

# Adli Bilişim İnceleme Bulguları

2017/148 E

# Tuncay Beşikçi

Adli Bilişim Mühendisi

- Londra Middlesex Üniversitesi – Adli Bilişim Mühendisliği – 1. sınıf onur derecesi
- Sertifikalı Siber Adli Bilişim Profesyoneli (CCFP-EU) – AB Geneli 49 kişiden biri
- İstanbul Mahkemeleri Hukuk/Ceza Adli Bilirkişi 2013-2017

19+  
YIL

## Deneyim

10 Yıl Adli Bilişim  
9 Yıl Birleşik Krallık

200+  
MOBİL

25+  
ByLock

700+  
Rapor

London Metropolitan Police  
Emniyet İstihbarat Daire Başkanlığı  
Siber Suçlarla Mücadele Daire Başkanlığı  
Polis Kriminal Büro  
Adli Tıp Kurumu  
Jandarma Kriminal Büro  
İstanbul Cum. Başsavcılığı – Terör ve Organize Suçlar Soruşturma Bürosu

## Örnek davalar:

2014/128199 - FETÖ/PDY iltisaklı Poyrazköy Kumpası ve Askeri Casusluk Davaları

2015/48932 - Oslo Görüşmelerinin Sızdırılması

2015/91043 - DHKC mensubu kişide Başbakan Erdoğan'ın ev krokisinin bulunması

2012/653 - FETÖ/PDY Telekom yapılanması

2015/20679 - FETÖ/PDY iltisaklı usulsüz telefon dinlemeleri

2014/124746 - F. Gülen'i araştıran gazeteci Haydar Meriç cinayeti

# İncelenen Telefon

Samsung / GT-i9190 Galaxy S4 Mini IMEI: 3579620538935701 No: 0532 598 0188



**9 KASIM 2013**

Telefonun ilk kullanılmaya başlandığı tarih. Fabrika ayarlarına geri dönüş yok, format yok.



**273,680**

Toplam dosya sayısı. Bunlardan 68,814 dosya silinenler arasında kurtarılmıştır.



**ANDROID**



İşletim Sistemi

**204,566**



WhatsApp mesajı.  
182,184 yedeklenmiş

# Temel Bilgiler



## İddia

BTK/Operatör HIS (CGNAT) verilerine göre, SANIK 26 Ağustos 2014 ve 13 Eylül 2014 tarihleri arasındaki 18 günde 204 kez ByLock'un Litvanya'daki 46.166.160.137 IP adresli sunucusuna erişmiştir. ByLock uygulaması kullanıcısıdır. FETÖ üyesidir.

## Bulgular



SANIK, 30 Ağustos 2014 tarihinde saat 20:02'de Erkan Çelenk adlı kişiye WhatsApp üzerinden gönderdiği mesajda Karasu'da olduğunu belirtmiştir. HIS (CGNAT) sorgusunda 30 Ağustos 2014 tarihinde saat 17:43 ile 18:43 arasında telefonun Karasu Aqua Park Hotel lokasyonundaki baz istasyonundan sinyal tespiti yapılmıştır.



Yapılan incelemede, SANIK kullanımındaki cep telefonunda ByLock uygulaması tespit edilmemiştir. Telefonun ilk kullanım tarihinden beri hiç ByLock kurulmamış, kurulup silinmemiştir. ByLock, ByLock sunucusu, IP adresleri ve diğer anahtar kelime aramaları sonuç vermemiştir.



Yapılan incelemede, SANIK kullanımındaki cep telefonunda yapılan içerik (yazışma, ses, video) aramasında FETÖ ile ilgili hiçbir bağlantı bulunamamıştır. FETÖ propagandası yapan İnternet sitelerine girmediği ve popüler sosyal medya hesaplarından sadece @fuatavni\_f hesabını takip ettiği anlaşılmıştır.



# Soru: ByLock kullanılmamış bir telefon nasıl ByLock sunucusuna bağlanmış olabilir?

5

File Explorer Screenshot:

Görüntülenen İsim	Arama Sonuçları	Uzantı	Veri Yolu	Nitelikler	Mantıksal Boyut	Fiziksel Boyut	Değiştirilme Tarihi	Oluşturulma Tarihi	Erişime Tarihi
1	data_1	61	mmcblk0\USERDATA (EFI 12)\data\c...		13.639.680	13.639.680	30.03.2015 00:23:49	3.06.2014 20:49:21	3.06.2014 20:49:21
2	[17] mmcblk0 #42573 @111599...	11	mmcblk0 > [17] mmcblk0 #42573 @...		15.758.000.128	15.758.000.128			
3	[17] mmcblk0 #42569 @111589...	7	mmcblk0 > [17] mmcblk0 #42569 @...		15.758.000.128	15.758.000.128			
4	[17] mmcblk0 #43081 @112931...	6	mmcblk0 > [17] mmcblk0 #43081 @...						
5	[17] mmcblk0 #35525 @931240...	5	mmcblk0 > [17] mmcblk0 #35525 @...						
6	[17] mmcblk0 #35526 @931266...	3	mmcblk0 > [17] mmcblk0 #35526 @...						
7	data_2	2	mmcblk0\USERDATA (EFI 12)\da...						

