Adli Bilişim İnceleme Bulguları

2017/148 E

Tuncay Beşikçi

31 Ekim 2017

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 arasından 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.

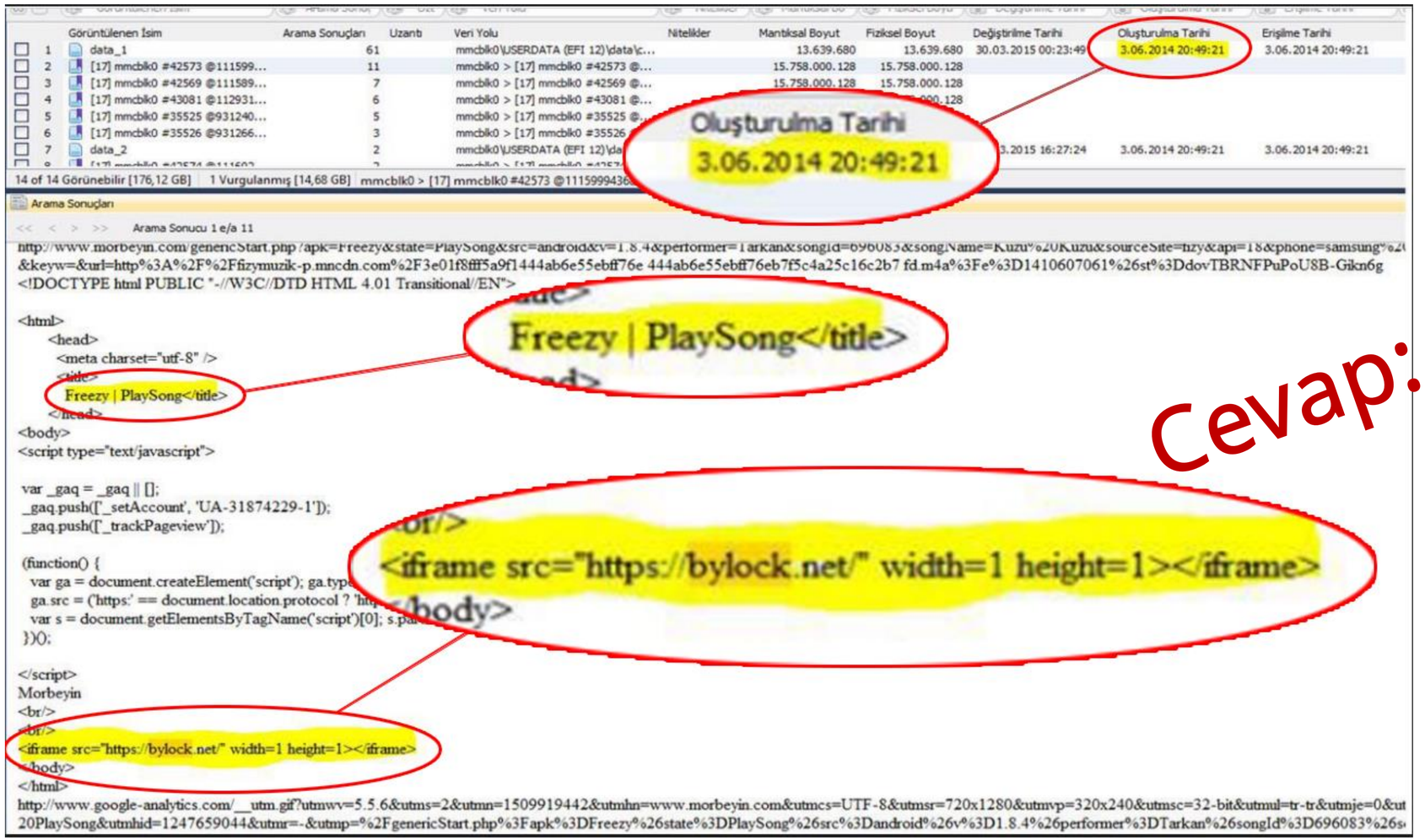
Bulgular

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?

