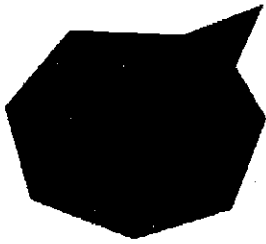


**BYLock Uygulaması**  
**Teknik Raporu**

**Lock**<sup>by</sup>



TANIMLAR ve KISALTMALAR .....	4
1.GİRİŞ .....	9
2. BYLOCK UYGULAMASI .....	9
2.1 Uygulamanın Özellikleri .....	9
2.2 Bylock Uygulamasına Kayıt Olma İşlemi .....	10
2.3. Bylock Sürümleri .....	10
2.4 Bylock Uygulamasını Global ve Ticari Anlık Mesajlaşma (Instant Messaging - IM) Uygulamalarından Ayrık Farklılıklar .....	11
3. BYLOCK UYGULAMASINA YÖNELİK TEKNİK ÇALIŞMALAR .....	12
3.1 Dayanak ve Yöntem .....	12
3.2 Bylock Uygulaması IP/Alan Adı Analizi .....	12
3.3 Bylock Uygulamasına İlişkin Açık Kaynak Tespitleri .....	14
3.4. Kriptografik Protokol Analizi ve Tersine Mühendislik Çalışması .....	16
3.4.1 Kriptografik Protokol Analizi .....	16
3.4.2 Tersine Mühendislik Çalışmaları .....	18
3.5 Sunucuya Yönelik Teknik Çalışmalar .....	21
3.5.1 Uygulamanın İşleyiş Şeması .....	21
3.5.2 Uygulama Sunucusunun Vazımlı Modelleri .....	21
3.5.3 Uygulama Sunucusunda Çalışan Yazılımlarda Rastlanan Türkçe İfade .....	21
3.5.4 Uygulamanın Sunucusunu Yöneten Şahsın Faaliyetlerine Yönelik Tespitler .....	22
3.5.5 Uygulama Sunucusuna Ortadoğu IP Adreslerinden Erişimin Engellenmesi .....	25
3.6. Bylock Uygulama Sunucusu Verileri .....	27
3.6.1 Sunucudan Elde Edilen Veri Tabanı Dosyaları .....	27
3.6.2 Bylock Uygulamasına Ait Veri Tabanı Deseni ve Özellikleri .....	27
3.7 Bylock Uygulamasına Ait İstatistik Veriler .....	52
4. DEĞERLENDİRME ve SONUÇ .....	53
5. EKLER .....	57
EK-1: Bylock Uygulamasının Versiyon Tarihleri .....	58
EK-2: Bylock Uygulamasının Google Play'den Yaklaşık İndirime Sayısı .....	59
EK-3: Bylock Sunucusuna Ait Sertifikanın Ekran Görüntüsü .....	60
EK-4: Bylock Sunucusu IP Adreslerine İlişkin virustotal.com Sorgusu .....	61
EK-5: Kaynak kodlarda Geçen Türkçe İfadeler .....	62
EK-6: İstemci Kaynak kodlarında Geçen Kriptografik Algoritmalar .....	65

EK-7: Kayıt ve İki Kullanıcı Arasındaki Şifreli Mesajlaşmaya Ait Akış Şeması .....	69
EK-8: Uygulama Sunucusu Yazılım Modelleri .....	70
EK-9: Uygulama Sunucusunda Çalışan Yazılımda Rastlanan Türkçe İfade .....	75
EK-10: Uygulama Sunucusunda Engellenen IP Adresleri Listesi .....	79
EK-11: Çözümlenen Şifrelere İlişkin İstatistikî Veriler .....	85



TANIMLAR ve KISALTMALAR

- Ag : Birden fazla sayıdaki bilgisayarın birbirlerine bağlanarak haberleşmesini sağlayan iletişim ortamı
- Ag Analizi : Bir yazılımın bilgisayar ağları üzerinde gerçekleştirdiği iletişimin incelenmesi ve yorumlanması işlemi
- Ag topolojisi : Bir ağı oluşturan bilgisayar ve diğer ağ bileşenlerinin yapılandırmasının tarihi
- Alan adı (domain) : IP adreslerinin insanların hatırlayabileceği kelime ve harf gruplarıyla eşleştirilerek İnternet üzerinde ilgili sunucuya erişim kolaylığı sağlayan adres
- Android : Akıllı telefon ve tablet bilgisayarlarda çalışmak üzere tasarlanmış, geliştirilmesine Google'in öncülük ettiği açık kaynaklı işletim sistemi
- Asimetrik Şifreleme : Gizli ve açık olarak nitelendirilen iki adet anahtar barındıran, açık anahtar ile şifrelenen verimin yalnızca gizli anahtar kullanılarak deşifre edilebileceği şifreleme yöntemlerine verilen ad (Açık Anahtarlı Şifreleme)
- Bulanıklaştırma : Yazılım üzerinde tersine mühendislik yapılmasını zorlaştırmak için yazılımın kaynak kodundan program haline dönüştürülmesi aşamasında karmaşıklık ilave etme yöntemlerine verilen ad
- Censys.io : IPv4 adres sistemindeki tüm adresleri günlük olarak tarayıp elde edilen verimin sorgulanmasını sağlayan web arama motoru

DNS : Alan adlarının hangi IP adres(ler)ine karşılık geldiğinin sorgulanmasına yarayan çözümleme sistemi

Google Play : Android yükli telefonlara yönelik geliştirilen uygulamaların sunulduğu resmi uygulama marketi

Hata Ayıklama : Yazılımları kontrolü bir biçimde adımlara bölerek geliştirerek barındırdıkları hataları bulmak için kullanılan bir yöntem. Tersine mühendislik çalışmalarında yazılımın hangi işlemleri gerçekleştirdiğini takip etmek ve dolayısıyla işleyiş şekline dair detaylı bilgi elde etmek için kullanılmaktadır

HTTPS Güvenlik Protokolü : HTTP protokolü üzerinde uçtan uca şifreleme sağlayan protokol

IOS : Akıllı telefon ve tablet bilgisayarlarda çalışmak üzere Apple tarafından geliştirilen işletim sistemi

IP Adresi : İnternet ağına doğrudan bağlanan her cihazın verilen, numaralardan oluşan benzersiz adres

IPv4 : 1 ile 255 değerleri arasındaki 4 adet sayı ile ifade edilen, teorik olarak 4 milyardan fazla adres sağlayabilen adresleme sistemi

ISS : İnternet Servis Sağlayıcı

Kaynak Kod : Yazılımın geliştirici tarafından yazıldığı, geliştirilebilir bir programa dönüştürmesi için belirli aşamalardan geçmesi gereken kodlar/yazılar bütünü.

Kriptografik Özet Fonksiyonu : Girdi olarak verilen değişken boyutlu veriyi belirli boyutlu bir özet değerine dönüştüren

kriptografik matematiksel fonksiyonlara verilen ad. Bu fonksiyonlar verideki 1 bit degerinin deęiřmesi gibi küçük farklılıklarda bile  zet fonksiyon iktisinde b y k  lekli farklılıklara sebebiyet verecek ve aynı ıktıyı verecek girdileri bulmanın neredeyse imk nsız olacaęı bir Őekilde tasarlanır.

: Bilgisayar sistemlerinde gerekleřtirilen iřlemlerin kayıtları

Parola/Anahatar

: Bir sistemde yetki kontrol  yahut veri Őifrelenmesi gibi amalar iin kullanılmak  zere belirlenen, sembol (harf, sayı, bit vb.) dizisi.

Port

: Internet  zerinden bilgisayara ulařtırılan verinin bilgisayarda iřleneceęi uygulamayı bildiren numara

PTRR

: DNS sunucularında IP adresinden ilgili domain(ler)in sorgulanmasına olanak saęlayan kayıt tipi

ptrarchive.com

: DNS sunucularındaki PTR kayıtlarını arřıvleyerek gemiře d n k arama yaptıran bir web arama motoru

Simetrik Őifreleme

: Tek bir anahatar kullanılarak Őifrelenen verinin yalnızca tekrar aynı anahatar kullanılarak deřifre edilebileceęi Őifreleme y ntemlerine verilen ad.

SSL

: Internet  zerinde g venli iletiřim kurmayı saęlayan bir Őifreleme protokol  (Secure Sockets Layer)

SSL Sertifikası

: SSL protokol nde iletiřimin tarafların birbiriyle kimlięinden emin olması iin kullanılan, genellikle iki tarafın ortak olarak g vendięi bir Sertifika Otoritesi tarafından verilmiř olan sertifika

Sunucu (Server) : İnternet üzerinde kendisine ulaşan istekleri değerlendirilen ve yanıtlayan bilgisayar

Şifre : Şifreleme işlemi kullanılan yöntem ve yapıların her birine verilen ad

Şifreleme : Bir verinin bir parola/anahtar kullanılarak, yalnızca tekrar aynı parola/anahtar kullanılarak açılabilir şekilde, matematiksel belirli yöntemler kullanılarak anlamsız hale getirilmesi.

Tersine Mühendislik : Bir uygulamanın derlenmiş hâlinde kaynak kodlarını ve/veya uygulamanın işleyiş yordamlarını elde etmeye yönelik olarak gerçekleştirilen teknik çalışma

TLS : Eski adı SSL olan bu şifreleme yönteminin adının ağırlıklı olarak TLS, İnternet gibi IP üzerine kurulumuş bilgisayar ağlarında iletişim için uçlar arasında gerçekleştirilen kriptografik şifreleme yaparak gerçekleştirilen iletişimin uçlar arasında trafiğin geçtiği noktalarda anlamlandırılabilir bir şekilde olmasını sağlar. (Transport Layer Security)

UML : Bir uygulamanın bileşen yapısını, çalışma şekillerini vb. grafikler şeklinde raporlamakta kullanılan modelleme standardı (Unified Modelling Language)

Uygulama Paketi : Bir uygulamayı oluşturan tüm dosyaları barındıran, ilgili işletim sistemi üzerine yüklenelidir durumdaki dosya

virusotal.com : Kullanıcılar tarafından kendisine gönderilen dosya, uygulama paketi ve internet adresleri üzerinde



analizler yapıp sonuçlar üzerinde aramalar yapılımasını sağlayan web arama motoru

: Aralarında yerel ağ kuruluması imkânı bulunmayan bilgisayarlar arasında İnternet üzerinden sanal şifreleme ile bağlantımın güvenliğini sağlayan protokollerin genel adı

whois.domaintools.com : İnternetteki alan adları ve IP adresleri üzerinde birçok analiz ve sorgulamalar yapmayı sağlayan web sitesi

VPN

Arkadaş ekleme işlemi, anılan uygulamaya kayıt olurken kullanıcı tarafından belirlenen ve "Kullanıcı Adı (Kodu/Rumuz)" olarak isimlendirilen şahsa özel kodun girilmesi suretiyle gerçekleştirilmektedir. Uygulama üzerinden telefon numarası veya "ad soyad" bilgileryle arama yapılarak kullanıcı eklenmesine imkan bulunmamaktadır. Diğer taraftan, ByLock'da, muadil veya yaygın mesajlaşma uygulamalarında bulunan; telefon rehberindeki kişilerin uygulamaya otomatik olarak eklenmesi özelliği bulunmamaktadır.

özellikleri mevcuttur.

- Kriptolu anlık mesajlaşma,
- Kriptolu sesli görüşme,
- Grup mesajlaşmaları,
- Dosya paylaşımı,
- E-posta iletimi,
- Arkadaş ekleme

Google Play'de 2014 yılının başlarında kullanıma sunulan ve 2016 yılının ilk aylarına kadar geçitli versiyonlarla kullanılan ByLock uygulamasında;

## 2.1 Uygulamanın Özellikleri

## 2. BYLOCK UYGULAMASI

Fetullahçı Terör Örgütü/Paralel Devlet Yapılanması FETÖ/PDY üyelerince, akıllı telefonlara yüklenen kriptolu bir haberleşme aracı olan "ByLock(ByLock: Chat and Talk)" adlı mobil uygulama üzerinden iletişim kurulduğuna dair bilgilerin istihbar olunması üzerine, konuyla alakalı kapsamlı bir çalışma yürütülmüştür. Bu kapsamda, gerek ByLock mobil uygulamasi gerekse iletişim kurduğu uygulama sunucuları ayrıntılı teknik çalışmalara tabi tutulmuştur. Bu çalışmalarda uygulamanın teknik tasarımına, mimarisine, işleyişine, aynı işlevi gören uygulamalarla benzer ve farklı yönlerine, kullanıcı profiline ilişkin hususlar ele alınmıştır.

## 1. GİRİŞ

Kullanıcıların birbirleriyle ByLock uygulaması üzerinden iletişime geçebilmeleri için tarafların birbirlerinin "Kullanıcı Adı/Kodu" bilgilerini bilmeleri ve her iki tarafın diğerini arkadaş olarak eklemesi gerekmektedir.

## 2.2 ByLock Uygulamasına Kayıt Olma İşlemi

Uygulamada gerçekleştirilen kullanıcı kayıt işlemi esnasında,

- Kullanıcıdan telefon numarası ya da e-posta adresi talep edilmeyeceği,
- Sadece bir kullanıcı adı ve parola üretmesinin istendiği,
- "SMS" mesajı ya da arama ile doğrulama yapılmadığı,
- Kullanıcı adı ve parola girildikten sonra, kullanıcıdan talep edilen bilgiler ile (ekranda rastgele parmak hareketleri yaptırılarak vb. yöntemlerle) bir kriptografik anahtar üretildiği

tespit edilmiştir.

## 2.3. ByLock Sürümleri

Uygulamanın, Android işletim sistemi üzerinde çalışan "1 serisi" ve "2 serisi" olarak adlandırılabilen iki temel sürümü bulunmaktadır. 2 serisi aynı zamanda "ByLock++" olarak da adlandırılmış olup, Google Play'de farklı bir sayfadan yeni bir uygulama gibi sunulmuştur.

1 serisi sürümlerin en sonucusu olan "ByLock 1.1.7" 2014 yılının Aralık ayında güncellendiği anlaşılmaktadır. Daha sonraki süreçte, ByLock++ (2 serisi) piyasaya sürülmüş, uygulama Google Play'den kaldırılana kadar bu sürüm kullanıma sunulmaya devam edilmiştir. Versiyonların yaklaşık tarihlerini gösteren ekran görüntüsü Ek-1'de, uygulamanın Google Play'den yaklaşık indirilme sayılarına ilişkin ekran görüntüsü Ek-2'de sunulmuştur.

2.4 ByLock Uygulamasını Global ve Ticari Anlık Mesajlaşma (Instant Messaging - IM) Uygulamalarından Ayrılan Farklılıklar

Anlık mesajlaşma uygulamalarının göçü, kullanıcılar arasında kolay kullanım özelliği sunmaktadır. ByLock uygulamasında ise, uygulamayı kullanan şahıs, iletişim kurmak istediği şahsa ait "Kullanıcı Adı" bilgisine sahip değilse, bu kişi ile iletişim kuramaz.

Anlık mesajlaşma uygulamaları, kullanıcılarına hızlı iletişim imkanı sunar. ByLock uygulamasını kullanan bir şahıs uygulamayı telefonuna indirmediğinde, rehberindeki diğer şahısların uygulamayı kullanıp kullanmadığını görememekte, şahıslar ile doğrudan iletişime geçememektedir.

Anlık mesajlaşma uygulamalarının göçü, reklam vb. servisler ile uygulamaların olabildiğince çok kullanıcı tarafından kullanılmasını sağlamak suretiyle uygulamaların 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.

Anlık mesajlaşma uygulamalarında, şahıslar sosyal çevresiyle günlük ve günlük rutinlerle ilgili iletişime geçmektedir. ByLock uygulamasındaki iletişim ağı ve içerikler incelendiğinde ise, örgütsel amaç ve temalı bir kullanım görülmektedir.



## 3. BYLOCK UYGULAMASINA YÖNELİK TEKNİK ÇALIŞMALAR

## 3.1 Dayanak ve Yöntem

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 gelişme usul, prensip ve tekniklerini kullanabileceği (i) bendinde ise Milli İstihbarat Teşkilatı "dış istihbarat, milli 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.

Söz konusu kanuni 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. Yine işbu rapor bünyesinde, kendi imkânlarının ifşa olmaması adına, eğer açık kaynaklı bir veri, veri tabanı ve araçlar üzerinden izah/teyit imkanı varsa, doğrulama amacıyla kullanılabilircek bir takım hususlara Teşkilatın kendi imkanlarına atıfta bulunulmadan yer verilmiştir.

Devletin teknik istihbarat faaliyetlerine ilişkin imkân ve kabiliyetlerin ağıca çıkarılmaması ve istihbarata karşı koyma amacıyla, verilerin temin edilmesine ilişkin hassas yöntem, usul ve araçlara yer verilmemiştir. Bu amaçla, sadece raporun kapsamına girmesi gerektiği değerlendirilen hususlara değinilmiştir.

## 3.2 ByLock Uygulaması IP/Alan Adı Analizi

Söz konusu uygulamaya ait internet trafiğinin incelenmesi neticesinde, ByLock uygulamasının sunucu sistemine çoğunlukla **doğrudan** IP adresi üzerinden erişildiği, bazı sürümlerde ise (Örn. ByLock 1.1.3 sürümü) "*bylock.net*" alan adı üzerinden aynı sunucuya bağlanmak suretiyle iletişim kurulduğu görülmüştür.

Uygulamamın bağlandığı IP adreslerinin tespit edilmesi amacıyla farklı zamanlarda tekrarlanan testlerde, uygulamamın farklı sürümlerinin farklı birer IP adresine bağlandığı görülmüştür. Uygulama sunucusunda geliştiricisinin uygulamaya özgü oluşturup imzaladığı bir sertifika (self-signed SSL certificate) ile HTTPS güvenli protokolü kullanıldığı görülmüştür. Ayrıca tespit edilen sertifikaya yönelik çalışmalar neticesinde Litvanya'da sunucu kiralama hizmeti veren "Baltic Servers" isimli firmaya tahsisli 9 adet IP adresinin ByLock uygulamasının güvenli sürümlerince kullanıldığı tespit edilmiştir:

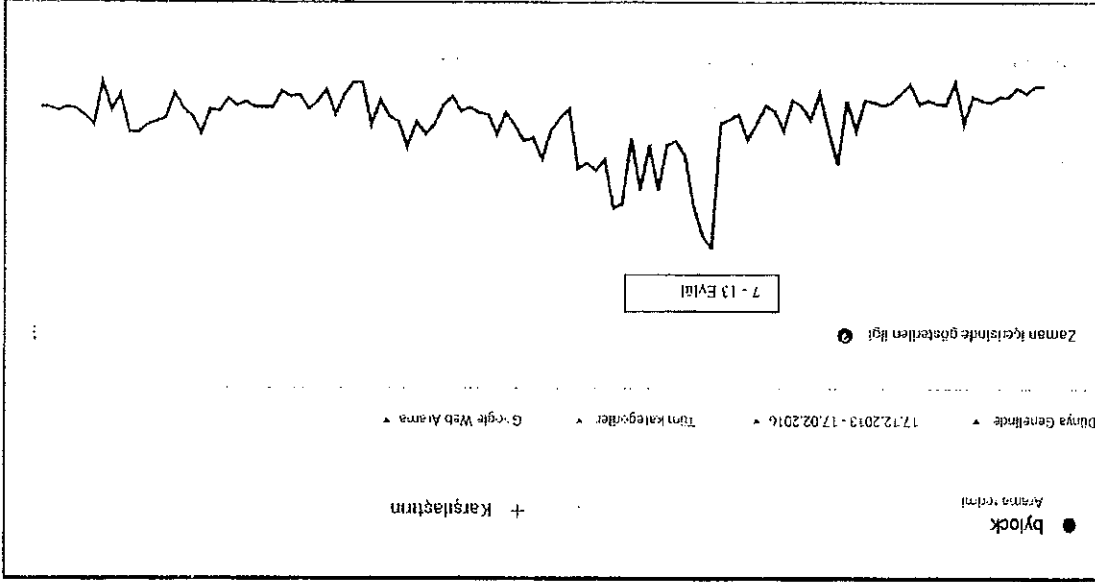
→ 46.166.160.137	→ 46.166.164.178	→ 46.166.164.181
→ 46.166.164.176	→ 46.166.164.179	→ 46.166.164.182
→ 46.166.164.177	→ 46.166.164.180	→ 46.166.164.183

'censys.io' isimli web sitesinde (söz konusu sitede tüm IPv4 adres uzayını kapsayan, geçmişe dönük genişli taramalar ve bunların sonuçlarına ait veriler sunulmaktadır) yayımlanan bilgiler kullanılarak çalışma teyit edilmiştir. ByLock hakkında elde edilen verilerin doğrulanması için 'censys.io' sitesinden örnek olarak Ocak 2016 tarihine ait SSL/TLS protokolü için 443/TCP portlarına yönelik yapılan tarama verileri indirilmiş, bu veri üzerinde yapılan aramada ByLock sunucusu için hazırlanan TLS sertifikaları aranmıştır. Arama sonucunda yukarıda listelenen 9 adet IP adresine ait TLS sertifikaları bulunmuştur. Bulunan sertifikalardan birine ait ekran görüntüsü örnek olarak EK-3'de sunulmuştur. Söz konusu sertifikamın "David Keynes" adıyla oluşturulduğu görülmüştür.