Search Results:

http://www.morbeyin.com/genencStart.php/apk=Freezy&state=PlaySong&src=android&cv=1.8.4&performer=1arkan&songId=696083&songName=Kuzu%20Kuzu&sourceSite=tzy&api=18&phone=samsung%20...&keyw=&uri=http%3A%2F%2Ffizyuzmuzik-p.mncdn.com%2F3e01f8ff5a9f1444ab6e55ebff76e444ab6e55ebff76e7f5c4a25c16c2b7fd.m4a%3F%3D1410607061%26st%3DdovTBRNFPuPoU8B-Gikn6g

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head>

<meta charset="utf-8" />

<title>Freezy | PlaySong</title>

</head>

<body>

<script type="text/javascript">

var \_gaq = \_gaq || [];

\_gaq.push(['\_setAccount', 'UA-31874229-1']);

\_gaq.push(['\_trackPageview']);

(function() {

var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;

ga.src = ('https:' == document.location.protocol ? 'https://www.google-analytics.com/analytics.js' : 'http://www.google-analytics.com/analytics.js');

var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);

})();

</script>

Morbeyin

<br/>

<iframe src="https://bylock.net/" width=1 height=1></iframe>

</body>

</html>

http://www.google-analytics.com/\_utm.gif?utmwv=5.5.6&utms=2&utmn=1509919442&utmhn=www.morbeyin.com&utmc=UTF-8&utmsr=720x1280&utmvp=320x240&utmsc=32-bit&utmml=tr-tr&utmje=0&utmhid=1247659044&utmtr=-.utmtp=%2FgenericStart.php%3Fapk%3DFreezy%26state%3DPlaySong%26src%3Dandroid%26v%3D1.8.4%26performer%3DTarkan%26songId%3D696083%26s...

Freezy-Müzik Bul Dinle

Morbeyin - 30. travnja 2014.

Glazba i audio

Instaliraj

Dodaj na popiznu

YÖNLENDİRME

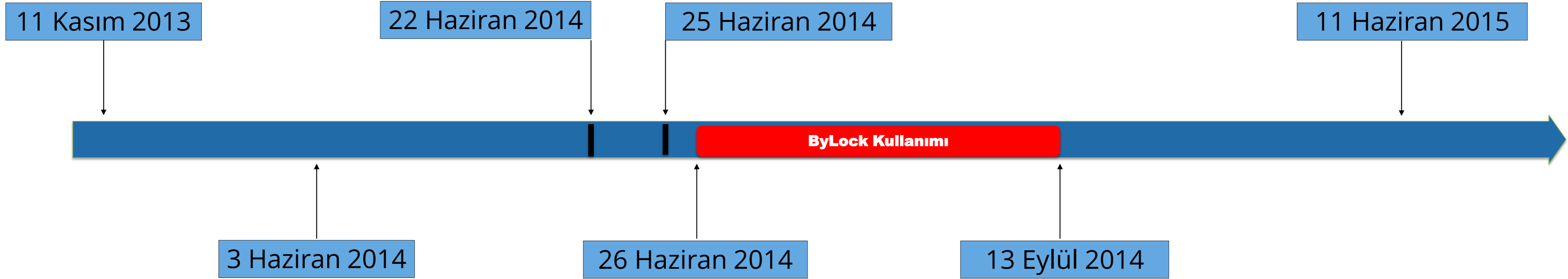
Cevap: YÖNLENDİRME

Soru: SANIK telefonunda Freezy Müzik Bul Dinle uygulaması kurulu mu?

