetini bir başkası ile paylaşma durumunda da geçerlidir. Ayrıca başkası adına alınan telefon hatlarında da hat sahibi listede bulunurken, gerçek kullanıcı liste dışı kalabilir.

Hatalı kimlik tespiti, telafisi mümkün olmayan sorunlara neden olabilir. Örneğin polisin, çocuk fotoğraflarını paylaşan kişinin IP adresini yazarken bir rakamı yanlış yazması so-

nucu, Nigel Lang ve eşi "çocukların uygunsuz fotoğraflarını yayma" iddiasıyla gözaltına alındı. Sağlığını ve kariyerini kaybetti. Gerçek 6 yıl sonra ortaya çıktı [22] [Ek-5].

ByLock uygulaması IOS veya android işletim sistemlerinde çalışabilmektedir. Bilindiği gibi IMEI numarası asla bulunmayan tabletlere ve android emulatörlere de uygulamalar yüklenebilmektedir. ByLock veri tabanı sunucusundaki log tablosunda veya user tablosunda da cihaz kimliği (IMEI numarası veya MAC Adresi) ilgili bir alan bulunmamaktadır. Dolayısı ile Liste'deki cep telefon numaralarının yanındaki IMEI numaralarının teknik olarak hiçbir tutar yanı bulunmamaktadır.Listeyi güçlendirmek için kullanıldığı düşünülmektedir. Bu IMEI numaraları operatör tarafından saklanan konudan bağımsız bilgilerdir. Liste'deki IMEI numaraları kontrol edildiğinde bazılarının akıllı bir telefona ait olmadığı görülecektir.

Elde edilen son liste bir otorite tarafından gözden geçirilmiş ve bazı satırlar silinmiş olamaz mı [23] [24]?

Loglardan elde edilen listeye eklemenin ve silmenin olması (manipülasyon) gayet muhtemeldir. Bu durum, tarafsız bir kurulun, ham veriler üzerindeki işlemleri tekrar etmesiyle ancak ortaya çıkabilir. (Umarız ki ham veriler, bozulmamış ve bütünlüğü hash değeri ile korunmuştur.)Listede bulunduğu iddia edilen kişilerin böyle bir araştırmayı talep etmeleri en doğal haklarıdır. Aşırı hız yaptığı tespit edilen araca ceza yazmamak, cezaya maruz kalan vatandaşın hakkını gasp etmektir. Kaldı ki "aşırı hız yapmak" tanımı olan bir eylem olmasına karşın, "ByLock Listesinde bulunmak" oldukça izafidir.

5. SONUÇ VE DEĞERLENDİRME

ByLock Listesi oluşturulurken birçok belirsizlik, hukuksuzluk, hata ve şaibe olmasına karşın, sanki kutsiyet atfedilmiş gibi hiç kimse tarafından sorgulanamamaktadır. Kişinin listede olup olmadığı gösterir bir A4 çıktısı ve altındaki sicilli paraf, *mukaddes belge* olarak dosyalara girmektedir. Maalesef örgüt üyeliğini gösterir aslî unsur ve sertifika niteliğinde değerlendirilmektedir.

Öncelikle RAPOR'a konu olan tüm ham veriler, tarafsız bir kurul tarafından yeniden incelenmeli, elde edilen bilgilerin birleştirilmesindeki hatalar giderilmelidir. Sonuç listesinin manipüle edilip edilmediği,verilerin elde edilme yöntemlerinin hukukî olarak sakıncalı olup olmadığı, delil niteliği taşıyıp taşıyamayacağı hassas bir şekilde kontrol edilmelidir. Tüm çalışma ayrıntılarıyla raporlanarak sanık ve/veya avukatları tatmin edilmelidir. Bu şeffaflık talebi sanık ve/veya avukatlarınen doğal haklarıdır. Bu talepte ısrar edilmelidir.

Kimlik tespit çalışmaları, RAPOR'da iddia edildiğinin aksine, ByLock veri tabanındaki log tablosundan yapılmış olması imkânsızdır. Çünkü log tablosundaki ilk veriden (11 Aralık 2015 tarihinden) çok önce (17 Kasım 2014 tarihinde) Türkiye IP'leri zaten engellenmişti [1]. Dolayısıyla log tablosundaki IP'lerin neredeyse tamamı yurt dışı servis sağlayıcılarına ait.