Tespit edilen IP adreslerinin incelenmesi kapsamında bu IP adreslerinin ByLock'un etkin olduğu tarihlerde hangi alan adı veya adları ile ilişkilendirildiği sorgulanmıştır. Bu kapsamda 1 Eylül 2015 – 9 Ekim 2016 tarihleri arasında alınan IP adreslerinden yalnızca 46.166.160.137 adresinin bylock.net alan adı ile kullanıldığı, diğer IP adreslerinin herhangi bir alan adı ile eşleşmediği bulgusuna ulaşılmıştır. Açık kaynaklarda yapılan araştırmalardan çıkan sonuçlar da bu durumu destekler niteliktedir. virustotal.com, whois.domaintools.com, ptrarchive.com gibi web sitelerinde yapılan sorgulamalarda ByLock sunucularının aktif olduğu dönemde ait başka bir alan adı kullanılmamıştır. (EK-4)

## 3.3 ByLock Uygulamasına İlişkin Açık Kaynak Tespitleri

15 Temmuz 2016 tarihinden öncesine dair olarak "ByLock" uygulamasına ilişkin açık kaynaklarda yürütülen muhtelif araştırmalar neticesinde; "ByLock" uygulamasının, Google Play ve Apple AppStore uygulama marketlerinden yayından kaldırılmasının ardından, uygulama kurulum dosyalarına erişimin, APK indirme siteleri üzerinde, hangi versiyonun hangi zaman aralığı için sunucu tarafından desteklendiği ve çalışır vaziyette olduğu ayrı bir çalışmanın konusu olmakla birlikte, devam ettiği tespit edilmiş olup arama motorlarında "ByLock" kelime aramalarına ilişkin istatistikler ve karşılaştırmalar aşağıda grafiksel olarak sunulmuştur:



"ByLock" Arama İstatistikleri (Türkiye)

17 Aralık 2013 ve 17 Şubat 2016 tarihleri arasında "ByLock" anahtar kelimesi kullanılarak yapılan Google aramaları incelendiğinde; aramaların 7 - 13 Eylül 2014 tarih aralığında tavan yaptığı, 2015 yılının başlarında inişe geçtiği ve sonraki süreçte de tekrar yükselişe geçmediği belirlenmiştir.



gibi hususlar bir arada değerlendirildiğinde, indirme sayılarının uygulama sunucusu üzerinde olduğu görülen 215.092 adet kullanıcı sayısıyla uyumsuz olmadığı değerlendirilmektedir. Nitekim tüm çalışmalarda bilinçli veya bilinçsiz 'indirme' değil

- Farklı bir cihaza kurulması
- İndirilip kullanıcı oluşturul(a)maması,
- Uygulamanın, cihazdan silinip tekrar yüklenmesi,

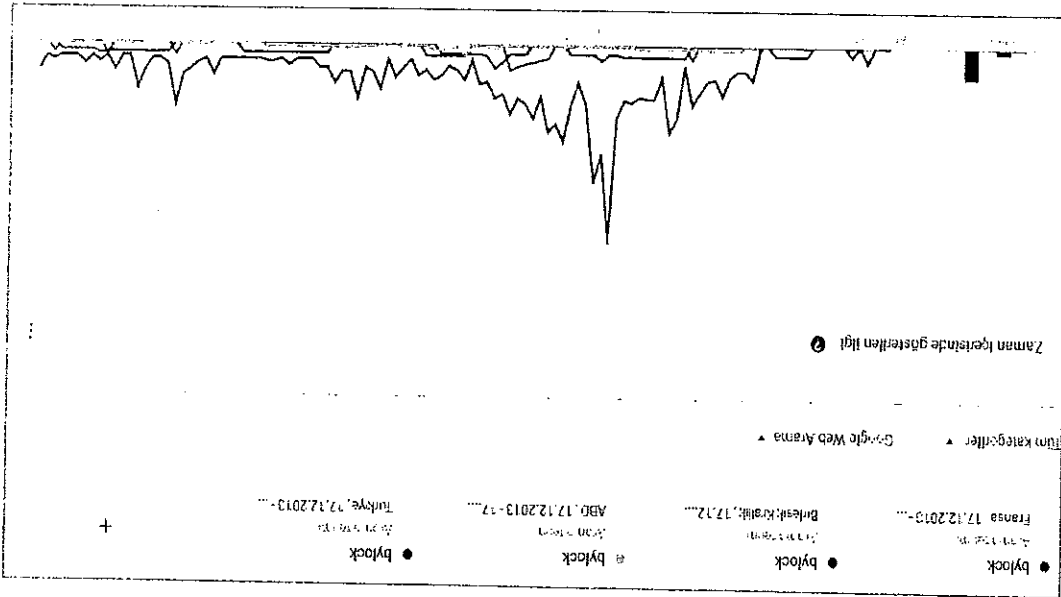
rakamlara ulaşıldığı varsayılabilir;

istatistiklerinin, ne ölçüde doğru sayıyı ifade ettiği teyit edilememekte birlikte, bu APK indirme sitelerinde yer alan 500.000 - 1 milyon adet indirme

gerçekleştirildiği değerlendirilmektedir.

mensupları tarafından veya Türk kullanıcılar tarafından VPN bağlantısı ile kaynaklı olduğu, diğer ülkelerden yapılan aramaların da örgütün yabancı ülkelerdeki olmakla birlikte anılan uygulamaya ilişkin aramaların neredeyse tamamının Türkiye incelendiğinde, Türkiye dışında Fransa, İngiltere ve ABD'nin yer aldığı tespit edilmiş "ByLock" uygulamasına ilişkin dünya genelinde yapılan aramalar

### "ByLock" Arama İstatistikleri (Dünya)



kullanma durumu irdelenmiştir. Dolayısıyla, muhtelif indirme rakamlarından ziyade, anılan 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 (gerçek kimliklerine bu rapor da yer verilmemiştir) FETÖ/PDY'ye müzahir şahıslar olduklarının, kamuya yansımada önce uygulamayı bildiklerinin ve yaygın şekilde kullanıldıklarının göstergesi olarak değerlendirilmiştir.

"ByLock" uygulamasına yönelik olarak yapılan açık kaynak çalışmalarında;

- Anılan uygulamanın 15 Temmuz 2016 tarihinden önce, belirli sayıda olmak üzere, Twitter dışındaki çok az platformda yer aldığı,
- Eksi Sözlük, Uıudag Sözlük, İnci Sözlük gibi güncel konuların ve kavramların yoğun olarak paylaşıldığı ve tartışıldığı platformlarda, 15 Temmuz 2016 tarihinden öncesine ait herhangi bir bilgiye rastlanmamıştır.

Toplumda ve hatta teknik konularla ilgili insanlar arasından bilinirliği yok denebilecek seviyedeyken, istatistikler göz önünde bulundurulduğunda; diğer ülkelere kıyasla Türkiye'den kullanım değerlerinin açık farkı yüksek olması (diğer tüm ülkelerin toplamından çok daha fazla) uygulamanın amacı hakkında fikir veren en önemli unsurlar arasında görülmektedir.

### 3.4. Kriptografik Protokol Analizi ve Tersine Mühendislik Çalışması

#### 3.4.1 Kriptografik Protokol Analizi

Çalışmanın bu bölümünde "ByLock" uygulamasının istemcisi ve sunucusu arasındaki haberleşme ağ analizi yapılmıştır. Yapılan bu analizle istemci ve sunucu arasındaki ağ trafiği "IP" paketi seviyesinde ele alınmış olup, bu paketlerin yapısı, kullanılan protokol katmanları, içerdiği verilerin tespiti ve bu verilerin şifreli olup olmadıklarının belirlenmesi amaçlanmıştır. Ağ analizi işlemi, burada yer verilen uygulamamın 4 farklı sürümü üzerinde ayrı ayrı tekrarlanmıştır.

Uygulamanın ağ trafiği incelendiğinde bahse konu uygulamanın "TCP" katmanında şifreleme sağlayan "TLS" (Transport Layer Security) kriptografik protokolünü kullandığı tespit edilmiştir. Test ortamında, istemci tarafından gönderilen isteklerin ve sunucudan istemciye dönen cevapların çözümü "TLS" şifrelemesinin çözümlenebilmesiyle sağlanmıştır.

"ByLock" uygulamasının istemcisinin kayıt aşamasında "XML" biçiminde gönderdiği mesajın çözümlenmesi sonucunda mesaj içeriğinde,

- Kullanıcıya ait özel bir kayıt numarası,
- Kullanıcı adı,
- Kullanıcı parolasının kriptografik özet fonksiyonu (cryptographic hash function) çıktısı,
- Gizli anahtarın (private exponent) şifrelenmiş hali,
- Açık anahtarlı şifreleme (public key encryption) değışkeni olan taban değeri (modulus),
- Uygulamanın hangi işletim sistemi sürümünde çalışmakta olduğu,
- Kullanıcının bulunduğu saat dilimi,

bilgilerinin bulunduğu gözlemlenmiştir. Gözlemlenen mesaj yapısına dair fikir vermesi için içeriği kısıllanmış olan bir mesaj örneği aşağıda sunulmuştur:

```
<?xml version="1.0" encoding="UTF-8"?>
<request id="">
  <userId>0</userId>
  <username>CIKARILMISTIR</username>
  <password>183B...6786</password>
  <privateExponent>gg3g...9yx0</privateExponent>
  <modulus>A78K...U7bk</modulus>
  <edition>android</edition>
  <tzid>Europe/Istanbul</tzid>
  <audioV2>1</audioV2>
</request>
```

asğıdaki tabloda sunulmuştur.

adlandırılmıştır.) ve toplam kod dosyası sayısı ile kod satır sayısı kütüphaneleri hariç diğer kodlar, uygulama özetindeki (UÖ) kodlar olarak

- Uygulamanın 4 ayrı sürümüne dair "uygulama özetindeki (UÖ)" (Kod tespit edilmiştir.
- "ByLock" uygulamasının, "androidsupport", "android-telechooser" ve "googlegms" (sadece 1.1.6 sürümü için) kod kütüphanelerini kullandığı

tespitler asğıda sunulmuştur:

Kaynak kodların kurulum dosyasından elde edilmesi çalışması sonucunda bahse konu bulanıklaştırılmış kaynak kodları üzerinde yapılan incelemeler neticesindeki

uygulamanın kaynak kodlarının güvenliğini sağlamak amaçlanmıştır.

çok zamanını alarak işi zorlaştırmak, karışıklık yaratmak aynı zamanda da değişken isimleri gizlenerek, tersine mühendislik ile statik analiz yapacak kişinin daha Bulanıklaştırma yöntemi ile kaynak kodlarda kullanılan sınıf isimleri, yordam isimleri, olan bulanıklaştırma (obfuscation) yönteminin kullandığı gözlemlenmiştir. sırasında "Android" uygulama geliştiricileri tarafından sıkça uygulanan bir yöntem kodları üzerinden analizler yapılmıştır. Söz konusu kaynak kodların incelenmesi kodları "small" dosyaları halinde elde edilmiştir. Elde edilen bu "small" kaynak biçiminde olan kaynak kodları (sadece akıllı telefonlar için derlenebilir ve anlaşılabilir aracılığıyla "ByLock" uygulamasının ele alınan sürümlerinin "dalvik bytecode" uygulamaları için geliştirilmiş bir disassembler yazılımı kullanılmıştır. Bu yazılım "ByLock" uygulamasının kaynak kodlarını elde edebilmek amacıyla "Android"

### 3.4.2.1 Statik Analiz

mühendislik analizleri gerçekleştirilmiştir.

verilen 4 farklı sürümünün kurulum dosyalarına yönelik statik ve dinamik tersine

"ByLock" uygulamasının, "Android" işletim sisteminde çalışan ve burada yer

### 3.4.2 Tersine Mühendislik Çalışmaları



- İstemci kaynak kodlarında yer alan kriptografik algoritmalara ilişkin bölümler Ek-6'da sunulmuştur.
- Asimetrik gizli anahtarın ise simetrik yapılı bir blok şifreleme algoritması olan "AES/CBC/PKCS5Padding" ile şifrelenmesiyle ilgili gözlemlenmiştir.
- Veriler gizli anahtar olmaksızın çözülmemektedir.
- Algoritmaların şifreleme yapmaktadır. Açık anahtar kullanılarak şifrelenen algoritması olup, biri gizli diğeri açık olmak kaydıyla iki adet anahtar kriptografik algoritma bir tür açık anahtar/asimetrik şifreleme algoritması kullanılarak şifrelenmiştir. Söz konusu kriptografik algoritma "RSA/ECB/OAEPWithSHA-1andMGF1Padding" kriptografik algoritması kullanılarak şifrelenmiştir. Söz konusu asimetrik algoritma arasında iletilen verilerin 2048 bitlik asimetrik alan adlarının yer aldığı tespit edilmiştir.

- "https://bylock.net:443/SHU-Server"  
- "https://46.166.164.181:443/App-Server"

sirasıyla;

- Uygulamanın 1.1.3 ve 1.1.7 sürümlerine ait kurulum dosyalarında Messaging – GCM) faydalanılmadığı görülmüştür.
- Kullanılmakta olan Google Bulut Mesajlaşması'ndan (Google Cloud tarafından geliştirilen ve yaygın biçimde mobil uygulamalar tarafından iletişime dair kodların mevcut olduğu, fakın bu işlev için Google Uygulamada, mesajlaşmaya dair anlık bildirimlerin (push notification) "Sesli Arama" şeklinde ifadelerin bulunduğu görülmüştür (Ek-5).
- Uygulamanın kaynak kodları içerisinde, Türkçe "Dosya", "Posta" ve

Tablo - 4 ayrı sürüm dair UÖ ve toplam kod dosyası sayısı ile kod satırı sayısı

Sürüm	UÖ için Kod Dosyası Sayısı	Toplam Kod Dosyası Sayısı	UÖK için Kod Satırı Sayısı	Toplam Kod Satırı Sayısı
2.0.0	287	772	74542	184400
1.1.7	288	773	87686	215329
1.1.6	295	1560	88042	383325
1.1.3	288	773	88883	214621

- Uygulamaya kayıt ve iki kullanıcı arasındaki mesajlaşmaya ait kriptografik akış şeması Ek-7'da sunulmuştur.

### 3.4.2.2 Dinamik Analiz

"ByLock" uygulamasının statik analizinin yapılmasının ardından, uygulamanın burada yer verilen 4 ayrı sürümü, diğer bir tersine mühendislik yöntemi olan dinamik analiz ile incelenmiştir.

Uygulamaya kayıt esnasında, kullanıcının belirlemiş olduğu parolanın, "xml" mesajı içerisindeki "password" alanında "MD5" kriptografik özet algoritmasıyla, asimetrik gizli anahtarın (private exponent) ise "privateExponent" alanında şifreli olarak sunucuya iletildiği tespit edilmiştir.

Söz konusu şifreleme yönteminde;

- Kayıt sırasında giriş ekranına girilen parolanın "SHA-256" kriptografik özet algoritmasından geçirildiği,

- Elde edilen 32 byte uzunluğundaki kriptografik özet değerinin 16 byte'lik iki parçaya ayrılarak kullanıldığı,

- Söz konusu kriptografik özet değerinin ilk 16 byte'lik kısmının "AES/CBC/PKCS5Padding" blok şifreleme algoritması için simetrik gizli

anahtar (secret key) olarak, son 16 byte'lik kısmının ise başlangıç vektörü (initialization vector) olarak kullanılarak, istemci tarafında oluşturulan

asimetrik gizli anahtarın (private key) şifrelediği (Bahse konu asimetrik gizli anahtar her kullanıcı için özel olarak kayıt sırasında üretilerek

haberleşmede kullanılmaktadır.),

- Şifrelenmiş olan bu çıktının "xml" formatlı mesajda "privateExponent"

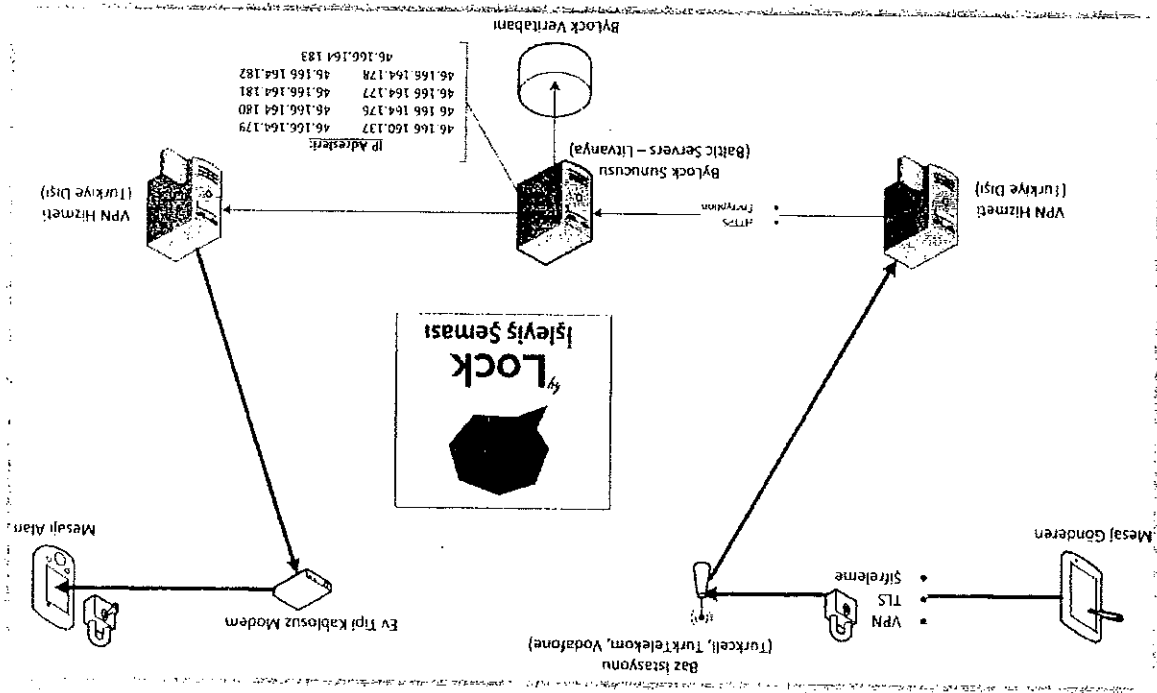
bölümünde yer aldığı

tespit edilmiştir.

## 3.5 Sunucuya Yönelik Teknik Çalışmalar

## 3.5.1 Uygulamanın İşleyiş Şeması

ByLock uygulaması ve uygulamaların sunucularında çalışan yazılımlara ilişkin İşleyiş Şeması aşağıda yer verilmiştir:



## 3.5.2 Uygulama Sunucusunun Yazılım Modelleri

Yürütülen çalışmalar neticesinde, uygulama sunucusundaki yazılım detaylı incelemelere tabii tutulmuş ve söz konusu yazılıma ilişkin yazılım modelleri Ek-8'de sunulmuştur.