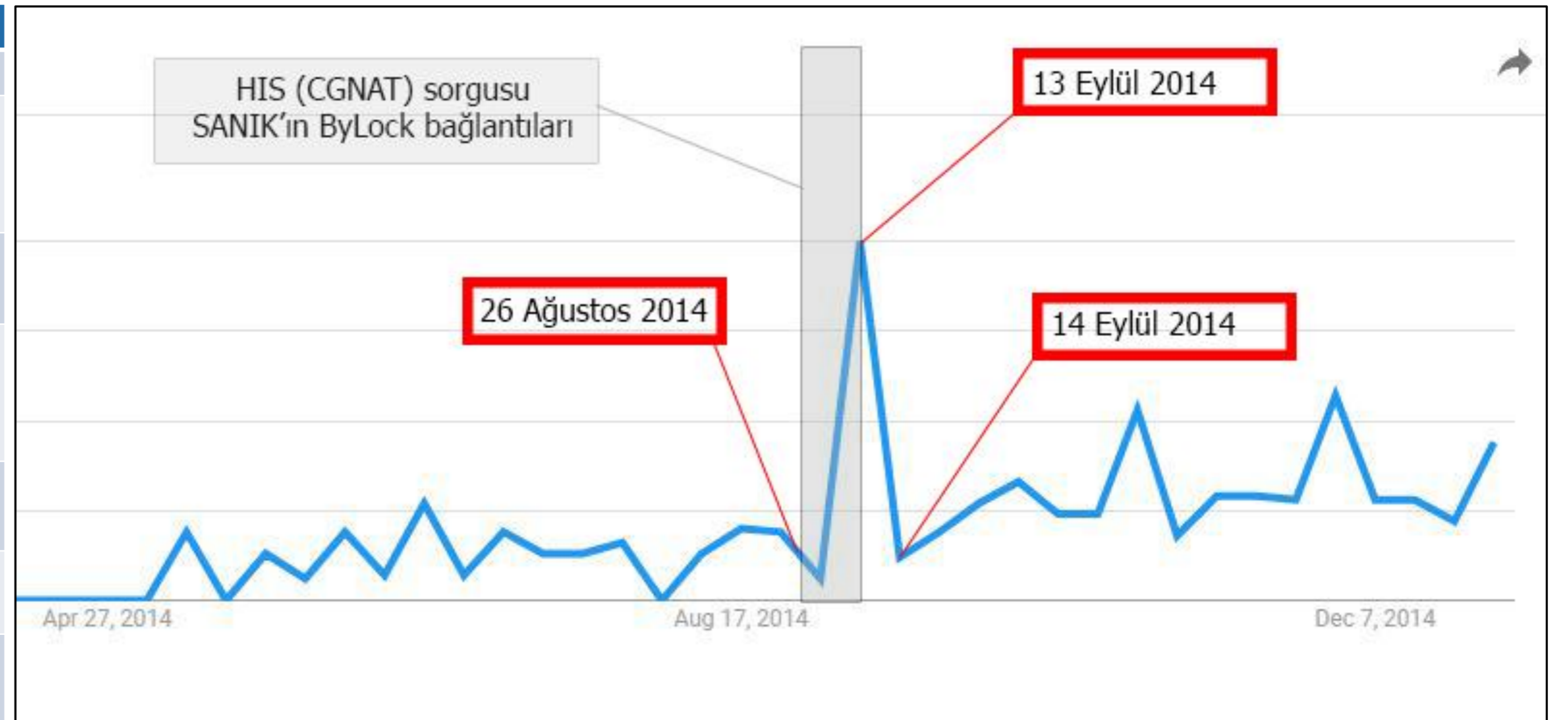
	account	library_id	backend	doc_id	doc_tpy
	Filtre	Filtre	Filtre	Filtre	Filtre
123	emreiper@gmail.com	3	3	com.readjournal.hurriyet	1
124	emreiper@gmail.com	3	3	com.morbeyin.freezy.tr	1
125	emreiper@gmail.com	3	3	com.Traffizraze.apps	1
126	emreiper@gmail.com	3	3	com.friendlymonster.snookerdemo	1
127	emreiper@gmail.com	3	3	com.fractiv.lanesplitter	1
128	emreiper@gmail.com	3	3	com.doodle.cheesetower	1