Yaklaşık 16 milyon Türkiye IP'si sunucu seviyesinde engellendiği için, bu IP'lerden uygulamanın özüne ulaşılamadığı anlaşılmıştır. Ancak engellenmeyen Türkiye IP'lerinin de olduğu görülmüştür. Buradan sızan Türkiye'deki kullanıcıların kimlik tespiti ve mesaj içeriklerine kısmen ulaşılabilir.

ByLock kullanıcı sayısı veri tabanındaki user tablosuna göre 215 bin olmakla birlikte Kimlik tespiti yapılan kişi sayısı 122 bindir [16]. Ancak içerik çalışması 60 bin kullanıcı hesabıyla ilgilidir [1]. Yani listenin yarısı için içerik çalışması kesinlikle yoktur.

RAPOR'da ve/veya basında yer alan içerik ve log kayıtları hakkında bilgiler toparlandığında, içerik çalışmamasının 31 Ekim 2015 ve 17 Şubat 2016 tarihleri arasında olduğu anlaşılmıştır. Bu tarihler arasında ByLock kullananların içeriklerine ulaşmak mümkün değildir.

MİT'in ByLock için kimlik tespit ve içerikleri çalışmaları yaptığı 2016 yılının Eylül ayından beri bilinmektedir [6]. Tüm kamuoyunun, hukukçuların, devlet erkânın üzerinde durduğu özel bir konudur. 6 aydan fazla zaman geçmesine rağmen, iddianamelere giren, mahkemelere sunulan içerik sayısının hâlâ tek haneli olması, içerik konusundaki tespitlerimizi güçlendirmektedir.

Nasıl elde edildiğine dair hiçbir bilgiye yer verilmeyen 122 bin kişilik listedeki kişiler ile ByLock veri tabanındaki en az bir içerik gönderen veya alan 60 bin kullanıcının ilişkilendirilmesi de kanaatimizce mümkün görünmemektedir. Yani hangi kullanıcı adı hangi kişiye ait eşleştirmesi ulaşılamaz durumdadır.Böylece bazı istisnalar dışında kişilerin her biri için göndermiş oldukları içerikleri tespit etmek mümkün değildir.

Log tablosundaki ender Türkiye IP'lerinden veya gizemli başka kaynaklardan elde edilen IP'lerin kimlik numarasına dönüştürülmesinde %100 kesinlik mümkün değildir. IP'lerin kaynağı (her neyse) ve servis sağlayıcıların saat uyumundan, internet ve IP paylaşımına kadar belirsizlik vardır.

ByLock veri tabanı sunucusundaki log tablosunda veya user tablosunda da cihaz kimliği (IMEI numarası veya MAC Adresi) ilgili bir alan bulunmamaktadır. Dolayısı ile Liste'deki cep telefon numaralarının yanındaki IMEI numaralarının teknik olarak hiçbir tutar yanı bulunmamaktadır. Listeyi güçlendirmek için kullanıldığı düşünülmektedir.

ByLock veri tabanında sesli görüşmeler için içerik kaydı yoktur. Kullanıcıların birbirleriyle yapmış oldukları görüşmelerin tarih ve süreleri vardır. Ancak kullanıcı hesabı ve kimlik eşleştirmesi olmadığı için gerçek kişiler arasındaki görüşme kayıtları da erişilebilir durumda değildir.

KAYNAKLAR

1. **Milli İstihbarat Teşkilatı.** *ByLock Uygulaması Teknik Raporu.* s.l. : Milli İstihbarat Teşkilatı, 2017.

2. Yandex Mail. *Yandex.* [Çevrimiçi] https://mail.yandex.com.tr.

3. **Yahoo.** Yahoo Messenger. *Yahoo.* [Çevrimiçi] https://messenger.yahoo.com.

4. **SOMA Messenger.** FAQ. *SOMA Messenger.* [Çevrimiçi] [Alıntı Tarihi: 20 Mart 2017.] https://somaapp.com/faq#q-why-should-i-trust-you-with-my-data.

5. **Saymaz, İsmail.** İşte 'By Lock' David Keynes. *Hürriyet.* [Çevrimiçi] 24 10 2016. [Alıntı Tarihi: 12 Mart 2017.] http://www.hurriyet.com.tr/iste-by-lock-david-keynes-40257030.