## 3.5.3 Uygulama Sunucusunda Çalışan Yazılımla Kastanan Türkiye İfade

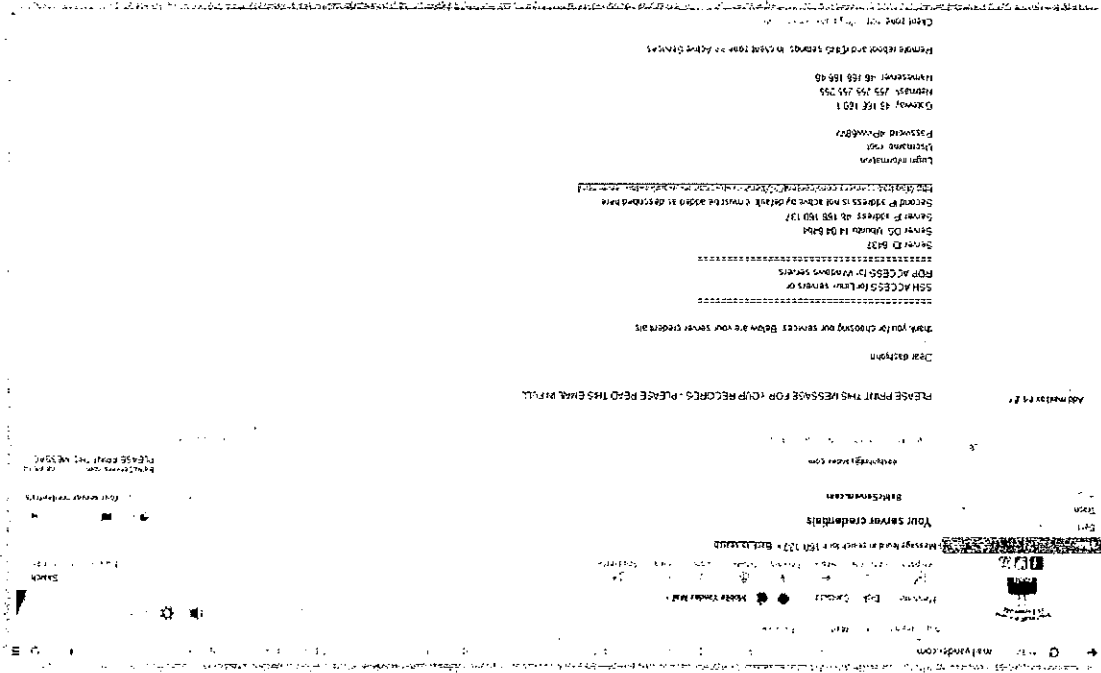
Sunucuda çalışan yazılımların kaynak kodları içerisinde, Türkiye olarak "Yetkiniz Yok" şeklinde bir ifadenin bulunduğu görülmüştür (Ek-9).



### 3.5.4 Uygulamamın Sunucusunu Yöneten Şahsın Faaliyetlerine Yönelik Tespitler

Uygulamamın sunucusunu yöneten şahsın, uygulamamın hizmet verdiği sunucusunu ve IP adreslerini kiralamaya yöntemi ile temin ettiği, söz konusu hizmetlere ait bedelleri aylık ve üç aylık aralıklarla ödediği, bu işlemleri dashjohn@yandex.com adlı elektronik posta adresi üzerinden gerçekleştirildiği tespit edilmiştir.

ByLock uygulamasının, "46.166.160.137" IP adresine sahip sunucu üzerinden hizmet sunduğu görülmüştür. Bahsi geçen sunucusunun dashjohn@yandex.com isimli e-posta adresi kullanılarak kiralandığına dair e-posta içeriğine aşağıda yer verilmiştir. Bahsi geçen sunucusunun, Litvanya'da hizmet veren "Baltic Servers" isimli firmanın kiralandığı sunuculardan biri olduğu görülmüştür.



Uygulamamın sunucusunu yöneticisinin, uygulamamı kullananların tespitini nispeten zorlaştırmak amacıyla 8 adet ilave IP adresi (46.166.164.176, 46.166.164.177, 46.166.164.178, 46.166.164.179, 46.166.164.180, 46.166.164.181, 46.166.164.182, 46.166.164.183) kiralamıştır. Kiralanan IP adreslerine ilişkin elde edilen e-posta içeriğine aşağıda yer verilmiştir.

Compose Check mail Reply Forward Delete Spam Unread Add button

[#OXV-385-5700]: extra ip

tomase@alticervers.com

dashy@yandex.com

Hi,

IP range is ready: 46.166.164.176/29

If you have any additional question, please feel free to contact me: 14/08/24 17:48, Tomas Felciskis

Ticket number: OXV-385-5700

Type: Sales

Status: Open

Level: High

ByLock uygulamasının hizmet verdiği sunucu ve ek IP adreslerinin aylık ve 3 aylık dönemlerde tahakkuk eden faturalara ilişkin elde edilen e-posta içeriklerine aşağıda yer verilmiştir:

**Baltic Servers**

Invoice No: 01-2015-131243

Service provider: UAB DIOMENŲ CENTRAS  
Company code: 145747029  
VAT number: LT145747029  
Address: TIBAS 74-320 Šilutė LT-78140  
Lithuania  
Telephone: +370 700 050 30  
Account number: LT21700010126825917  
SWIFT code: IABAL122  
Bank: AB "Swedbank"

Date issued: 2015-01-19  
Pay until: 2015-02-03

ID	Description	Period	Price	Price total
6437	Custom 2 Xeon 56xx	From: 2015-02-18 To: 2015-03-08	278,00 EUR	330,82 EUR
Total:			278,00 EUR	
VAT:			52,82 EUR	
Total amount:			330,82 EUR	

Not paid

Invoice prepared by hand of customer under agreement from 17.01.14

Bahsi geçen ödemeler incelendiğinde sunucu ve IP adreslerinin 2016 yılı Şubat ayına kadar [dashjohn@yandex.com](mailto:dashjohn@yandex.com) e-posta adresi kullanılarak kayıt olunan anonimlik sağlayan "PaySera" ödeme sistemi vasıtası ile ödemelerinin yapıldığı tespit edilmiştir. Ödemelere ilişkin örnek bir e-posta içeriğine aşağıda yer verilmiştir:

**paySera**

Date: 2014-09-03 03:11:05  
Mokėjimo unikalus numeris: 63531140

Sveik, dashjohn

Svetainėje <https://myballiscervers.com> Jūs sumokėjote 34.96 USD

Atliū, kad naudotais PaySera Pasōme išsaugot šį laišką, nes tai yra ailiū mokėjimo įrodymas.

<b>PARDAVĖJAS</b>	Quomenų centras https://myballiscervers.com +370005030 info@duomenencentras.lt Tiltės g. 74 Šiauliai Lietuva
-------------------	--

<b>PASLAUGOS AR PREKĖS APRAŠYMAS</b>	<b>MOKĖJIMO</b>	<b>SUMA</b>
	<b>BŪDAS</b>	
Užsakymas nr: 108429 https://myballiscervers.com projekte. (Pardavėjas: Duomenų centras)	Cashų sistema	364.96 USD

Mokėdami per PaySera sąskaitą, Jūs galėjote sutaupti. Nuo šio mokėjimo Jums į sąskaitą sugrįžė - 1.14 (17%)

**Atidarykite sąskaitą dabar**

Jei turite klausimų dėl prekių pristatymo, pasiūlytų teikimo arba jei reikalinga sąskaita-faktūra, kreipkitės į pardavėją.  
Telefonu: +370005030  
El. paštu: [info@duomenencentras.lt](mailto:info@duomenencentras.lt)

Visą informaciją apie savo pirkimų istoriją per PaySera galite pamatyti prisijungę prie sistemos.

Jei per keletą kartus nepavyko susisiekti su paslaugos teikėju ar su juo susitanči, prašome pranešti PaySera Klientų aptarnavimo skyriui. Užpildydami kontaktinę formą.

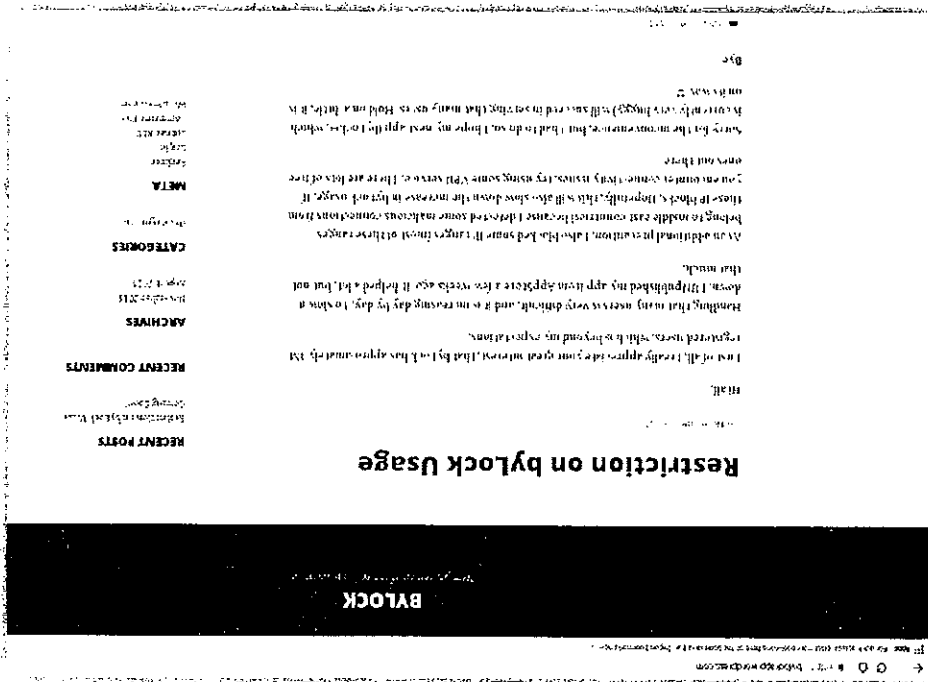
Mes pastengsime padėti išspręsti Jūsų problemą susisiekdami su pardavėju tiesiogiai.

PaySera  
Klientų aptarnavimo skyrius



## 3.5.5 Uygulama Sunucusuna Ortadoğu IP Adreslerinden Erişimin Engellenmesi

15.11.2014 tarihinde ByLock uygulama sunucusunun yöneticisi olduğu değerlendirilen şahıs, uygulama için açtığı "bylockapp.wordpress.com" adresli web sayfasında, Ortadoğu'dan gelen bazı IP adreslerinin uygulamaya erişimini engellediğini duyurmuştur. Uygulama sunucularına yönelik yürütülen teknik incelemeler neticesinde elde edilen bilgilerle, şahsın engelleme işlemini 17.11.2014 tarihinde yaptığı, fakat 15.11.2014 tarihinden önceki erişim log kayıtlarını veri tabanından sildiği tespit edilmiştir. Şahsın konuyla ilgili yazısının ekran görüntüsüne aşağıda yer verilmiştir:



Sunucudan elde edilen bilgiler doğrultusunda, bu engellemeye yönelik çalışmaların bir kısmı, örnek olarak aşağıda sunulmuştur:

```
root@hst-46-166-160-137:~#
iptables -N LOGGING
iptables -A INPUT -s 5.2.80.0/21 -j LOGGING
iptables -A INPUT -s 5.11.128.0/17 -j LOGGING
iptables -A INPUT -s 5.23.120.0/21 -j LOGGING
iptables -A INPUT -s 5.24.0.0/14 -j LOGGING
iptables -A INPUT -s 5.44.80.0/20 -j LOGGING
iptables -A INPUT -s 5.44.144.0/20 -j LOGGING
```

```
iptables -A INPUT -s 5.46.0.0/15 -j LOGGING  
iptables -A INPUT -s 5.63.32.0/19 -j LOGGING
```

Söz konusu şahsın engellediği IP adres blokları Ek-10'da yer almaktadır.

Engelleme işleme 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.

Söz konusu şahsın, IP adreslerini engellemesi neticesinde, Türkiye'deki kullanıcılarının Sanal Özel Ağ (Virtual Private Network - VPN) kullanımını sarti olarak kullanıcı tespitini engellemeye çalıştığı anlaşılmaktadır. Bu yöntem ile uygulamayı kullanmaların tespitinin önüne geçilmesini amaçlayan kurumsal başka bir tedbir alındığı değerlendirilmektedir.

Uygulama sunucusu yöneticisinin gerçekleştirdiği IP engellemesinin, Türkiye'deki kullanıcıların uygulamaya erişimlerini engellemekten ziyade, kullanıcıların VPN kullanılması sonucunda gerçek IP adresleri ile sunucuya bağlanmalarının tespit edilmesini önlemeyi amaçladığı sonucuna varılmaktadır.

### **3.6. ByLock Uygulama Sunucusu Verileri**

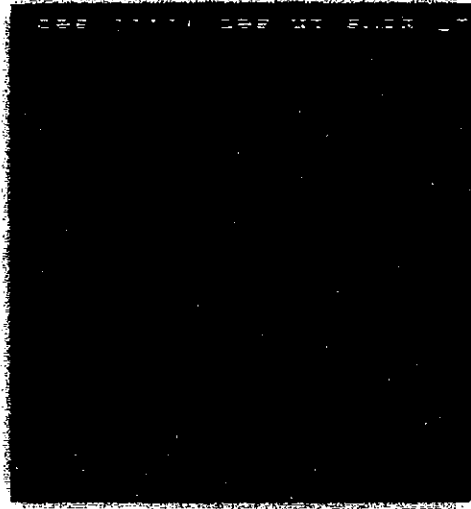
Yürütülen çalışmalar neticesinde, ByLock uygulama sunucusundaki veri tabanı dosyaları, sunucu yöneticisi tarafından girilen komutlar, sunucuda çalışan yazılım dosyaları elde edilmiştir. Ayrıca Türkiye'den sunucuya doğrudan bağlanmasını engelleyen yazılım içerisinde yer alan ve tamamına yakını Türkiye'ye ait olan IP adres blokları elde edilmiştir.

#### **3.6.1 Sunucudan Elde Edilen Veri Tabanı Dosyaları**

ByLock uygulamasına ait verilerin saklandığı **109 GB**'lık veri tabanı dosyası elde edilmiştir. Elde edilen verilerin incelenmesine ilişkin detaylara aşağıda yer verilmiştir:

#### **3.6.2 ByLock Uygulamasına Ait Veri Tabanı Deseni ve Özellikleri**

Veri tabanı dosyaları üzerinde gerçekleştirilen çalışmalar neticesinde, aşağıdaki tablolar elde edilmiştir:



#### **Şekil 3.6.2.1: Uygulamaya ait tablo isimleri**

Elde edilen tabloların veri yapıları ve/veya tablo içeriklerine ilişkin tespit edilen detay bilgilere aşağıda yer verilmiştir:

Action tablosu, kullanıcıların uygulama etkileşimlerinin tutulduğu "log" tablosuyla ilişkilidir. Action tablosunda, "log" tablosundaki "actionId" değerine karşılık gelen "işlem adı" bilgisi tutulmaktadır. Örneğin; actionId=3, kayıt olma işlemi, actionId=1 ise "Add Friend (Arkadaş Ekleme)" işlemi ifade etmektedir. Arkadaş ekleme işlemi sırasında parameter1 değerine her kullanıcıya uygulama sunucusu tarafından atanan UserId kod numarası, parameter2 değerine ise her kullanıcının kayıt olurken oluşturduğu "Kullanıcı Adı" (nickname) bilgilerinin gönderildiği görülmüştür. Uygulamayı kullanan şahısların yapmış oldukları kayıt olma, uygulamaya giriş yapma (Login), Çıgır gerçekleştirme, e-posta iletimi dahil olmak üzere farklı işlemlerin hepsi için Action tablosundaki ilgili işlemin numarasına ve eklenecek değerlere göre bir log kaydı oluşturulmaktadır.

Şekil 3.6.2.2: Action tablosunun alan adları ve özellikleri

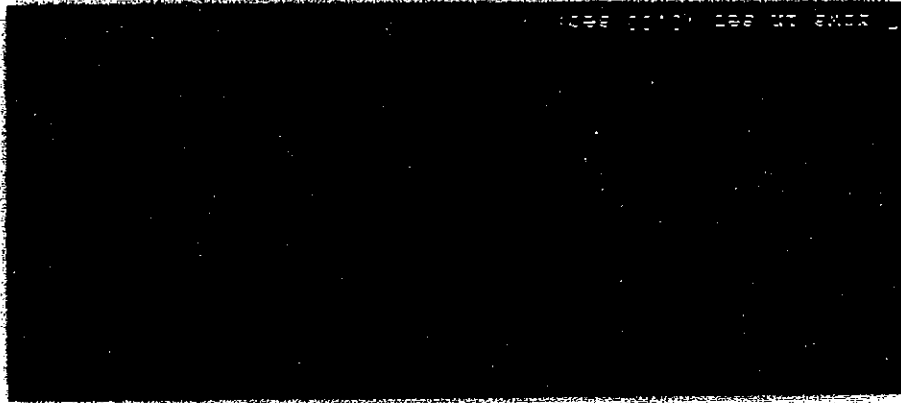


3.6.2.1 "action" tablosu:



Attachment (İlgiik) tablosu, uygulamayı kullanan şahısların e-posta iletişimi sırasında yazdıkları meime ilave ettilikleri dosya, resim vb. farklı formatları içeriklerinin isimlerinin saklandığı tablodur. Attachment tablosunda, 4.675 adet e-posta ekine ait isim bilgisinin kriptolu olarak saklandığı görülmüştür.

Şekil 3.6.2.3: attachment tablosunun alan adları ve özellikleri



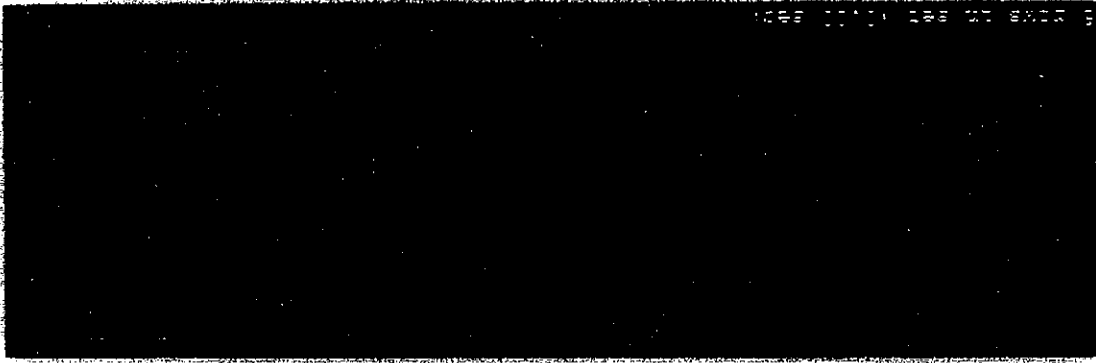
3.6.2.2 "attachment" tablosu:

"call\_history" tablosu, bütün çağrı hareketlerine ilişkin bilgilerin kayıt edildiği tablodur. Uygulamanın sesli çağrı özelliğiyle arama yapıldığında, yapılan çağrıya ilişkin log kaydı "call\_history" tablosunda oluşmaktadır. "call\_history" tablosunda, arayan\_id (callerId), aranan\_id (calleeId), arama\_zamanı (callTime), aramanın başarılı olma durumu (result), görüşme süresi (duration) vb. bilgiler tutulmaktadır. "call\_history" tablosundan elde edilen verilerde toplam 1.218.784 çağrı kaydı bulunmaktadır. Üzeride eşleştirilmesi yapılabilen şahıslara ait elde edilen çağrı hareketlerine ilişkin kayıtlardan, kimlerin, ne zaman ByLock uygulaması üzerinden sesli iletişim kurduğunun tespiti yapılabilmektedir.