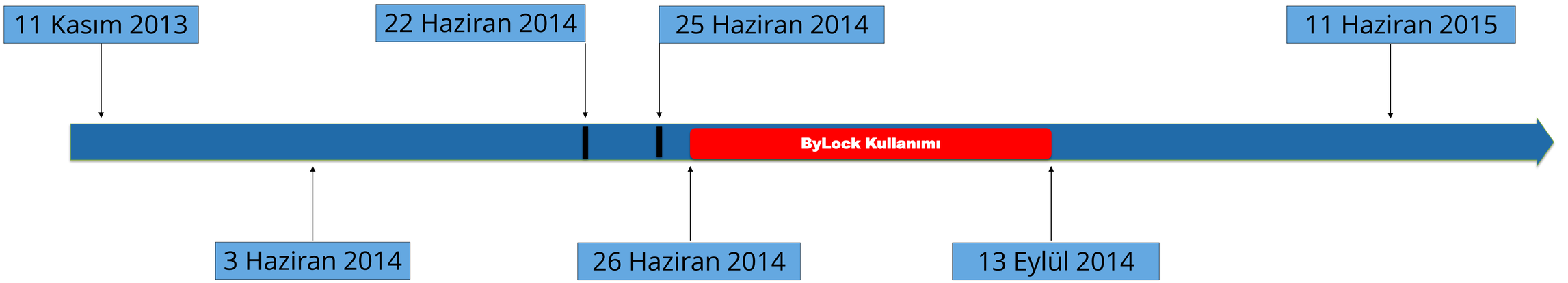


Cevap: YÖNLENDİRME

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

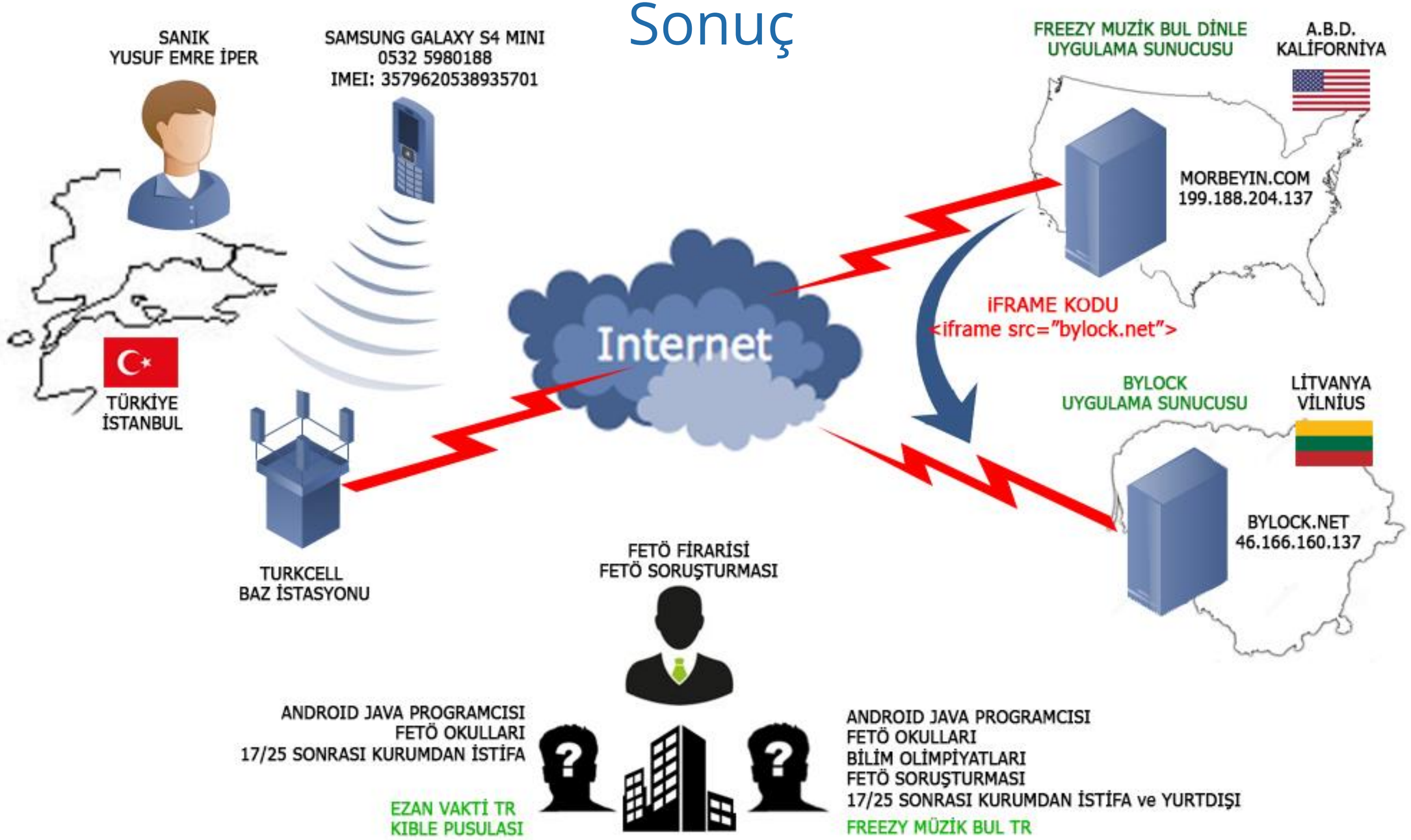
	account	library_id	backend	doc_id	doc_typ
	Filtre	Filtre	Filtre	Filtre	Filtre
123	emreiper@gmail.com	3	3	com.readjournal.hurriyet	1
124	emreiper@gmail.com	3	3	com.morbeyin.freezy.tr	1
125	emreiper@gmail.com	3	3	com.Traffizraze.apps	1
126	emreiper@gmail.com	3	3	com.friendlymonster.snookerdemo	1
127	emreiper@gmail.com	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 morbeyin.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


SANIK
YUSUF EMRE İPER
SAMSUNG GALAXY S4 MINI
0532 5980188
IMEI: 3579620538935701
FREEZY MUZİK BUL DİNLE
UYGULAMA SUNUCUSU
A.B.D.
KALİFORNİYA
MORBEYIN.COM
199.188.204.137
İFRAME KODU
<iframe src="bylock.net">
Internet
TÜRKİYE
İSTANBUL
TURKCELL
BAZ İSTASYONU
BYLOCK
UYGULAMA SUNUCUSU
LİTVANYA
VİLNİUS
BYLOCK.NET
46.166.160.137
FETÖ FİRARİSİ
FETÖ SORUŞTURMASI
ANDROID JAVA PROGRAMCISI
FETÖ OKULLARI
17/25 SONRASI KURUMDAN İSTİFA
EZAN VAKTİ TR
KIBLE PUSULASI
ANDROID JAVA PROGRAMCISI
FETÖ OKULLARI
BİLİM OLİMPİYATLARI
FETÖ SORUŞTURMASI
17/25 SONRASI KURUMDAN İSTİFA ve YURTDIŞI
FREEZY MÜZİK BUL TR

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.