6. **Yetkin, Murat.** Hürriyet. *Darbe yolundaki gizli yazışmalar: ByLock.* [Çevrimiçi] 12 Eylül 2016. [Alıntı Tarihi: 13 Mart 2017.] http://www.hurriyet.com.tr/yazarlar/murat-yetkin/darbe-yolundaki-gizli-yazismalar-bylock-40222697.

7. **Erciş, Emre.** ByLock hizmet vermeyi durdurdu. *Twitter.* [Çevrimiçi] 24 Şubat 2017. [Alıntı Tarihi: 16 Mart 2017.] https://twitter.com/EmreErcis1/status/835371695804383232.

8. **Gazete Vatan.** FETÖ'ye bir darbe daha! Mesut Yılmazer yakalandı. *Gazete Vatan.* [Çevrimiçi] 10 Eylük 2016. [Alıntı Tarihi: 15 Mart 2017.] http://www.gazetevatan.com/feto-ye-bir-darbe-daha-mesut-yilmazer-yakalandi-985253-gundem/.

9. **Köseoğlu, Ersin.** Avukatın ilginç bylock savunması. *Adaletbiz.* [Çevrimiçi] 4 Mart 2017. [Alıntı Tarihi: 15 Mart 2017.] http://www.adaletbiz.com/ceza-hukuku/avukatin-ilginc-bylock-savunmasi-h135138.html.

10. **Cryptii.** *Cryptii.* [Çevrimiçi] https://cryptii.com/text/md5.

11. **Open Security Research.** Brute Force Calculator. *Open Security Research.* [Çevrimiçi] Open Security Research. [Alıntı Tarihi: 11 Mart 2017.] http://calc.opensecurityresearch.com.

12. **MİT.** 2937. *MİT.* [Çevrimiçi] [Alıntı Tarihi: 18 Mart 2017.] https://www.mit.gov.tr/2937.pdf.

13. **Elibol, Nuri.** TSK'da halen 10 bin Bylock'çu var. *MermurlarNet.* [Çevrimiçi] 28 Şubat 2017. [Alıntı Tarihi: 15 Mart 2017.] http://www.memurlar.net/haber/649724/.

14. **Yüksel, Mevlüt.** BySok. *Takvim.* [Çevrimiçi] 30 Ocak 2017. [Alıntı Tarihi: 13 Mart 2017.] http://www.takvim.com.tr/guncel/2017/01/30/bysok.

15. *GoDaddy.* [Çevrimiçi] www.godaddy.com.

16. **Dişkaya, Neşet.** 122 bin kişinin telefonunda ByLock çıktı. *HaberTürk.* [Çevrimiçi] 1 Mart 2017. [Alıntı Tarihi: 13 Mart 2017.] http://www.haberturk.com/gundem/haber/1408800-122-bin-kisinin-telefonunda-bylock-cikti.

17. **Erciş, Emre.** Bylock Mesajları. *Twitter.* [Çevrimiçi] 13 Mart 2017. [Alıntı Tarihi: 16 Mart 2017.] https://twitter.com/EmreErcis1/status/841235407840903168.

18. **Sabah.** İşte örgüt içi izdivaç kepazeliği. *Sabah.* [Çevrimiçi] 18 Ocak 2017. [Alıntı Tarihi: 16 Mart 2017.] http://www.sabah.com.tr/gundem/2017/01/18/iste-orgut-ici-izdivac-kepazeligi.

19. **Ipligence.** Bulk IP address location. *Ipligence.* [Çevrimiçi] [Alıntı Tarihi: 16 Mart 2017.] http://www.ipligence.com/iplocation.

20. **BULK SEO TOOLS.** Bulk IP to location lookup. *BULK SEO TOOLS.* [Çevrimiçi] [Alıntı Tarihi: 16 Mart 2017.] http://www.bulkseotools.com/bulk-ip-to-location.php.

21. **Ofluoğlu, Rahmi.** Bylock davalarında önemli gelişme. *Adaletbiz.* [Çevrimiçi] 19 Mart 2017. [Alıntı Tarihi: 20 Mart 2017.] http://www.adaletbiz.com/ceza-hukuku/bylock-davalarinda-onemli-gelisme-h139479.html.