**Şekil 3.6.2.4: call\_history tablosuna ait örnek kayıtlar**



3.6.2.3 "call\_history" tablosu:



**Şekil 5: Chat tablosunun alan adları ve özellikleri**

"Chat" tablosu, uygulama vasıtasıyla gerçekleştirilen mesajlaşmalara ait bilgilerin saklandığı tablo olup, uygulamanın sohbet özelliği kullanılarak gönderilen her bir mesaj için; mesajı gönderen kullanıcı, mesajı alan kullanıcı, mesajın şifreli hali, imza, mesajın gönderilme zamanı ve mesajın karşı tarafta okunma zamanı bilgilerinin "chat" tablosunda saklandığı görülmüştür. "chat" tablosundan elde edilen verilerde toplam **17.169.632** kayıt bulunmaktadır.

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. Veri tabanında kriptolu olarak tutulan ve çözümlenen mesaj içeriklerine ait örneklerle aşağıda yer verilmiştir:

GİZLİ

32

kontnuerid : kuberid | ophertid  
363829 34436  
17 Aralık operasyonunda görev olduğundan dolayı 08/12/2015 günü gazihane alındı. O sabah namazdan sonra hanim kahvaltı hazırladı. Kahvaltı yaptikten sonra kapam zeki geldi. Beklenen bir durumda kapam açıldığında pakler, sübriye giymeniz gerekliğin söylerler. Ben hastahandem gıda üyüdüğü için yandırmadan optüm hanimla vedalaştıktan sonra, sokakla bilmene emanet ediyorum Çıdan geri kılıyorum" dedi. Rahat bir şekilde kapamdan çıkerten ben de Alaha emanet olun dedim ve ben akarak birtakım götürüldüm. Gözlerimde olduğunuz son gece hoc üyüdü. Geçen namaz ve duayla geçirdik. Önceki hantırlarım hocamıza bol bol dua ettim. Sabahleyim savcıba sevki olduk ve ben dahil tüm arkadaşlarım serbest kaldık.  
Rabbim emanetimi geri gönderdi.  
Ben yokken eşim yatak odasında his yuyunması, Öuma odasında yurken uyku ile uyumak arası kapam açıldığını duyums. Bakışında Hocamızın biriydi beyaz tabak ve üzünde kol ayağı için emniyetli olan ciltkesiciyle emniyet korunda döşeyip, hanimla birlikte sona yatak odasına doğru gittiğim görüncü hanim uyumak ile yabide ayağı kalkarak hocamıza giriş istikametine bakiyor ama görüyor ve o esnada sabah ezan okunmaya başlıyor.  
Biz Hocamızın ağzından çıkan her kereden emindik. Alaha Şükürler olsun ki Hocamızın bidden emime emniyet denetlemeye gittiği. Akkerm Rabbim bizi de bir araber inşallah. Bunu gözlerinizdeyken daha iyi anladım. He olur duaya devam edelim.

sentime  
2015-12-12 19:21:27  
recevetime  
2015-12-13 01:34:05

Mesaj İçeriği Örneği 1

GİZLİ

GİZLİ

From:Id	To:Id	Content	Time
73605	201087	alk barm res unevre gib	2016-01-24 04:29:46
73605	201087	uygur bosand	2016-01-24 04:30:03
73605	201087	yal bey uygur kars paralic oclugu kon bosandga soylen	2016-01-24 04:31:39
73605	201087	ayrica uygur emnye de barm paralic oclugunu soylen	2016-01-24 04:33:39
73605	201087	emreveler barm soylic	2016-01-24 04:33:56
73605	201087	bassavd tme gutt	2016-01-24 04:33:56
73605	201087	steyman bassavdeh ddu	2016-01-24 04:34:01
73605	201087	yan geln adl	2016-01-24 04:34:25
73605	201087	deha cek var akt de	2016-01-24 04:34:39
73605	201087	bte ni akt	2016-01-24 04:35:00
73605	201087	onu barm kon sube mduru arlat	2016-01-24 04:36:13
73605	201087	save metmet us bun cek e getirdiler evrde	2016-01-24 04:36:25
73605	201087	o da bassavde gordup	2016-01-24 04:36:28
73605	201087	lde etme	2016-01-24 04:36:34
73605	201087	kon sube mduru omer koosam odama gelp barm arlat	2016-01-24 04:37:07
73605	201087	ne ypatm dgor bu esdele evrak lade edimes dogru mu dgor	2016-01-24 04:38:25
73605	201087	alk bassavde ,metmet demir og, uygur meylan ,hasan res onumuzde hafta yokat	2016-01-24 04:39:10
73605	201087	ire ayrtdk	2016-01-24 04:39:20
73605	201087	steyman kendur spot etmek: savor	2016-01-24 04:40:06
73605	201087	alk barm arlat: yok operasyon kon steyman biddi diye belyum	2016-01-24 04:42:27
73605	201087	ok akt ben yan geln gormeym	2016-01-24 04:44:33
73605	201087	alk barm arlat: dardan barm biddemaya scrk edetirse ne yokat	2016-01-24 04:45:47
73605	201087	m	2016-01-24 04:46:50
73605	201087	ok akt	2016-01-24 04:46:50
73605	201087	alk yetliya basvuraym ni	2016-01-24 04:47:23

Mesaj İçeriği Özetli 2

GİZLİ













GİZLİ

edilmektedir.)

Yükarıdaki mesaj içeriklerindeki son dört satır, henüz çözümlememiş mesaj örneğidir. (Çözümleme çalışmalarına devam

from:sender	to:recipient	subject	date	time
6605	1382	NTN	2015-11-03	14:08:48
6605	1382	ram beyi hat beye senin de olduğun bir yerde (yemek) tanıştım..fahri abi de olacak...hat beye konuşabiliriz...	2015-11-03	20:10:13
6605	1382	birim	2015-11-03	14:11:01
6605	1382	gönderdiğin mektap neydi...hamza beye	2015-11-12	22:28:48
6605	1382	ben burun ne diye deniydim...şu an düşünedim	2015-11-12	16:29:25
6605	1382	17500 o başka bir yerde ki	2015-11-12	22:34:29
6605	1382	düşünüyüm	2015-11-12	16:34:25
6605	1382	birim	2015-11-12	22:36:13
6605	1382	evet..şimdi bilgisayarında daha indirdi mi?	2015-11-12	22:38:07
6605	1382	herde bulduğunuz parmak fiş de yanlış..zaten yalın bilyer	2015-11-12	22:38:44
6605	1382	benim için gerek yok..sen benim..2 saatte öğreniyorsun	2015-11-12	16:39:42
6605	1382	okur	2015-11-12	16:44:57
6605	1382	yanın ki kiti dosyalar ne zaman geliyor...	2015-12-02	14:31:59
6605	1382	bedd yorum	2015-12-02	14:33:37
6605	1382	nyee...	2015-12-09	17:15:49
6605	1382	/33+0KkKcKZTbEDHfJbBfLpGfPmYhSkXU171CL2+HbZHER78LlUoZQhKruVQAbQaHE+nHb5XhONiBOvKQdMmWStGH78PbYwSPYarjB...	2015-12-15	18:31:36
6605	1382	/zvqKQNF+J15mEMfRtqgULmPDAkEzVhVdYV/ZBRU2CUj/ZmYqUvBxKOvY4kU/s9qVWdKQSZAJj5c38WkMfZ3UuHGOxJ7Y663SSCOgac...	2015-12-15	12:33:41
6605	1382	/agcDkxUocqgh9TzEdaBdUs4w4ZVMnTmKlEjEgUuZkHmYgUarF5mEhD1H5b6L5KQK2gOPRQgZmPdkXOP4bqkZopf...	2015-12-15	22:32:36
6605	1382	/ZkqH000QUSW+7MBGwuhNk/cOh86oAcU7mJbdmULBYHfFTeIG+AOl3PR8jvDkVMW1K3vDpZGf10WthEhFfKULtUeZvzd4HdHfL...	2015-12-16	04:42:31

Mesaj İçeriği Örneği 6

GİZLİ

3.6.2.5 "client" tablosu:

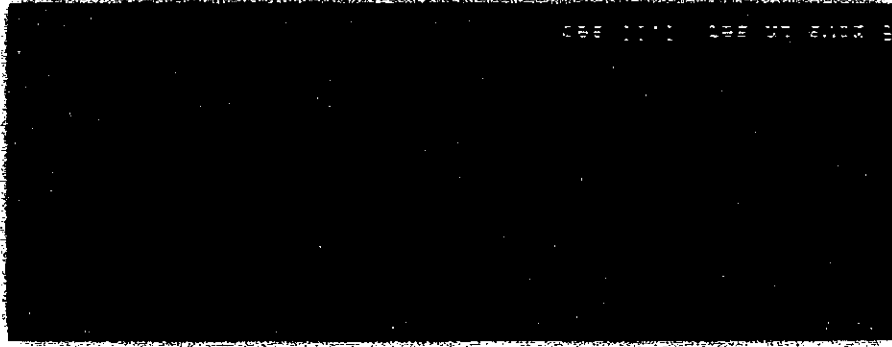


Şekil 6: client tablosunun alan adları ve özellikleri

"client" tablosunun uygulama geliştiricisi tarafından gerçekleştirilen kısa süreli

teknik çalışmalarında kullanıldığı değerlendirilmektedir.

3.6.2.6 "exception" tablosu:



Şekil 7: exception tablosunun alan adları ve özellikleri

Uygulama kullanıcılarının karşılaştıkları yazılımsal hataların "exception" tablosunda saklandığı görülmüştür. Tabloda uygulamamın kullanım sırasında karşılaşılan problemlere ilişkin kayıtlar yer almaktadır.

"file\_transfer" tablosunda, transfer edilen dosyanın hangi kullanıcı tarafından (fromUserId), kime gönderildiği (toUserId), dosyanın gönderilme ve iletilme zamanı gibi bilgilerin saklandığı görülmüştür (Dosya bilgileri şifreli bir şekilde tutulmaktadır).

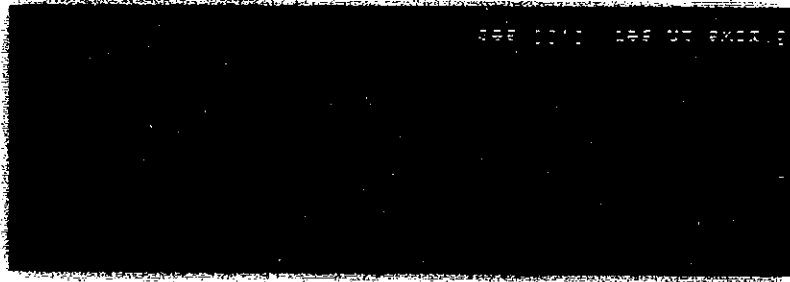
Şekil 9: file\_transfer tablosunun alan adları ve özellikleri



3.6.2.8 "file\_transfer" tablosu:

"file" tablosunda, kullanıcıların birbirleri ile paylaştıkları dosyalara ait bilgilerin yer aldığı görülmüştür.

Şekil 8: file tablosunun alan adları ve özellikleri



3.6.2.7 "file" tablosu:

id	userid	name
10087	202603	1.sosyal ekip
5253	31687	ABILER
9827	1157	adli grup
28073	85680	ahmet talha
28281	111201	Balikesir
26694	1443	BAYAN IZDVC
26821	136433	BEDRİN ASLANLARI
28106	1756	bilecik heyeti
28151	26130	Bolge Bayan
27282	1020	Dergici

3.6.2.10 "user\_group" tablosu:

"group\_member" tablosunda, uygulama üzerinde kullanıcılar tarafından oluşturulan gruplarda (groupid), hangi kullanıcıların (userid) hangi grupta bulunduğu bilgisi yer almaktadır. Oluşturulan gruplarda yer alan şahıslara ait "userid (Kullanıcı kodu)" bilgisi bu tabloda tutulmaktadır. "Groupid" olarak adlandırılan numara ile "User\_group" tablosundaki Id sütunu eşleştirildiğinde oluşturulan grup isimlerine dahil olan şahıslara ait bilgiler elde edilebilmektedir. "User" tablosundaki Userid ile "group\_member" tablosundaki Userid bilgisi eşleştirilerek ise aynı grupta yer alan şahıslara ait "Kullanıcı adı" bilgisi de elde edilebilmektedir. Toplamda 187.629 kayıt bulunmaktadır.

Şekil 10: group\_member tablosuna ait örnek kayıtlar

groupid	userid	24	59
24	522	24	528
24	533	24	619
24	836	24	296
24	3984	26	101683
25	312	25	365
25	444	25	566
25	53	26	112
26	26	26	26

3.6.2.9 "group\_member" tablosu:

"user\_group" tablosunda, hangi grubun hangi kullanıcı tarafından oluşturulduğu ve grubun isminin saklandığı görülmüştür. "user\_group" tablosundan toplam 31.886 kayıt bulunmaktadır. "user\_group" tablosu ilişkili olduğu diğer tablolar ile beraber değerlendirildiğinde oluşturulan gruplara hangi Userid ye sahip şahısların dahil olduğu bilgisi elde edilebilmektedir.

Şekil 16: user\_group tablosuna ait örnek kayıtlar

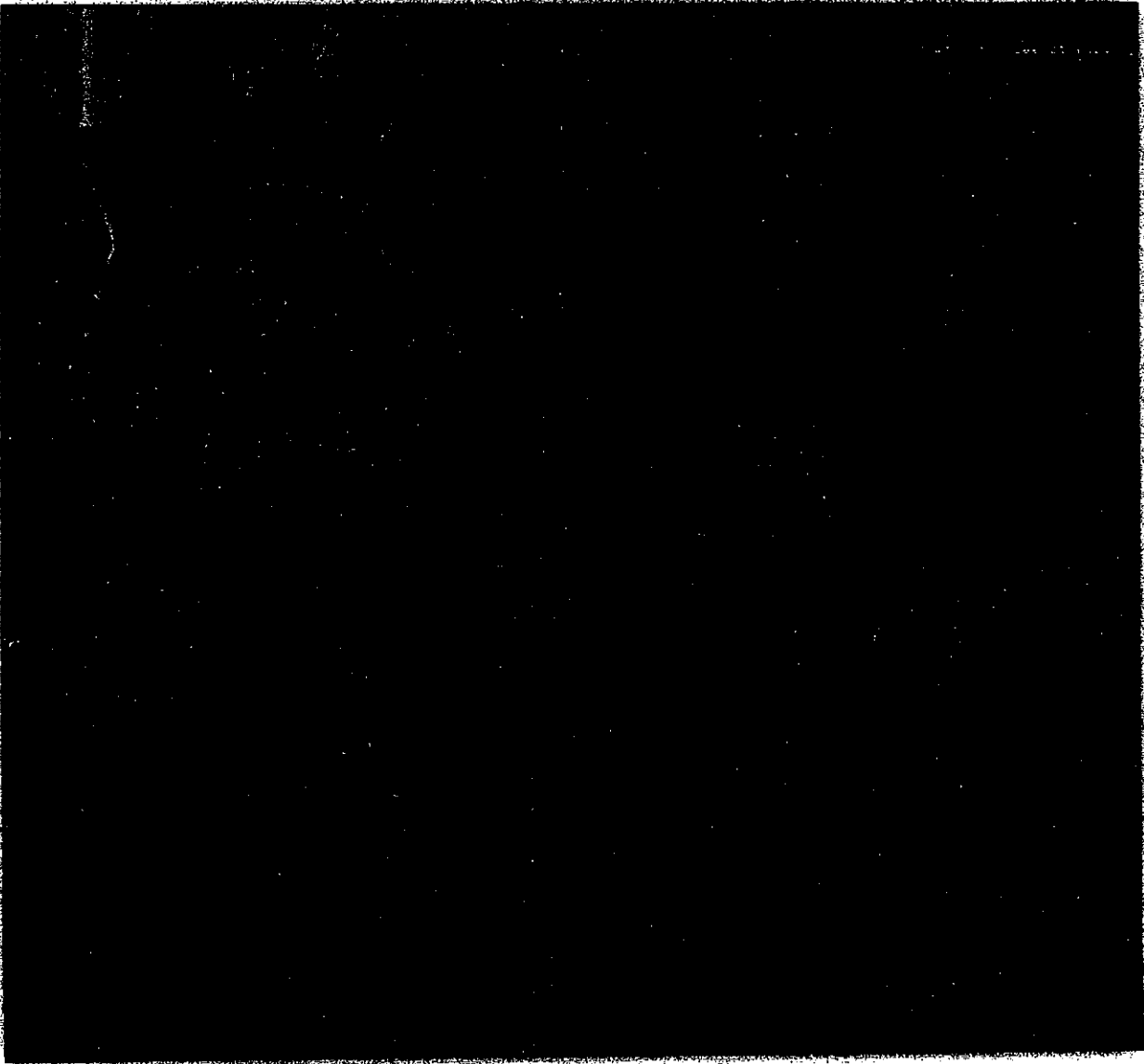
11631	3904	ISTISARE
28521	46519	İLÇE MESULLER
7391	755	ÜNİV GM
28146	2529	Samsun Unv
27271	48208	prizma
26697	59407	MüdürDisB
11688	87555	mdur+zumre
28410	72453	merkezi müdür mesul
27074	343230	merkez md
51319	121260	Manisa
27233	154395	LİSE GM
27719	107144	kordinasyon
27455	53714	koordinatör
27073	343230	ilçe mdr
27860	127098	ilçe bblm
9915	200800	il dışı öğrenciler
2298	3792	hkk
26315	203536	esnaf
12191	142211	drgrubbankara
9722	183441	DNSTY - GRB
2665	1560	devreler
26205	235480	DERSHANE

"Register" işlemlerinde, kullanıcılara ait IP adres bilgilerinin de "log" tablosuna uygulamaya giriş işlemi olan "Login" ile uygulamaya kayıt olma işlemi olan

anlatılmaktadır.

"actionId" alanı eşleştirilerek parameter alanlarında kayıtlı veriler tablosunda saklandığı görülmüştür. "action" tablosundaki "id" alanı ile bu tablodaki "parameter" alanlarında kayıtlı verilerin hangi anlama geldiği bilgisi, "action" "log" tablosunda, uygulamaya ait log kayıtları tutulmaktadır. Parametreler

Şekil 11: log tablosuna ait örnek kayıtlar

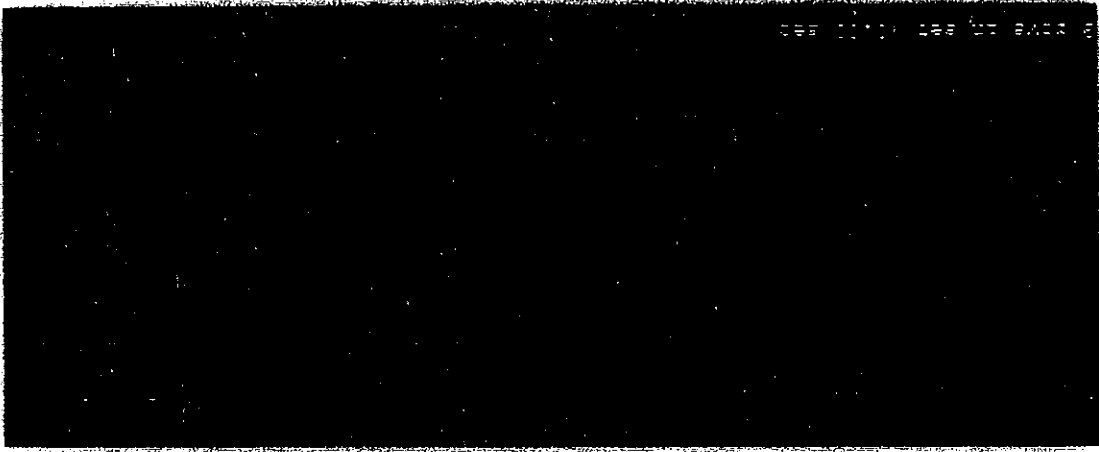


3.6.2.11 "log" tablosu:



"mail" tablosunda yer alan içeriklere ait örnek verilere aşağıda yer verilmiştir:  
İçeriği gözümlemişdir. Çözümleme işlemi devam etmektedir.  
tabloda saklanmaktadır. Gerçekleştirilen gelişmeler neticesinde 2.293.518 adet e-posta  
görülmüştür. Toplamda ulaşılabilen 3.158.388 adet e-posta içeriği kriptolu olarak bu  
postanın gönderilen kişiye iletilme zamanı bilgilerinin "mail" tablosunda saklandığı  
konu, e-posta içeriğinin şifreli hali, imza, e-postanın gönderilme zamanı ve e-  
gönderen kullanıcı, e-postayı alan kullanıcı, e-postayı diğer kullanıcılar,  
Uygulamamızın e-posta özelliği kullanılarak gönderilen her bir e-posta için; e-postayı  
"mail" tablosu alan adları ve özellikleri ile "chat" tablosuna benzetmektedir.