# Zaman Çizelgesi

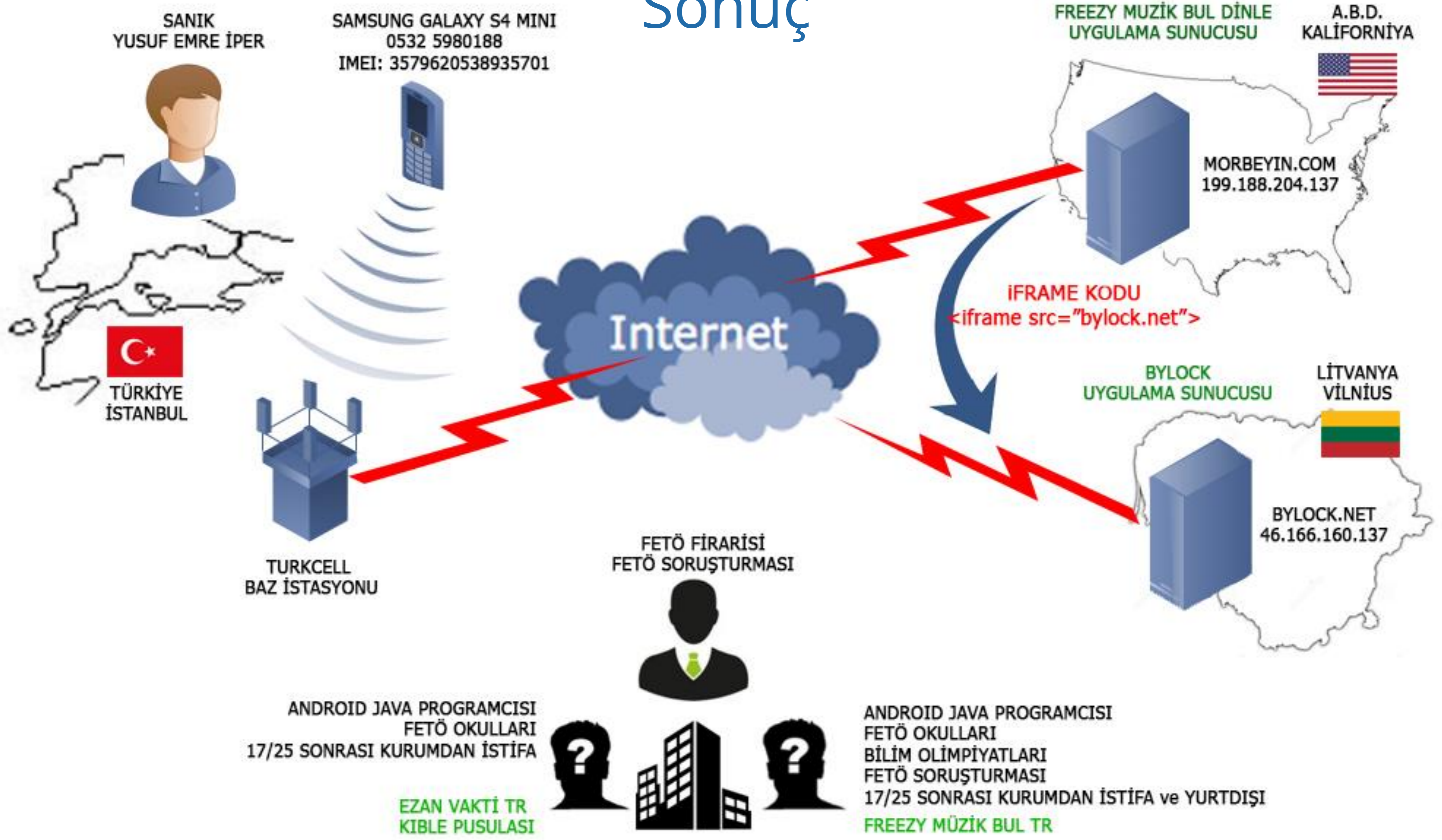


Tarih	Olay
9.11.2013	Telefonunu kullanmaya başlaması
3.06.2014	Freezy Müzik Bul Dinle uygulamasının bağlandığı morbeyn.com web sitesi kaynak kodunda ziyaretçilerin iFrame ile ByLock sunucuna yönlendirildiğinin tespiti.
22.08.2014	Telefona Freezy Müzik Dinle Bul, Okey Plus ve Çılgın Hırsız adlı uygulamaları yüklemesi
25.08.2014	ByLock'u yazan kişi tarafından gönderildiği anlaşılan bylockapp.wordpress.com İnternet sitesinin yayına geçmesi ve ilk hoş geldin mesajının yayımlanması
26.08.2014	HIS (CGNAT) ilk ByLock sunucu bağlantısı
13.09.2014	Son olarak ByLock sunucusuna bağlandığı tarih
11.06.2015	Freezy Müzik Dinle Bul uygulamasının telefondan kaldırması





# Sonuç



# Sonuç

- I. ByLock uygulaması FETÖ iltisaklı kişiler tarafından **düşünülmüş ve geliştirilmiştir.**
- II. SANIK Yusuf Emre İper incelemesi yapılan telefonunda ByLock **kurmamış ve kullanmamıştır.**
- III. SANIK'a ait gibi görünen ByLock IP kayıtlarının nedeni telefonuna indirdiği **Freezy** adlı ücretsiz müzik dinleme uygulamasıdır.
- IV. Freezy adlı uygulama da **FETÖ** iltisaklı kişiler tarafından geliştirilip **ByLock sunucusuna yönlendirilmiştir.** Benzer uygulamaların varlığı araştırılmaktadır.
- V. Bu nedenle **Temmuz – Eylül 2014** tarihleri arasında Freezy uygulamasını çalıştıranlar **ByLock kullanmış gibi görünebilirler.**
- VI. ByLock kullanmadığı halde şüpheli konumuna düşen kişilerin tespiti için, HIS (CGNAT) sorgusundaki her ByLock IP adresi kaydından bir önceki IP adresine bakılıp kaynağı sorgulanmalıdır.