22. **BBC Türkçe.** Bir yazım hatasıyla pedofil ilan edildi, hayatı değişti. *BBC Türkçe.* [Çevrimiçi] 22 Mart 2017. [Alıntı Tarihi: 22 Mart 2017.] http://www.bbc.com/turkce/haberler-39343504.

23. **Dilipak, Abdurrahman.** Kim FETÖ'cü kim değil? *Yeni Akit.* [Çevrimiçi] 30 Ağustos 2016. [Alıntı Tarihi: 13 Mart 2017.] http://www.yeniakit.com.tr/yazarlar/abdurrahman-dilipak/kim-fetocu-kim-degil-16292.html.

24. **Erciş, Emre.** Ömer Halisdemir. *Twitter.* [Çevrimiçi] 11 Şubat 2017. [Alıntı Tarihi: 15 Mart 2017.] https://twitter.com/emreercis1/status/830385054496989184.

25. **ByLock Meselesi.** Bylock Uygulamasının İndirilmesinin Suç Olmadığının İzahı. *ByLock Meselesi.* [Çevrimiçi] 7 Şubat 2017. [Alıntı Tarihi: 20 Mart 2017.] https://bylockmeselesi.wordpress.com/2017/02/07/bylock-uygulamasinin-indirilmesinin-suc-olmadiginin-izahi/.

26. —. ByLock Kullanıcılarının tespitinde hukuka aykırı delil elde edilmesi. *ByLock Meselesi.* [Çevrimiçi] 7 Şubat 2017. [Alıntı Tarihi: 20 Mart 2017.] https://bylockmeselesi.wordpress.com/2017/02/07/bylock-kullanicilarinin-tespitinde-hukuka-aykiri-delil-elde-edilmesi/.

27. **Hukuk Haber.** Bylock'tan Tutuklanan BM Hakimi: "FETÖ'cü Değil Masonum". *Hukuk Haber.* [Çevrimiçi] [Alıntı Tarihi: 30 Aralık 2016.] https://www.hukukhaber.com.tr/bylocktantutuklananbmhakimifetocudegilmasonum-224857.html .

EKLER

1. İstanbul Emniyet Müdürlüğü'nün, ekinde, "*ByLock modülü ile ilgili bilgiler PVSK Ek 7. Madde kapsamında ve istihbari mahiyette olduğundan hukuki delil niteliği taşımamaktadır. Bu nedenle haricen delillendirilmedikçe yapılacak adli ve idari işlemlerde bizzat gerekçe teşkil etmez.*" notu düşülmüş, 21.10.2016 tarih ve 35920 sayılı yazısı. (2 Sayfa).
2. Milli İstihbarat Teşkilatı Müsteşarlığı'nın, "*Müsteşarlığımıza pek çok kaynaktan gelen bilgi ve belgelerin değerlendirilmesi ve yorumlanması neticesinde hazırlanarak ilgili makam ve kurumlara gönderilen istihbari bilgi ve belgelerin delil olarak kullanılması da mümkün değildir*" değerlendirmesinin yapıldığı, 23.12.2008 tarih ve 477 sayısı yazısı (1 sayfa).
3. Hatay İkinci Ağır Ceza Mahkemesinin 20.09.2016 tarihli kararı (2 Sayfa).
4. Fethullahçı Terör Örgütünün (FETÖ/PDY) 15 Temmuz 2016 Tarihli Darbe Girişimi ile Bu Terör Örgütünün FaaliyetlerininTüm Yönleriyle Araştırılarak Alınması Gereken Önlemlerin Belirlenmesi Amacıyla Kurulan Meclis Araştırma Komisyonu'nun 27.10.2016 tarihli tutanağın 22. sayfası (1 Sayfa).
5. Polisin, çocuk fotoğraflarını paylaşan kişinin IP adresini yazarken bir rakamı yanlış yazması sonucu, Nigel Lang ve eşi "çocukların uygunsuz fotoğraflarını yayma" iddiasıyla gözaltına alınması haberi (4 Sayfa).
6. Log tablosundaki IP'lerin Engellenen IP blokları içerisinde olup olmadığı sorgusu (1 Sayfa).