**Şekil 12: mail tablosunun alan adları ve özellikleri**



**3.6.2.12 "mail" tablosu:**

görülmektedir.  
tablosu uygulamayı kullanan şahısların sunucuda bırakmış oldukları izler olarak  
kayıt edildiği görülmüştür. Bu veriler şahıs tespit işlemlerinde kullanılmaktadır. Log

GİZLİ

44

bodyPartText: 33ee9dc0d8524bb8c76

bodyPartText: Mühürerem arkadaşları Şu ana kadar gözükenden tutuklanma geçte daha çok...

2015-12-28 17:20:43

receivedTime decrypted

bodyPartText

signature

sentTime

<p dir="rt" >br </p > ...

1

bodyPartText

1

bodyPartText

Mühürerem arkadaşlar! Şu ana kadar gözükenden tutuklanmaya geçte daha çok yakalanan evrak, kurban-burs-bağış-himmel-müktevell ve ders grubu küteleri, Yanış İfade, pank yapmak, avukat getirmeden rade veremeye başlamak, teknik bilginin malzemeleri (CD, bilgisayar, laptop vb) yakalamaya ve şikayet etmeden kayıtlı. Ortaklar dediriniz gözümlüğü de bilgi-bellek-teknik malzemeleri. Yani şu arama-taramaya yakalananlardan kaynaklı deliller oluşturuyor. Bu, neden kayıtlıdır? Önemli kayıtlıdır. Ben burun ama bulduğum ayarlamam soyunm. (Hizme kök gelmiş). -Bana bunlar özel haber... -Bana bu kadar çok kıymetli, siz bunun değeri bilirsiniz. -Gelecek, sene hizmet için bunlar lazım olacak. -Her sene kök gelmiyor var. Bir hizmet ne emeklerle buraya geldi. -Siz, kendinize bakın, Ben temizim zaten. -İdam da elsteler razıyım ben, Benim sakladığım yerde cinler bile bulamaz. -Yakında bu suçta olacak zaten. -Benim filmi bu yerde tanıdığım var. Ona soviyetim bize yardımcı olur...

vs..... Arkadaşlar! ailesi sadece düşüğü yen yakıyor, ailesi hepimizi yakıyor.... Lütfen yeniden ATM,

GİZLİ

Eposta İçeriği Özetli - 1



id	FromUserid	ToUserid	Nickname
1614883	25434	13690	yasin komser
369601	15882	88327	Albay
577245	170895	57572	albay133
1599444	349749	359042	zalbay
2127968	1185	467	yousuf albay
2369838	404376	378741	aalbay
1212882	121371	189573	yarbay
775159	8781	9891	4006 pilot karma
1372304	183366	84121	pilot abi
1809484	22189	402862	pilot3163
311151	852	46512	Fatih Yigit Komiser delikanlii
1209224	269043	152142	M.Akif Baskomiser
1223777	269043	1820	Ismail Baskomiser
1496338	248855	280030	Coskun komiserim
953721	54855	183982	ank900ara faik hsyk
1757555	151879	113586	tarsus fatih hsyk
1528960	202	343151	Halil Bey Kuuvet Asker
121697	48277	25921	farukhakim
2509336	472645	411050	savci20
2527154	513677	411050	savci
214579	50600	14396	Hakim a
369678	2019	14396	kayshakim
502138	153432	114772	hakim bey
838090	35441	25921	faruk hakim
1324263	211131	320752	Hakim Rakipi
1491175	347869	348172	Lukmannul hakim
2378077	27520	493923	hakim hoca

3.6.2.13 "roster" tablosu:

"roster" uygulamaya ait rehber bilgilerinin saklandığı tablodur. Bu tabloda, hangi kullanıcının, hangi kullanıcıyı, uygulama rehberine (telefon rehberi değildir) hangi isimle kaydettiği bilgisinin saklandığı görülmüştür. ByLock uygulamasının kullanan şahıs, "Kullanıcı Adı" ile bir arkaadışını uygulamada ekledikten sonra, kendi rehberinde eklediği kişinin isim bilgisini yeniden düzenleyebilmektedir. (Örn. "Kullanıcı Adı" "100" olan kişi, "Kullanıcı Adı" "500" olan kişiyi rehberine ekledikten

Şekil 13: roster tablosuna ait örnek kayıtlar

1963375	247967	111715	izmir kriz genel mudur hakki
2002545	247967	212333	muduru
2030074	247967	204116	aydınlik kolej muduru suleyman
2183272	247967	227925	afyon dersaneler genel muduru
2234374	247967	404312	yamanlar personel muduru
2284118	247967	258443	gaye koleji muduru
1459232	198273	91598	IZDIVAC MESULU
1485582	41937	221517	Bartın Mezun Mesulu
1548773	252699	157533	Ahmet inzya mesul
1902440	61414	152800	Fatih-Avukat mesulu
2061472	103819	43229	Fatih hukuk izm mesul
2101795	15701	113492	Bornova İletişim k. mesulu
2433830	493512	431708	İvane0808 Dr mesulu mrt
2494689	455475	415386	Tarik mesul
2515420	74717	234956	usak univ mesul
2553409	74717	102163	antalya 03 mesul
1015970	62153	107144	Burak Eğitim Abi Sorumlusu
1287653	74717	96040	antalya mucahit İİSE sorumlu
2336240	402417	130327	Turgutlu sorumlusu elif
2402531	402417	424228	manisa sorumlusu Dicle hnm
2526470	402417	239789	denizli Sorumlusu ahsen hoca

"user" tablosunda, Kullanıcı Adı, kullanıcının oluşturulma tarihi ve en son giriş yapma tarihi RSA Sertifika bileşenleri, kullanıcının oluşturulma tarihi ve en son giriş yapma tarihi (md5 kriptografik özet),

Şekil 15: user tablosunun alan adları ve özellikleri



3.6.2.15 "user" tablosu:

"setting" tablosunda, uygulama sunucusu çalışırken kullanılan bazı teknik parametrik değerlerin saklandığı görülmüştür.

Şekil 14: setting tablosuna ait örnek kayıtlar



3.6.2.14 "setting" tablosu:

tablosundan elde edilen verilerde toplam 1.350.624 kayıt bulunmaktadır. sonra, rehberinde "500" kodlu kişinin adını "Orhan A" olarak kaydetmiştir, "roster"

gibi bilgilerin tutulduğu görülmüştür. Bu tabloda aynı zamanda kullanıcının kendine özel RSA kriptografik anahtar setinin gizli anahtarı (privateExponent) mevcuttur. privateExponent bileşeninin tablodaki kriptolu bir şekilde saklandığı görülmüştür.

“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. User tablosunda yer alıp deşifre edilen verilere ilişkin örnekler aşağıda verilmiştir: (“username” bilgisi kullanıcı adına/koduna, “plain” bilgisi ise yürütülen çalışmalar neticesinde çözümlenmiş kullanıcı şifresine işaret etmektedir.)

username	plain
10001	qwertyuiopasdghjkl
bahadır559	qazwsxedcrtfgyb12345
umudumsun	qwertyuiop1234567890
adem999	asdghjkl1234567890
ih34	polytrewq1234567890
yusu2763	qwertyuiop0987654321
mehin63	qwertyuiop1234567890
ender3	1234567890qwertyuiop
Ahmetah126	0123456789987654321a
sinan20	1234567890qwertyuiop
serkans5363	qwertyuiop1234567890
sinand	1234567890qwertyuiop
aktalınzde2	olmayadaoimamak1234
haklar	1234567890qwertyuiop
incredible06	insansizhavaraaci2006
cinan6403	qwertyuiop1234567890
istanbul61	istanbulistanbul2001
adem2015	q1w2e3r4t5y6u7i8o9p0
34talha34	qwertyuiop1234567890
mchl2015	qwertyuiop1234567890
13muhacir12	polytrewq1234567890
serdar6342	qwertyuiop1234567890
sinanecz	qwertyuiop0987654321
ablah63	0987654321qwertyuiop
05721537	1234567890987654321h
ilkera	qwertyuiop1234567890
ih53	qwertyuiopasdghjkl1
efektili48	a123456789987654321z
mustatabakir	qwertyuiop0987654321
eczsedar	qwertyuiop0987654321
tehi061453	polytrewq1234567890
ismail2009	qwertyuiop0987654321
mcebisi163	qwertyuiop1234567890i
cem05	1234567890@qwertyuiop
selo1	ledbideldendibrakma.01
gazanfer0232	qazl@%jwsxlg@%j
haticeyurekdeleir	aaaaaaaaaaaaaaaaaaaaa1&
evren25	evrenatut@hotmail.com
gazanfer	qazl@%jwsxlg@%j
Nataniel	qwertyuiop1234567890@#s
ikm34	asdghjkl1234567890



## Kullanıcı Adı/Kodu ve Çözümlemiş Şifre Örneği - 2

plain	username
1234567890asdtghjkl	suleman
asdtghjkl.123456789	S1357
fahsultamemehmet7%	bedir313
123456i@#fatmaolmez	fatmaolmez
asdtghjkl.123456789	S9875
asdtghjkl@#%&+?!	neyzen19
Yildirim1234567890.	Yildirim5252
Lotusun@hotmail.com	ibrahimosun
gonulkaradeniz@@@	gonulkrdz061
123456789kara.anka	zeynel78
Murat2008Murat2008.	smurat
qweyuioplmnbvcxz	Sierra
seni.seviorum.1989	smha
234567890asdtghjkl.	Aykut12
istanbulistanbul.34	snh34
Yildirim1234567890.	Yildirim111
BugunlerdegECEK1.	kenan046
cihangircihangir29.	cihangirdaloglu
tuyellin@gmail.com	tuyellin
chocolate123456789.	camilabastel
Yildirim1234567890.	500269
qweasd123.qweasd123	Numan111
qawseftrgyhuj1234.	asdtghzxc
qwertgdsa123454321	Allim0671
serdar.gul1234567890	serdar.gul
1234567890asdtghjkl.	AYKUT12
123123123123123123a/	123123123123123123a/
1234567890.poliytrwq	honda0101
asdtghjkl.1234567890	ensaara0015
icisendisibenyakar	newbutold
qawseftrgyhujkiop.	bydokfortank
1234567890poliytrwq	Allim
olmalyadaolmama123.	akifalnzde
Qazwsxedc1234567890.	Davud44
Qazwsxedc1234567890.	davud500217
1234567890Asdtghjkl.	efendi
qazwsxedcftvgb1452\$	59bahadir
qazwsxedcftvgb1452\$	59bahadir
1234567890asdtghjkl.	serdar03
1234567890asdtghjkl.	sanliurfa63
fatmaeilik123456789	imrance58

## 3.7 ByLock Uygulamasına Ait İstatistikî Veriler

Tespit	Sayı
Uygulamaya Kayıt Olan Kullanıcı Sayısı	215.092
Parolası Çözümünebilen Kullanıcı Sayısı	184.298
(Çözümleme İşlemi Devam Etmemektedir.) Uygulamada Oluşturulmuş Toplam Grup Sayısı	31.886
Uygulamadaki Toplam Mesaj İgeriği (Gönderilen ve Alınan Bütün Mesajlar)	17.169.632
Çözümlenen Mesaj İgeriği (Çözümleme İşlemi Devam Etmemektedir.)	15.520.552
Uygulama Verilerindeki Toplam E-Posta İgeriği	3.158.388
Çözümlenen E-Posta İgeriği	2.293.518
Block Uygulamasında En Az 1 Kez Mesaj Atmış ve/veya Almış Şahıs Sayısı	60.473
Uygulamadaki Sesli Görüşmeyi Kullanan Şahıs Sayısı	78.165
Uygulamayı Sadece Sesli İletişim İçin Kullanan Şahıs Sayısı	46.799

Ayrıca çözümlenen şifrelere ilişkin istatistikî veriler Ek-11'de sunulmuştur.

- Uygulamaya ait kaynak kodları içerisinde bir takım "Türke" ifadelerinin yer alması,
- Kullanıcı adlarının, grup isimlerinin ve çözümlenen şifrelerin büyük çoğunluğunun Türke ifadelerden oluşması,
- Çözümlenen içeriklerin neredeyse tamamının Türke olması,

Kaldı ki,

bulunmadığı teyit etmektedir.

Diger taraftan, uygulamanın Litvanya'da sunucu kiralanmak suretiyle kullanılmasına sunulması ve kiralama bedellerinin ise "Paysera" adlı anonimlik sağlayan ödeme sistemiyle gerçekleştirilmiş olması, bu girişimin kurumsal ve ticari mahiyetinin görülmüştür.

- Uygulamanın tanıtılmasına yönelik girişimlerin bulunmadığı,
- Kullanıcı sayısını artırmayı ve ticari değer haline gelmeyi hedeflemediği,
- Anonimlik içeren yöntemlerle (Paysera) gerçekleştirildiği,
- Gerçekleştirilen iş ve işlemlere (sunucu ve IP kiralama) ait ödemelerin Erişilebilir İletişim Bilgilerinin bulunmadığı,
- Sektördeki geçmişinin belirsizlik arz ettiği,
- Daha önce yaptığı işlere ilişkin referanslarının bulunmadığı,

## 2- Uygulamayı geliştiren ve kullanıma sunan şahsın,

ile şifrelenerek iletmesine dayanan bir tasarıma sahip olduğu görülmüştür. 1- ByLock uygulamasının, güçlü bir kriptosistemle internet bağlantısı üzerinden iletişim sağlamak üzere, gönderilen her bir mesajın farklı bir kripto anahtarı

yer verilen sonuç ve değerlendirilmelere ulaşılmıştır: ByLock uygulaması, tersine mühendislik, kriptosistem analizi ve bağlantı kurulan sunucular tarafından cevap veren kodlar da dahil olmak üzere detaylarına yukarıda yer verilen ayrıntılı teknik çalışmalara tabi tutulmuş olup, aşağıda

## 4. DEĞERLENDİRME ve SONUÇ

Diğer taraftan, kullanıcı hesabı oluşturulması sırasında kişiye ait özel bir bilginin (telefon numarası, kimlik numarası, e-posta adresi vb.) talep edilmemesi, global ve ticari benzer uygulamalarda olduğu şekilde kullanıcı hesabını doğrulamaya yönelik bir işleyişin (sms şifre doğrulaması, e-posta doğrulaması vb.) bulunmamasının esaslı

3- Uygulamanın akıllı telefonlara yüklenirken sonra kullanılabileceği için kullanıcı adı/kodu ve parolanın, akabinde cihaz üzerinde rastgele el hareketleriyle oluşturulan kullanıcıya özel güçlü bir kriptografik şifrenin belirlenmesi ve bu bilgilerin uygulama sunucusuna kriptolu olarak iletilmesi işlemlerine, kullanıcı bilgilerinin ve iletişimin güvenliğinin azami şekilde korunmasının amaçlandığı görülmektedir.

sunulduğu anlaşılmıştır.

uygulama maskesi altında, FETÖ/PDY mensuplarının kullanımına

hususları birlikte değerlendirildiğinde, anılan uygulamanın global bir

- bilinmemesi/tanınamaması
- Girişimi" öncesinde ne Türk kamuoyu ne de yabancılar tarafından
- İki yüz bini aşkın kullanıcı kitlesine sahip ByLock'un "15 Temmuz Darbe paylaşımlarında bulunulması,
- Ayrıca, ByLock'la ilişkili internet kaynaklı yayınların (sosyal medya, web siteleri vb.), çoğunlukla sahte hesaplar üzerinden FETÖ/PDY lehine büyük bir artış olması,
- Bunun yanı sıra, ByLock'a ilişkin "Google" üzerinden gerçekleştirilen aramaların neredeyse tamamının Türkiye'deki kullanıcılar tarafından gerçekleştirilmesi ve uygulamaya Türkiye IP adreslerinden erişimin engellendiği tarih itibarıyla uygulamaya yönelik "Google" aramalarında
- Bunu yanı sıra, ByLock'a ilişkin "Google" üzerinden gerçekleştirilen erişimi, VPN vasıtasıyla gerçekleştirilmesine zorlanması,
- Türkiye'den erişim sağlayan kullanıcılara ait kimlik bilgilerinin ve iletişimin gizlenmesini sağlamak amacıyla kullanıcıların uygulamaya
- Bunu yanı sıra, ByLock'a ilişkin "Google" üzerinden gerçekleştirilen aramaların neredeyse tamamının Türkiye'deki kullanıcılar tarafından gerçekleştirilmesi ve uygulamaya Türkiye IP adreslerinden erişimin engellendiği tarih itibarıyla uygulamaya yönelik "Google" aramalarında
- Türkiye'den erişim sağlayan kullanıcılara ait kimlik bilgilerinin ve iletişimin gizlenmesini sağlamak amacıyla kullanıcıların uygulamaya
- Bunu yanı sıra, ByLock'a ilişkin "Google" üzerinden gerçekleştirilen erişimi engellediğini belirtmesine rağmen, gerçekleştirilen engellemelerin tamamına yakının Türkiye IP adreslerine yönelik olması,
- Uygulama sunucusu yöneticisinin, Ortadoğu IP adreslerinden uygulamaya

sebebinin, anonimliğin sağlanması ve kullanıcı tespitini zorlaştıracak önlemlerin kurulmasından kaynaklandığı değerlendirilmiştir.

4- Uygulama geliştiricisinin, otorite imzalı SSL sertifikası kullanmadığı, kendi oluşturduğu bir SSL sertifikasını kullandığı tespit edilmiştir. Ancak global ve ticari anlık mesajlaşma uygulamalarının "otorite imzalı SSL sertifikası" kullandığı, bununla kullanıcı bilgilerinin ve iletişim güvenliğinin sorumluluğunu ücreti mukabilinde bu otoriteye bıraktığı bilinmektedir. ByLock uygulamasında ise, uygulama geliştiricisinin, kullanıcılara ait bir takım bilgilerin sertifika otoritesine gitmesini istememesi nedeniyle "otorite imzalı SSL sertifikası"ni tercih etmediği değerlendirilmektedir. Uygulama geliştiricisinin sistem, işleyiş, kullanıcı güvenliği bakımından aldığı diğer önlemler de nazara alındığında, kullanıcılara ait haberleşme trafiğinin kendi uygulama sunucusu harici bir noktaya akışını engelleyen ilave bir önlem olarak tasarlaadığı görülmektedir.

5- Uygulamaya kayıt işleminin, sistemde kayıtlı kullanıcılarla iletişim kurmak için yeterli olmaması, iki kullanıcının haberleşmesi için her iki tarafın, çoğunlukla yüz yüze veya bir aracı (kurye, mevcut ByLock kullanıcısı üzerinden vb.) vasıtasıyla temin edilen kullanıcı adlarının/kodlarının eklenmesinin gerekmesi; mesajlaşmanın, her iki kullanıcının da birbiri eklemesinden sonra başlatılabilmesi sebebiyle haberleşmenin, sadece oluşturulan hücre tipine uygun şekilde gerçekleştirilmesine imkan verecek şekilde kurulandığı değerlendirilmiştir.

6- Uygulama üzerinden sesli arama, yazılı mesajlaşma, e-posta iletimi ve dosya transferi gerçekleştirilebilmektedir. Bununla, kullanıcıların örgütsel mahiyetteki haberleşme ihtiyaclarını, başka herhangi bir haberleşme aracına ihtiyaç duymadan gerçekleştirdiği ve tüm iletişim sunucu üzerinden geçtiğinden oluşturulan grupların ve haberleşme içeriklerinin uygulama yöneticisinin denetim ve kontrollerinde olmasını sağladığı değerlendirilmiştir.

7- Gerçekleştirilen haberleşmenin, cihaz üzerinden belirli sürelerde manuel işleme gerek duymaksızın otomatik olarak silinmesi, kullanıcıların, haberleşme güvenliği bakımından silmeleri gereken verileri silmeyi unutsa dahi sistemin gerekli tedbirleri alacak şekilde tasarlaadığını göstermektedir. Böylece ByLock

uygulamasının, olaş bir adli işlem neticesinde cihaza el konulması durumunda

dahi uygulamada ver alan kullanıcı listesindeki diğer kullanıcılara ve

uygulamadaki haberleşmelere ilişkin geçmiş verilere erişimi engelleyecek şekilde

kurulandığı değerlendirilmiştir. Ayrıca, uygulamaya ait sunucu ve iletişim

verilerinin, uygulama veri tabanında kriptolu olarak saklanması, kullanıcı tespitinin

önlenmesi ve haberleşme güvenliği için alınan ilave güvenlik tedbiri mahiyetinde

olduğu değerlendirilmiştir.

#### 8- Kullanıcıların kendilerini gizlemek amacıyla;

• Çok uzun haneli parola belirlediği, örneğin çözümü tamamlanan veriler

arasında 38 haneye vatan parolaların yer aldığı ve çözümü tamamlanan

parolaların yarısından fazlasının 9 hane ve üzerinde karakter içerdiği;

• Belirli bir tarihten sonra uygulamanın Android Market veya Apple

AppStore'dan indirilmesi yerine, kullanıcıların cihazlarına manuel olarak

yüklediği;

• 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

işeriklerinin tamamına yakınının FETÖ/PDY unsurlarına ait örgütsel temas ve

faaliyetleri içerdiği ve örgüte ait jargonla örtüştüğü görülmüştür.

9- FETÖ/PDY unsurlarınca gerçekleştirilen 15 Temmuz 2016 askeri darbe

girişimi sonrasında adli kontrol işlemlerine (gözaltı, tutuklama, yakalama vb.) tabii

tutulan örgüt mensuplarının ifadelerinden, 2014 yılının başlangıcında FETÖ/PDY

örgüt üyeleri tarafından örgütsel haberleşme aracı olarak kullanıldığı anlaşılmıştır.

Yukarıda izah edilen durumların hepsi birlikte değerlendirildiğinde, ByLock

uygulamasının, global bir uygulama görüntüsü altında münhasıran FETÖ/PDY terör

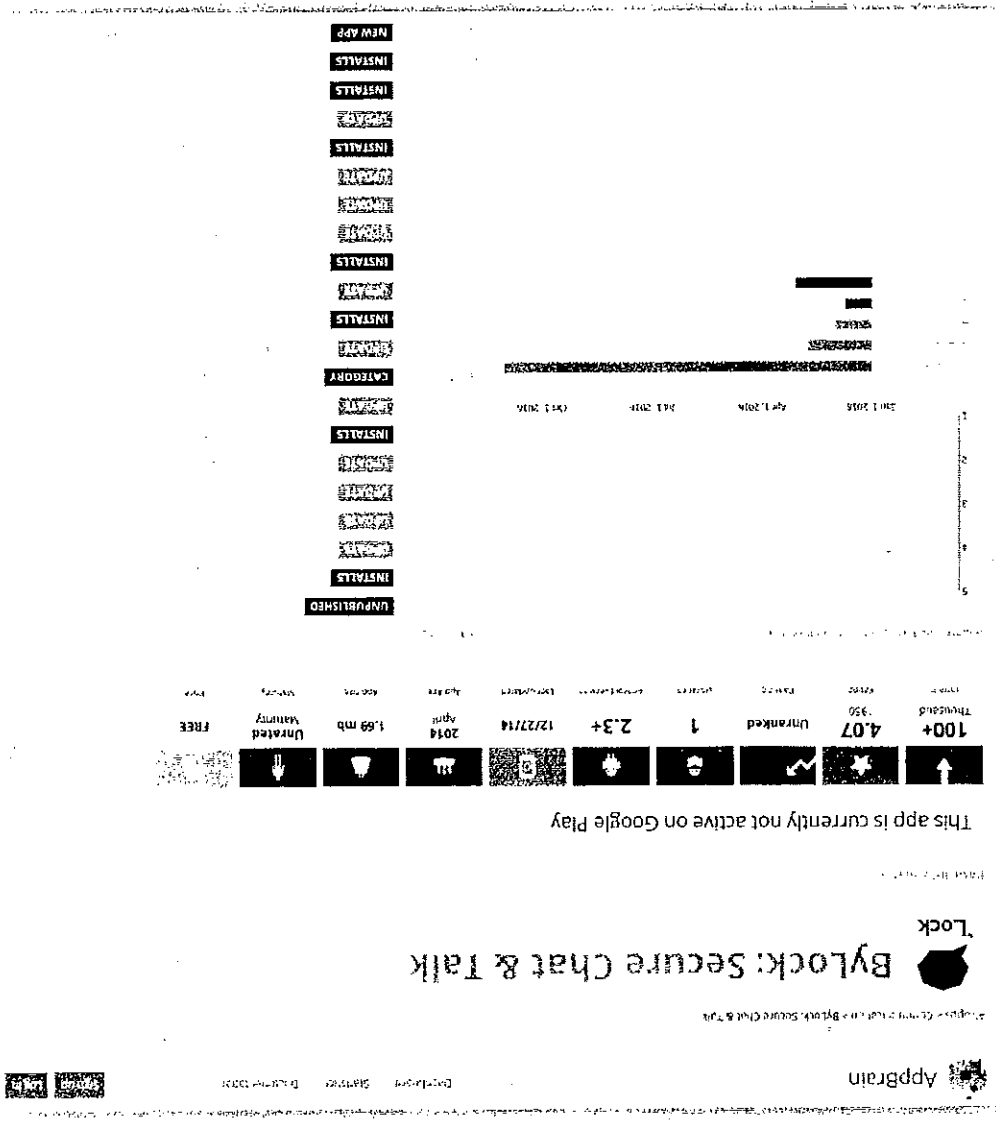
örgütü mensuplarının kullanımına sunulduğu sonucuna ulaşılmıştır.

- Ek-11: Çözümlenen Şifrelere İlişkin İstatistikî Veriler
- Ek-10: Uygulama Sunucusunda Engellenen IP Adresleri Listesi
- Ek-9: Uygulamanın Sunucusunda Çalışan Yazılımda Raslanan Türkçe İfade
- Ek-8: Uygulama Sunucusu Yazılım Modelleri
- Ek-7: Kayıt ve İki Kullanıcı Arasındaki Şifreli Mesajlaşmaya Ait Akış Şeması
- Ek-6: İstemci Kaynak Kodlarında Geçen Kriptografik Algoritmalar
- Ek-5: Kaynak Kodlarda Geçen Türkçe İfadeler
- Ek-4: ByLock Sunucusu IP Adreslerine İlişkin virustotal.com Sorgusu
- Ek-3: Bylock Sunucusuna Ait Sertifikanın Ekran Görüntüsü
- Ek-2: ByLock Uygulamasının Google Play'den Yaklaşık İndirilme Sayısı
- Ek-1: ByLock Uygulamasının Versiyon Tarihleri

EK-1: ByLock Uygulamasının Versiyon Tarihleri

Version	Release Date	Android Version	App Size	Download Link
1.17	Dec 24, 2014	Android 2.3 and up	1.17 MB	ByLock Secure Chat & Talk 1.17
1.16	Sep 4, 2014	Android 2.3 and up	1.16 MB	ByLock Secure Chat & Talk 1.16
1.15	Aug 27, 2014	Android 2.3 and up	1.15 MB	ByLock Secure Chat & Talk 1.15
1.14	Aug 23, 2014	Android 2.3 and up	1.14 MB	ByLock Secure Chat & Talk 1.14
1.13	Jul 11, 2014	Android 2.3 and up	1.13 MB	ByLock Secure Chat & Talk 1.13
1.12	Jun 23, 2014	Android 2.3 and up	1.12 MB	ByLock Secure Chat & Talk 1.12
1.11	May 25, 2014	Android 2.3 and up	1.11 MB	ByLock Secure Chat & Talk 1.11
1.10	May 24, 2014	Android 2.3 and up	1.10 MB	ByLock Secure Chat & Talk 1.10
1.09	May 14, 2014	Android 2.3 and up	1.09 MB	ByLock Secure Chat & Talk 1.09
1.08	May 11, 2014	Android 2.3 and up	1.08 MB	ByLock Secure Chat & Talk 1.08
1.06	May 9, 2014	Android 2.3 and up	1.06 MB	ByLock Secure Chat & Talk 1.06
1.05	May 8, 2014	Android 2.3 and up	1.05 MB	ByLock Secure Chat & Talk 1.05
1.04	May 8, 2014	Android 2.3 and up	1.04 MB	ByLock Secure Chat & Talk 1.04
1.03	Apr 26, 2014	Android 2.3 and up	1.03 MB	ByLock Secure Chat & Talk 1.03
1.02	Apr 26, 2014	Android 2.3 and up	1.02 MB	ByLock Secure Chat & Talk 1.02
1.01	Apr 9, 2014	Android 2.3 and up	1.01 MB	ByLock Secure Chat & Talk 1.01
1.00	Apr 9, 2014	Android 2.3 and up	1.00 MB	ByLock Secure Chat & Talk 1.00





Ek-2: ByLock Uygulamasının Google Play'den Yaklaşık İndirime Sayısı

**46.166.160.137**  
Identity: 46.166.160.137  
Verified by: David Keynes  
Expires: 08/21/2024  
◀ Details

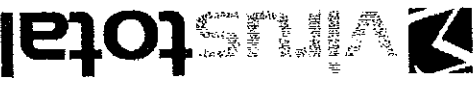
**Subject Name**  
C (Country): US  
ST (State): Oregon  
L (Locality): Beaverton  
O (Organization): Unknown  
OU (Organizational Unit): Unknown  
CN (Common Name): 46.166.160.137

**Issuer Name**  
C (Country): US  
ST (State): Oregon  
L (Locality): Beaverton  
O (Organization): by Lock  
OU (Organizational Unit): CA  
CN (Common Name): David Keynes

**Issued Certificate**  
Version: 3  
Serial Number: 1B 8F A2 F4  
Not Valid Before: 2014-08-24  
Not Valid After: 2024-08-21

EK-4: ByLock Sunucusu IP Adreslerine Iltisikin VirusTotal.com Sorgusu

46.166.160.137 IP address information

 VirusTotal

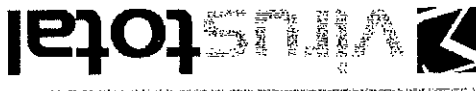
Geolocation  Country  Autonomous System  Passive DNS replication

Country: LT  
Autonomous System: 59642 (UAB DUOMENU CENTRAS)

VirusTotal's passive DNS only stores address records. The following domains resolved to the given IP address.  
2016-02-19 bylock.net

---

46.166.164.177 IP address information

 VirusTotal

Geolocation  Country  Autonomous System  Passive DNS replication

Country: LT  
Autonomous System: 59642 (UAB DUOMENU CENTRAS)

VirusTotal's passive DNS only stores address records. The following domains resolved to the given IP address.  
No domains found in the VirusTotal database.

EK-5: Kaynak Kodlarda Geçen Türkçe İfadeler

```

.methodprotected a(Ljava/lang/String;
    .locals 3
    .prologue
    .line 35
    new-instance v0, Ljava/lang/StringBuilder;
        get-object v1, p0, Lnet/client/by/lock/b/d;->i:Ljava/lang/String;
        invoke-static {v1, p0, Lnet/client/by/lock/b/d;->i:Ljava/lang/String;
            {v1},
        >valueOf(Ljava/lang/Object;Ljava/lang/String;
        move-result-object v1
        invoke-direct {v0, v1},
        <<init>(Ljava/lang/String;)V
        const-string v1, "(Dosya)"
        invoke-virtual {v0, v1},
        append(Ljava/lang/String;Ljava/lang/String;Lder;
        move-result-object v0
        get v1, p0, Lnet/client/by/lock/b/d;->a:I
        int-to-long v1, v1
        invoke-static {v1, v2, Lnet/client/by/lock/f/j;->a(J)Ljava/lang/String;
        move-result-object v1
        invoke-virtual {v0, v1},
        append(Ljava/lang/String;Ljava/lang/String;Lder;
        move-result-object v0
        const-string v1, ""
        invoke-virtual {v0, v1},
        append(Ljava/lang/String;Ljava/lang/String;Lder;
        move-result-object v0
        invoke-virtual {v0, v1},
        >append(Ljava/lang/String;Ljava/lang/String;Lder;
        move-result-object v0
        invoke-virtual {v0, v1},
        move-result-object v0
        return-object v0
    .endmethod

```

```

.methodprotected a(Ljava/lang/String;
    .locals 2
    .prologue
    .line 21
    new-instance v0, Ljava/lang/StringBuilder;
        get-object v1, p0, Lnet/client/by/lock/d/m;->b:Ljava/lang/String;

```

```

.invoke-static {V1}, Ljava/lang/String;-
>valueOf(Ljava/lang/Object;)Ljava/lang/String;
move-result-object V1
invoke-direct {V0, V1}, Ljava/lang/String;-
<init>(Ljava/lang/String;)V
const-string V0, "Sesli Arama"
invoke-direct {V1, V0}, Ljava/lang/String;-
new-instance V1, Ljava/lang/String;-
const-string V0, "Sesli Arama"
move-result-object V0
invoke-virtual {V0}, Lnet/content/lock/f/h;->a(Ljava/lang/Object;)
get-object V0, p0, Lnet/content/lock/f/h;->f:Lnet/content/lock/f/h;
move-result-object V0
check-cast V0, Ljava/lang/String;
const-string V2, "CLOSED"
invoke-virtual {V0, V2}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z
move-result V0
if-eqz V0, :cond_0
new-instance V2, Ljava/lang/String;-
const-string V0, "("
invoke-direct {V2, V0}, Ljava/lang/String;-
<init>(Ljava/lang/String;)V
get-object V0, p0, Lnet/content/lock/f/h;->f:Lnet/content/lock/f/h;
invoke-virtual {V0}, Lnet/content/lock/f/h;->a(Ljava/lang/Object;)
move-result-object V0
check-cast V0, Ljava/lang/String;
const-string V2, "CLOSED"
invoke-virtual {V0, V2}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z
move-result V0
if-eqz V0, :cond_0
new-instance V2, Ljava/lang/String;-
const-string V0, "("
invoke-direct {V2, V0}, Ljava/lang/String;-
<init>(Ljava/lang/String;)V
get-object V0, p0, Lnet/content/lock/f/h;->f:Lnet/content/lock/f/h;
invoke-virtual {V0}, Lnet/content/lock/f/h;->a(Ljava/lang/Object;)
move-result-object V0
check-cast V0, Ljava/lang/String;
append(Ljava/lang/String;)Ljava/lang/String;-
invoke-virtual {V2, V0}, Ljava/lang/String;-
>toString(Ljava/lang/String;
move-result-object V0
return-object V0
.endmethod

```

```

.invoke-static {V1}, Ljava/lang/String;-
>valueOf(Ljava/lang/Object;)Ljava/lang/String;
move-result-object V1
invoke-direct {V0, V1}, Ljava/lang/String;-
<init>(Ljava/lang/String;)V
const-string V1, "(Posta)"
invoke-virtual {V0, V1}, Ljava/lang/String;-
append(Ljava/lang/String;)Ljava/lang/String;-
invoke-virtual {V2, V0}, Ljava/lang/String;-
>toString(Ljava/lang/String;
move-result-object V0
invoke-virtual {V0, V0}, Ljava/lang/String;-
return-object V0
.endmethod

```

```

move-result-object v0
const-string v2, ""
invoke-virtual {v0, v2},
append(Ljava/lang/String;)Ljava/lang/String;
move-result-object v0
invoke-virtual {v0}, Ljava/lang/String;
move-result-object v0
goto_0
invoke-virtual {v1, v0},
append(Ljava/lang/String;)Ljava/lang/String;
move-result-object v0
invoke-virtual {v0}, Ljava/lang/String;
move-result-object v0
move-result-object v0
return-object v0
:cond_0
const-string v0, ""
goto_0
.endmethod

```

```

.time 89
:try_start_0
const-string v1, "MD5"
invoke-static {v1, Ljava/security/MessageDigest;
>getInstance(Ljava/lang/String;)Ljava/security/MessageDigest;
:try_end_0
.catchLjava/security/NosuchAlgorithmException; {:try_start_0 ..
:try_end_0} :catch_0
move-result-object v0
.time 93
goto_0
invoke-virtual {v0}, Ljava/security/MessageDigest; >reset()V
.time 94
invoke-static {}, Lnet/client/by/lock/d/r;-
>f(Lnet/client/by/lock/d/r;-
invoke-virtual {v1}, Lnet/client/by/lock/d/r;-
move-result-object v1
invoke-virtual {v1}, Ljava/lang/String; >getBytes() [B
move-result-object v1
invoke-virtual {v0, v1}, Ljava/security/MessageDigest; >update([B)V
.time 96
new-instance v1, Ljava/math/BigInteger;
invoke-virtual {v0}, Ljava/security/MessageDigest; >digest() [B
move-result-object v3

```

Tablo - Asimetrik gizli anahtarın şifrelenmesi için kullanılan kodları içeren dosyaların uygulamamanı kurulum paketleri içerisindeki yolları

"MD5" kriptografik özel algoritmasının kullanımına ait kaynak kodların bir kısmına aşağıda yer verilmiştir:

Sürüm Numarası	Dosya Yolları
1.1.3	smali\ne\client\by\lock\m\smali
1.1.6	smali\ne\client\by\lock\m\smali
1.1.7	smali\ne\client\by\lock\m\smali
2.0.0	smali\ne\client\by\lockapp\two\c\l\smali

Kayıt sırasında girilen parolanın "MD5" kriptografik özeti için kullanılan fonksiyonları içeren "smali" dosyalarının 4 ayrı uygulama sürümüne ait kurulum paketleri içerisindeki yolları aşağıda sunulmuştur:

Ek-6: İstemci Kaynak Kodlarında Geçen Kriptografik Algoritmalar

Asimetrik gizli anahtar, "SHA256" kriptografik özel fonksiyonu ve "RSA/ECB/OAEPWithSHA-1andMGF1Padding" algoritmasına dair fonksiyonları içeren "smali" dosyaların 4 ayrı uygulama sürümüne ait kurulum paketleri içerisindeki yollarına aşağıdaki tabloda yer verilmiştir:

<pre> invoke-static {v0}, Ljava/security/KeyFactory; -&gt;getInstance(Ljava/lang/String;Ljava/security/KeyFactory; move-result-object v0 input-object v0, p0, Lnet/client/by/lock/d/f; -&gt;b:Ljava/security/KeyFactory; .time 52 const-string v0, "SHA1withRSA" invoke-static {v0}, Ljava/security/Signature; -&gt;getInstance(Ljava/lang/String;Ljava/security/Signature; move-result-object v0 input-object v0, p0, Lnet/client/by/lock/d/f; -&gt;d:Ljava/security/Signature; .time 53 const-string v0, "RSA/ECB/OAEPWithSHA-1andMGF1Padding" invoke-static {v0}, Ljava/cipher; -&gt;getInstance(Ljava/lang/String;Ljava/cipher; move-result-object v0 </pre>
--

"RSA/ECB/OAEPWithSHA-1andMGF1Padding" kriptografik algoritmasının kullanımına ait kaynak kodların bir kısmı aşağıda sunulmuştur:

Tablo - Haberleşmenin şifrelenmesi için kullanılan kodları içeren dosyaların uygulanmanın kurulum paketleri içerisindeki yolları

Sürüm Numarası	Dosya Yolları
2.0.0	smalinetclient\lock\app\two\df\smali
1.1.7	smalinetclient\lock\app\two\df\smali
1.1.6	smalinetclient\lock\df\smali
1.1.3	smalinetclient\lock\df\smali

Uygulama istemcileri arasındaki 2048 bitlik asimetrik "RSA/ECB/OAEPWithSHA-1andMGF1Padding" algoritmasına dair fonksiyonları içeren "smali" dosyaların 4 ayrı uygulama sürümüne ait kurulum paketleri içerisindeki yollarına aşağıdaki tabloda yer verilmiştir:



Sürüm Numarası	Dosya Yolları
1.1.3	small\net\client\by\lock\dq\small
1.1.6	small\net\client\by\lock\dq\small
1.1.7	small\net\client\by\lock\dq\small
2.0.0	small\net\client\by\lockapp\two\dq\small

**Tablo -** Asimetrik gizli anahtarın şifrelenmesi için kullanılan kodları içeren dosyaların uygulamamızın kurulum paketleri içerisindeki yolları

“SHA256” ve “AES/CBC/PKCS5Padding” kriptografik algoritmalarının kullanılmalarına ait kaynak kodların bir kısmı aşağıda sunulmuştur:

```
.method public constructor <init>([B[B)V
    .locals 8
    .prologue
    .line 59
    invoke-direct {p0}, Lnet/client/by/lock/d/f;-><init>()V
    .line 60
    put-object p2, p0, Lnet/client/by/lock/d/q;-->f:[B
    .line 61
    const/4 v1, 0x0
    .line 63
    :try_start_0
    const-string v0, "SHA-256"
    invoke-static {v0}, Ljava/security/MessageDigest;
    >getInstance(Ljava/lang/String;)Ljava/security/MessageDigest;
    move-result-object v0
    .line 64
    invoke-static {}, Lnet/client/by/lock/d/r;-
    <i>Lnet/client/by/lock/d/r;
    move-result-object v2
    invoke-virtual {v2}, Lnet/client/by/lock/d/r;->1()Ljava/lang/String;
    move-result-object v2
    invoke-virtual {v2}, Ljava/lang/String;-->getBytes() [B
    move-result-object v2
    invoke-virtual {v0, v2}, Ljava/security/MessageDigest;-->update([B)V
    .line 65
    invoke-virtual {v0}, Ljava/security/MessageDigest;-->digest() [B
    move-result-object v0
    .line 66
    const-string v2, "AES/CBC/PKCS5Padding"
    invoke-static {v2}, Ljava/security/MessageDigest;
    >getInstance(Ljava/lang/String;)Ljava/security/MessageDigest;
    >getInstance(Ljava/lang/String;)Ljava/security/MessageDigest;
```

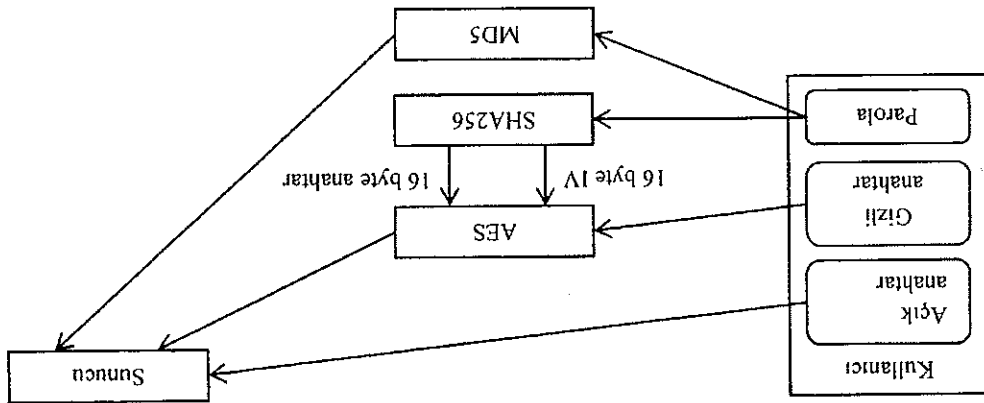
```

move-result-object v2
    .line 67
    const/4 v3, 0x2
    new-instance v4, Ljavax/crypto/spec/SecretKeySpec;
    const/4 v5, 0x0
    const/16 v6, 0x10
    const-string v7, "AES"
    invoke-direct {v4, v0, v5, v6, v7}, Ljavax/crypto/spec/SecretKeySpec;
    <<init>([BII)V
    new-instance v5, Ljavax/crypto/spec/IVParametersSpec;
    .line 68
    array-length v6, v0
    add-int/lit8 v6, v6, -0x10
    const/16 v7, 0x10
    invoke-direct {v5, v0, v6, v7}, Ljavax/crypto/spec/IVParametersSpec;
    <<init>([BII)V

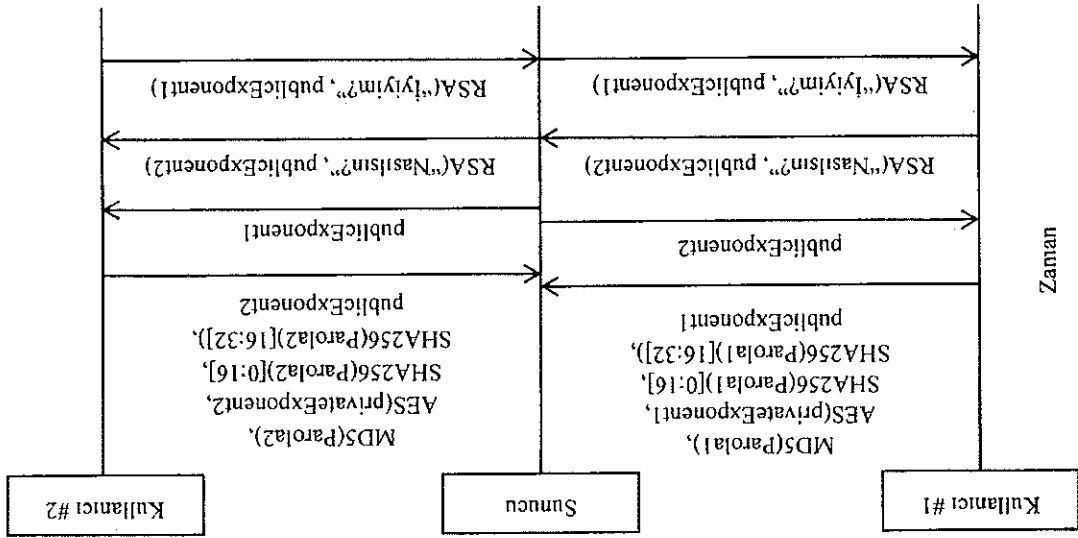
```

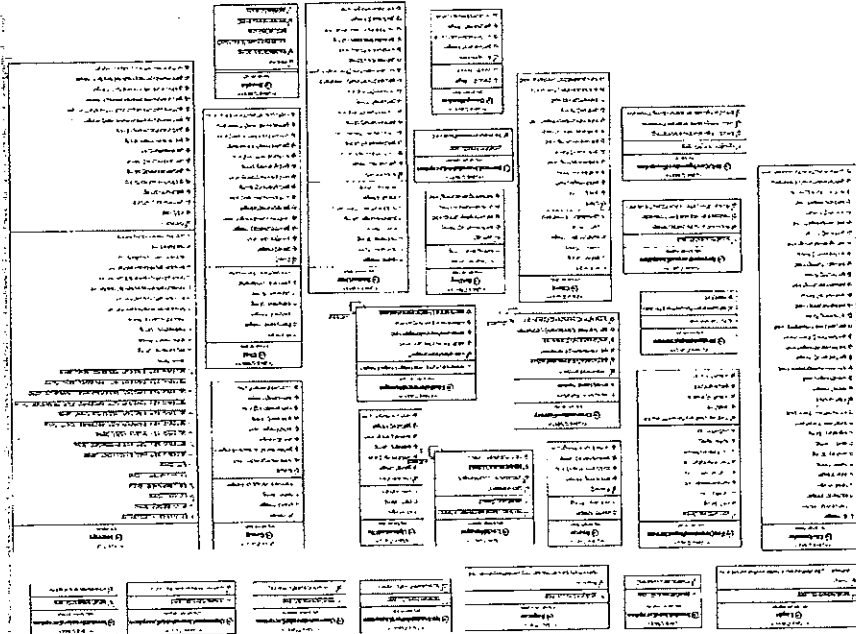
## Ek-7: Kayıt ve İki Kullanıcı Arasındaki Şifreli Mesajlaşmaya Ait Akış Şeması

Kayıt olan kullanıcıdan sunucuya gönderilen kriptografik değişkenler/anahtarlar akış şeması:

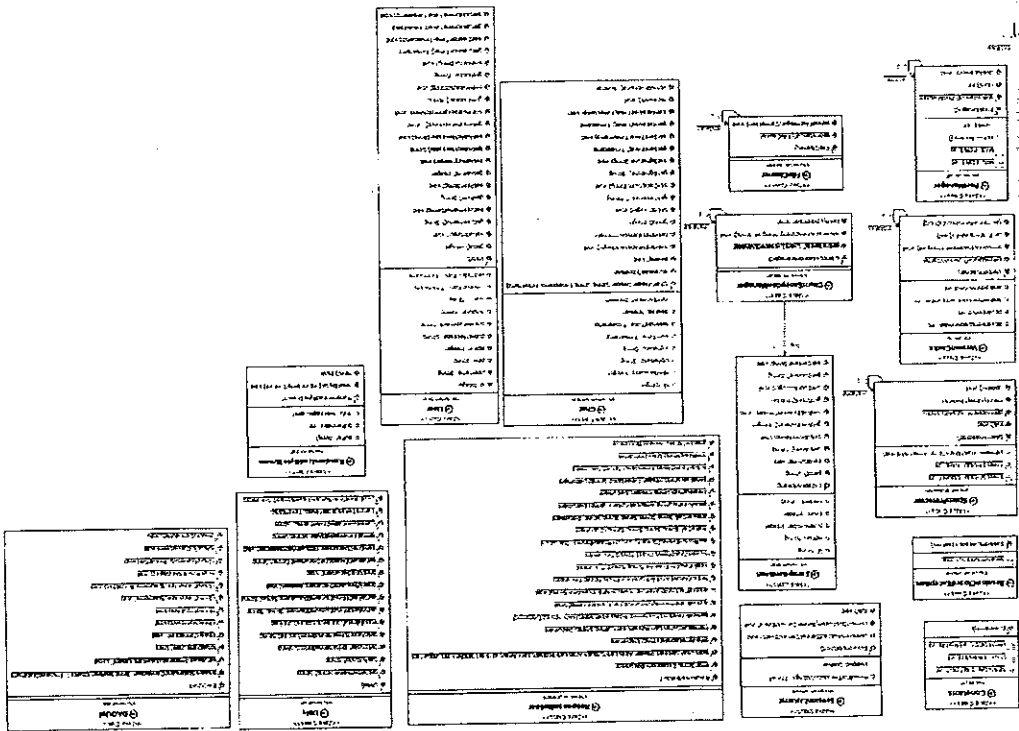


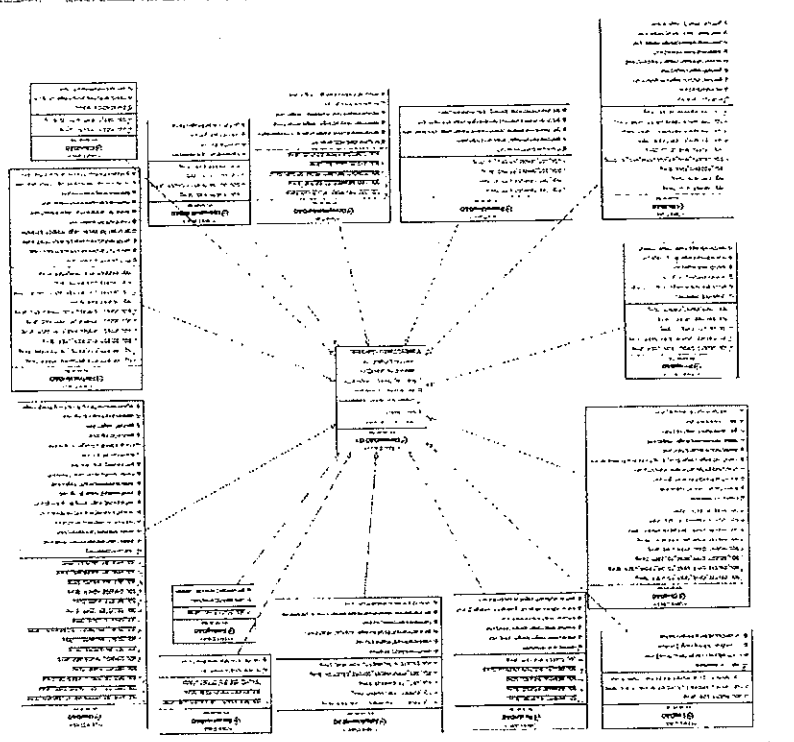
İki kullanıcı arasındaki şifreli mesajlaşmaya dair akış şeması:

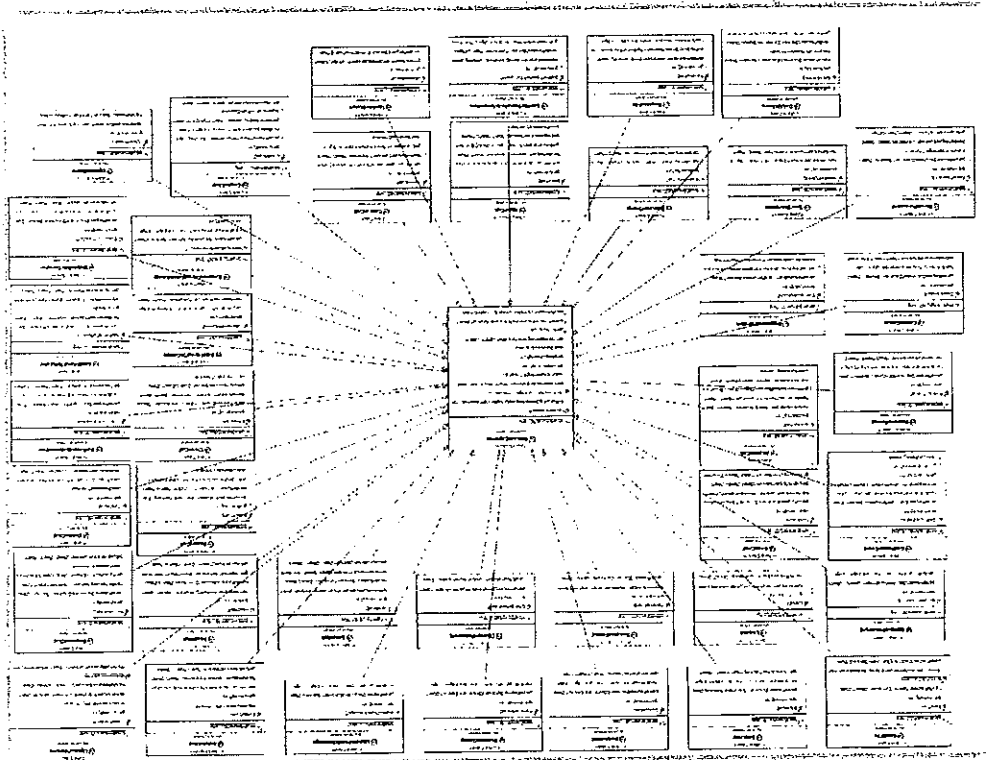


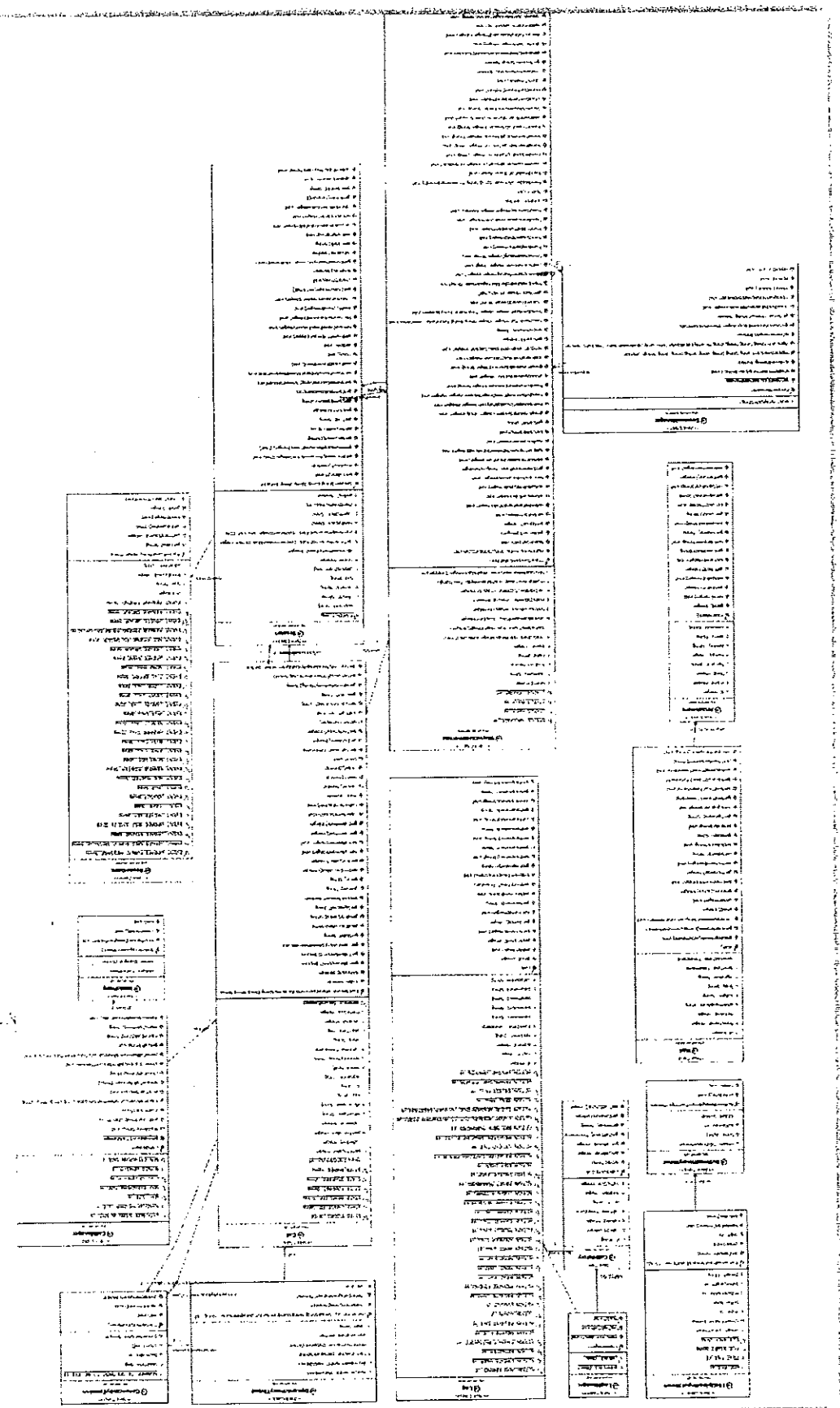


Bk-8: Uygulama Sunucusu Yazılım Modeli











```

package shu.server.listener;

import java.io.BufferedReader;
import java.io.File;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.net.URL;
import java.net.URLConnection;
import java.net.URLEncoder;
import java.util.ArrayList;
import java.util.Date;
import java.util.HashMap;
import java.util.List;
import java.util.Map;
import java.util.Random;
import java.util.StringTokenizer;
import java.util.zip.ZipEntry;
import java.util.zip.ZipOutputStream;
import javax.servlet.ServletException;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import org.xml.sax.SAXException;
import org.xml.sax.helpers.DefaultHandler;
import shu.server.bean.Log;
import shu.server.dao.ClientsDAO;
import shu.server.dao.ConnectionFactory;
import shu.server.dao.GenericDAO;
import shu.server.log.LogManager;
import shu.server.protocol.ResponseBuilder;
import shu.server.session.InvalidSessionException;
import shu.server.session.Session;
import shu.server.session.SessionClosedException;
import shu.server.session.SessionManager;
import shu.server.util.FileUploadInputStream;
import shu.server.util.Utils;

@WebServlet("/uploadversion")
public class UploadVersion
    extends GenericListener
{
    private static final long serialVersionUID = 1L;

    protected int getactionid()
    {
        return 35;
    }

    protected boolean requiresAdminRight()
    {
        return true;
    }

    protected Object parseRequestDocument(Document requestDocument,
        Session session)
        throws RequestFormatException
    {
        return null;
    }

    protected Object handleRequest(Session session, Connection
        connection, Object requestParameter)
    {
    }
}

```

Ek-9: Uygulama Sunucusunda Çalışan Yazılımda Kastlanan Türkçe İfade

```

throws SQLException, sessionClosedException
{
return null;
}
private static void deleteFile(File file) {
try {
Files.delete(file, topath());
} catch (Exception ex) {
ex.printStackTrace();
}
}
protected void doPost(HttpServletRequest request,
HttpServletResponse response)
throws ServletException, IOException
{
String filename = System.nanoTime() + "-" + (new
Random().nextInt(9000) + 1000);
FileUploadInputStream fuis = null;
response.setCharacterEncoding("UTF-8");
Integer userID = null;
String sessionId = "";
String edition = "";
String version = "";
int buildNumber = -1;
String clientIP = request.getRemoteAddr();
document requestDocument = null;
session session = null;
connection connection = null;
try {
fuis = new FileUploadInputStream(request.getInputStream(),
filename);
catch (IOException e) {
e.printStackTrace();
return;
}
File uploadedFile = new File(fuis.getFilepath());
try {
requestDocument = fuis.createMultipartStream(fuis);
utils.checkRequest(requestDocument, true);
try {
userID =
Integer.valueOf(Integer.parseInt(utils.getValueOfFirstElement(requestDocument, "userid"), "userid"));
catch (NumberFormatException | RequestFormatException
localNumberFormatException) {}
sessionId = utils.getValueOfAttribute(requestDocument, "id");
session = SessionManager.getInstance().getSession(userID,
sessionId);
if (session == null) {
throw new InvalidSessionException();
}
session.check(clientIP);
}
}
}
if (!uploadedFile.exists()) {
}
}

```

```

throw new RequestFormatException("filecontent does not exist");
}
jarfile jf = new Jarfile(uploadedfile);
zipentry versionentry = jf.getentry("VERSION");
jf.close();
throw new RequestFormatException("VERSION file is missing");
}
InputStream versionInputStream =
jf.getInputStream(versionentry);
jf.close();
throw new RequestFormatException("VERSION file cannot be opened");
}
br = new Bufferedreader(new
InputStreamReader(versionInputStream));
String versionAndBuildNumber = br.readLine().trim();
br.close();
StringTokenizer tokenizer = new
StringTokenizer(versionAndBuildNumber, "-");
if (tokenizer.countTokens() == 2) {
version = tokenizer.nextToken();
try {
buildNumber = Integer.parseInt(tokenizer.nextToken());
} catch (NumberFormatException localNumberFormatException1) {}
}
} catch (NumberFormatException localNumberFormatException1) {}
}
jf.close();
}
throw new RequestFormatException("invalid version
information in VERSION file!");
} catch
(SAXException|ParserConfigurationException|InvalidSessionException
e) {
e.printStackTrace();
deletefile(uploadedfile);
return;
} catch (RequestFormatException e) {
return;
} catch (ResponseBuilder.error(error(sessionId, new
Utils.sendxml(ResponseBuilder.error(sessionId, new
Exception("yatkini z yok!")), response);
deletefile(uploadedfile);
return;
}
int clientid = -1;
try {
connection = ConnectionFactory.getConnection();
ClientDAO cdao =
ClientDAO(ClientDAO.class, connection);
}
}
}

```

```
clientid = cdao.insertClient(editon, version,
Integer.valueOf(builidNumber), uploadedFile.getAbsolutePath());
versioncache.getInstance().versionUploaded(clientid, editon,
builidNumber);
} catch (SQLException e) {
    e.printStackTrace();
    deleteUploadedFile();
    if (connection != null) {
        try {
            connection.rollback();
        } catch (SQLException e1) {
            e1.printStackTrace();
        }
    }
    return;
} finally {
    if (connection != null) {
        try {
            connection.close();
        } catch (SQLException e) {
            e.printStackTrace();
        }
    }
}
Log log = (Log)super.getLogInstances(session, null, null);
log.setParameter1(clientid);
logManager.logAction(log);
Utils.sendxml(ResponseBulder.defaultResponse(sessionId),
response);
}
```

## EK-10: Uygulama Sunucusunda Engellenen IP Adresleri Listesi

İP Blokları	Türkiye
5.2.80.0/21	Türkiye
5.11.128.0/17	Türkiye
5.23.120.0/21	Türkiye
5.24.0.0/14	Türkiye
5.44.80.0/20	Türkiye
5.44.144.0/20	Türkiye
5.46.0.0/15	Türkiye
5.63.32.0/19	Türkiye
5.104.0.0/20	Türkiye
5.159.248.0/21	Türkiye
5.176.0.0/15	Türkiye
5.226.192.0/18	Türkiye
5.229.0.0/16	Türkiye
5.250.240.0/20	Türkiye
5.255.0.0/18	Türkiye
24.133.0.0/16	Türkiye
31.3.0.0/21	Türkiye
31.6.80.0/20	Türkiye
31.7.32.0/21	Türkiye
31.25.168.0/21	Türkiye
31.44.192.0/20	Türkiye
31.140.0.0/14	Türkiye
31.145.0.0/16	Türkiye
31.155.0.0/16	Türkiye
31.169.64.0/19	Türkiye
31.176.0.0/17	Türkiye
31.177.128.0/17	Türkiye
31.186.0.0/19	Türkiye
31.192.208.0/21	Türkiye
31.200.0.0/17	Türkiye
31.206.0.0/16	Türkiye
31.207.80.0/21	Türkiye
31.210.32.0/19	Türkiye
31.210.64.0/18	Türkiye
31.210.152.0/21	Türkiye
31.214.129.0/24	Almanya
31.214.152.0/24	Almanya
31.223.0.0/17	Türkiye
37.1.144.0/21	Hollanda
37.9.200.0/21	Türkiye
37.34.0.0/19	Türkiye

37.58.16.0/21	Türkiye
37.72.48.0/20	Türkiye
37.75.8.0/21	Türkiye
37.77.0.0/19	Türkiye
37.122.136.0/21	Türkiye
37.122.224.0/20	Türkiye
37.123.0.0/18	Türkiye
37.123.96.0/21	Türkiye
37.130.64.0/18	Türkiye
37.131.248.0/21	Türkiye
37.140.208.0/21	Türkiye
37.148.208.0/21	Türkiye
37.152.72.0/21	Türkiye
37.154.0.0/15	Türkiye
37.202.48.0/21	Türkiye
37.205.0.0/21	Türkiye
37.218.192.0/20	Kıbrıs
37.230.104.0/21	Türkiye
37.235.72.0/21	Türkiye
37.247.96.0/20	Türkiye
37.247.112.0/21	Türkiye
46.1.0.0/16	Türkiye
46.2.0.0/16	Türkiye
46.17.128.0/21	Türkiye
46.20.0.0/20	Türkiye
46.20.144.0/20	Türkiye
46.28.232.0/21	Türkiye
46.30.176.0/21	Türkiye
46.31.112.0/21	Türkiye
46.31.144.0/21	Türkiye
46.45.128.0/18	Türkiye
46.104.0.0/16	Türkiye
46.106.0.0/16	Türkiye
46.154.0.0/15	Türkiye
46.182.64.0/21	Türkiye
46.196.0.0/15	Türkiye
46.221.0.0/16	Türkiye
46.234.0.0/19	Türkiye
46.235.8.0/21	Türkiye
46.245.160.0/21	Türkiye
46.252.96.0/20	Türkiye
46.254.48.0/21	Türkiye

62.29.0.0/17	Türkiye
62.108.64.0/19	Türkiye
62.244.192.0/18	Türkiye
62.248.0.0/17	Türkiye
77.72.184.0/21	Türkiye
77.73.216.0/21	Türkiye
77.75.32.0/21	Türkiye
77.75.216.0/21	Türkiye
77.79.64.0/18	Türkiye
77.92.96.0/19	Türkiye
77.92.128.0/19	Türkiye
77.223.128.0/19	Türkiye
77.245.144.0/20	Türkiye
78.40.224.0/21	Türkiye
78.111.96.0/20	Türkiye
78.135.0.0/22	Türkiye
78.135.4.0/22	Türkiye
78.135.8.0/21	Türkiye
78.135.16.0/20	Türkiye
78.135.32.0/19	Türkiye
78.135.64.0/18	Türkiye
78.160.0.0/11	Türkiye
79.98.128.0/21	Türkiye
79.99.176.0/21	Türkiye
79.123.128.0/17	Türkiye
79.170.168.0/21	Türkiye
79.171.16.0/21	Türkiye
80.93.208.0/20	Türkiye
80.251.32.0/20	Türkiye
80.253.240.0/20	Türkiye
81.6.64.0/18	Türkiye
81.8.0.0/17	Türkiye
81.21.160.0/20	Türkiye
81.22.96.0/20	Türkiye
81.91.112.0/20	Türkiye
81.212.0.0/14	Türkiye
82.145.224.0/19	Türkiye
82.150.64.0/19	Türkiye
82.151.128.0/19	Türkiye
82.222.0.0/16	Türkiye
83.66.0.0/16	Türkiye
84.17.64.0/19	Türkiye

176.30.0.0/16	Türkiye
176.33.0.0/16	Türkiye
176.40.0.0/14	Türkiye
176.53.0.0/17	Türkiye
176.54.0.0/15	Türkiye
176.88.0.0/14	Türkiye
176.216.0.0/14	Türkiye
176.220.0.0/16	Türkiye
176.227.0.0/17	Türkiye
176.232.0.0/15	Türkiye
176.234.0.0/15	Türkiye
176.236.0.0/16	Türkiye
176.237.0.0/16	Türkiye
176.238.0.0/15	Türkiye
176.240.0.0/16	Türkiye
178.18.192.0/20	Türkiye
178.20.224.0/21	Türkiye
178.22.8.0/21	Türkiye
178.132.48.0/21	Türkiye
178.210.160.0/19	Türkiye
178.211.32.0/19	Türkiye
178.211.192.0/19	Türkiye
178.233.0.0/16	Türkiye
178.240.0.0/13	Türkiye
178.250.88.0/21	Türkiye
178.251.40.0/21	Türkiye
185.3.56.0/22	Türkiye
185.4.68.0/22	Türkiye
185.4.208.0/22	Türkiye
185.4.224.0/22	Türkiye
185.5.176.0/22	Türkiye
185.7.0.0/22	Türkiye
185.7.80.0/22	İngiltere
185.7.176.0/22	Türkiye
185.8.12.0/22	Türkiye
185.8.32.0/22	Türkiye
185.8.128.0/22	Türkiye
185.9.36.0/22	Türkiye
185.9.156.0/22	Türkiye
185.9.220.0/22	Türkiye
185.11.12.0/22	Türkiye
185.11.212.0/22	Türkiye
185.11.248.0/22	Türkiye
185.12.108.0/22	Türkiye
185.12.224.0/22	Türkiye

93.190.120.0/21	Türkiye
93.190.216.0/21	Türkiye
94.46.0.0/21	Portekiz
94.46.32.0/21	Türkiye
94.54.0.0/15	Türkiye
94.73.128.0/18	Türkiye
94.78.64.0/18	Türkiye
94.79.64.0/18	Türkiye
94.101.80.0/20	Türkiye
94.102.0.0/20	Türkiye
94.102.64.0/20	Türkiye
94.103.32.0/20	Türkiye
94.120.0.0/14	Türkiye
94.138.192.0/19	Türkiye
94.199.32.0/21	Türkiye
94.199.200.0/21	Türkiye
94.235.0.0/16	Türkiye
95.0.0.0/12	Türkiye
95.65.128.0/17	Türkiye
95.70.128.0/17	Türkiye
95.128.56.0/21	Türkiye
95.130.168.0/21	Türkiye
95.142.128.0/20	Türkiye
95.173.0.0/19	Türkiye
95.173.160.0/19	Türkiye
95.173.224.0/19	Türkiye
95.183.128.0/17	Türkiye
109.228.192.0/18	Türkiye
109.230.196.0/24	Almanya
109.232.216.0/21	Türkiye
109.235.248.0/21	Türkiye
128.127.168.0/21	Türkiye
134.19.200.0/21	Türkiye
134.255.199.0/24	Almanya
141.196.0.0/16	Türkiye
146.185.96.0/19	Türkiye
149.0.0.0/16	Türkiye
149.140.0.0/16	Türkiye
151.135.0.0/16	Türkiye
151.250.0.0/16	Türkiye
159.20.64.0/19	Türkiye
159.20.112.0/21	Türkiye
159.146.0.0/17	Türkiye
159.253.32.0/20	Türkiye
159.253.80.0/21	Türkiye

84.44.0.0/17	Türkiye
84.51.0.0/18	Türkiye
85.29.0.0/18	Türkiye
85.95.224.0/19	Türkiye
85.96.0.0/12	Türkiye
85.119.32.0/21	Türkiye
85.119.64.0/21	Türkiye
85.153.0.0/16	Türkiye
85.158.96.0/21	Türkiye
85.159.64.0/21	Türkiye
85.159.72.0/21	Türkiye
85.235.64.0/19	Türkiye
86.108.128.0/17	Türkiye
87.251.0.0/19	Türkiye
88.224.0.0/11	Türkiye
89.19.0.0/19	Türkiye
89.106.0.0/19	Türkiye
89.107.224.0/21	Türkiye
89.145.184.0/21	Türkiye
89.252.128.0/18	Türkiye
90.158.0.0/15	Türkiye
91.93.0.0/16	Türkiye
91.102.160.0/21	Türkiye
91.109.208.0/21	Türkiye
91.151.80.0/20	Türkiye
91.191.160.0/20	Türkiye
92.42.32.0/21	Türkiye
92.43.80.0/21	Türkiye
92.44.0.0/15	Türkiye
92.61.0.0/20	Türkiye
92.63.0.0/20	Türkiye
93.89.16.0/20	Türkiye
93.89.64.0/20	Türkiye
93.89.224.0/20	Kıbrıs
93.91.64.0/20	Türkiye
93.93.24.0/21	Türkiye
93.94.192.0/21	Türkiye
93.94.248.0/21	Türkiye
93.95.176.0/21	Türkiye
93.155.0.0/17	Türkiye
93.182.64.0/18	Türkiye
93.184.144.0/20	Türkiye
93.186.112.0/20	Türkiye
93.187.64.0/21	Türkiye
93.187.200.0/21	Türkiye

185.13.56.0/22	Türkiye
185.14.20.0/22	Türkiye
185.14.64.0/22	Türkiye
185.14.172.0/22	Türkiye
185.15.40.0/22	Türkiye
185.15.196.0/22	Türkiye
185.16.236.0/22	Türkiye
185.17.112.0/22	Türkiye
185.17.136.0/22	Türkiye
185.19.80.0/22	Türkiye
185.19.92.0/22	Türkiye
185.21.4.0/22	Türkiye
185.21.204.0/22	Türkiye
185.22.56.0/22	Türkiye
185.22.100.0/22	Türkiye
185.22.160.0/22	Türkiye
185.22.184.0/22	Türkiye
185.22.248.0/22	Türkiye
185.23.72.0/22	Türkiye
185.24.80.0/22	İngiltere
185.24.124.0/22	Türkiye
185.25.100.0/22	Türkiye
185.26.68.0/22	Türkiye
185.26.144.0/22	Türkiye
185.28.0.0/22	Türkiye
185.28.60.0/22	Türkiye
185.28.132.0/22	Türkiye
185.28.160.0/22	Türkiye
185.29.120.0/22	Türkiye
185.29.192.0/22	Türkiye
185.32.12.0/22	Türkiye
185.33.60.0/22	Türkiye
185.33.108.0/22	Türkiye
185.33.128.0/22	Türkiye
185.33.232.0/22	Kıbrıs
185.34.128.0/22	Türkiye
185.35.20.0/22	Türkiye
185.40.72.0/22	Türkiye
185.40.84.0/22	Türkiye
185.42.172.0/22	Türkiye
185.43.228.0/22	Türkiye
185.44.192.0/22	Türkiye
185.46.40.0/22	Türkiye
185.46.52.0/22	Türkiye
185.48.24.0/22	Türkiye

185.48.180.0/22	Türkiye
185.48.212.0/22	Türkiye
185.49.44.0/22	Türkiye
185.49.68.0/22	Almanya
185.49.128.0/22	Türkiye
185.50.68.0/22	Türkiye
185.51.24.0/22	Kıbrıs
185.51.36.0/22	Türkiye
185.51.112.0/22	Türkiye
185.51.164.0/22	Türkiye
185.52.228.0/22	Türkiye
185.53.60.0/22	Türkiye
185.54.88.0/22	Türkiye
185.56.236.0/22	Türkiye
185.57.64.0/22	Türkiye
185.58.244.0/22	Türkiye
185.59.28.0/22	Türkiye
185.59.44.0/22	Türkiye
185.59.72.0/22	Türkiye
185.60.224.0/22	Türkiye
185.61.44.0/22	Türkiye
185.64.80.0/22	Türkiye
185.65.68.0/22	Türkiye
185.65.204.0/22	Türkiye
185.66.124.0/22	Türkiye
185.67.32.0/22	Türkiye
185.67.120.0/22	Türkiye
185.67.124.0/22	Türkiye
185.67.204.0/22	Türkiye
185.68.220.0/22	Türkiye
185.70.84.0/22	Türkiye
185.70.96.0/22	Türkiye
185.70.140.0/22	Türkiye
185.71.116.0/22	Türkiye
185.72.252.0/22	Türkiye
185.73.128.0/22	ABD
185.73.200.0/22	Türkiye
185.76.140.0/22	Türkiye
185.76.152.0/22	Türkiye
185.76.196.0/22	Türkiye
185.76.200.0/22	Türkiye
185.77.0.0/22	Türkiye
185.77.40.0/22	Türkiye
185.77.88.0/22	Türkiye

185.78.84.0/22	Türkiye
185.79.12.0/22	Türkiye
185.80.20.0/22	Türkiye
185.80.72.0/22	Türkiye
185.80.136.0/22	Türkiye
185.81.152.0/22	Türkiye
185.81.236.0/22	Türkiye
185.82.220.0/22	Türkiye
185.82.252.0/22	Türkiye
185.83.144.0/22	Türkiye
185.83.244.0/22	Türkiye
185.84.180.0/22	Türkiye
185.85.72.0/22	Türkiye
185.85.104.0/22	Türkiye
185.85.188.0/22	Türkiye
185.85.204.0/22	Türkiye
185.85.236.0/22	Türkiye
185.86.4.0/22	Türkiye
185.86.12.0/22	Türkiye
185.86.80.0/22	Türkiye
185.86.152.0/22	Türkiye
185.86.164.0/22	Türkiye
185.86.244.0/22	Türkiye
185.87.24.0/22	Türkiye
185.87.120.0/22	Türkiye
185.87.172.0/22	Türkiye
185.87.252.0/22	Türkiye
185.88.4.0/22	Türkiye
185.88.172.0/22	Türkiye
185.90.4.0/22	Türkiye
185.90.80.0/22	Türkiye
185.90.240.0/22	Türkiye
185.92.0.0/22	Türkiye
185.92.12.0/22	Türkiye
185.92.212.0/22	Türkiye
185.93.52.0/22	Türkiye
185.93.68.0/22	Türkiye
185.93.248.0/22	Türkiye
185.95.0.0/22	Türkiye
185.95.84.0/22	Türkiye
185.95.120.0/22	Türkiye
185.95.168.0/22	Türkiye
185.96.52.0/22	Türkiye
185.96.112.0/22	Türkiye
185.96.168.0/22	Türkiye

195.142.244.0/22	Türkiye
195.142.248.0/21	Türkiye
195.155.0.0/18	Türkiye
195.155.64.0/19	Türkiye
195.155.96.0/22	Türkiye
195.155.100.0/22	Türkiye
195.155.104.0/21	Türkiye
195.155.112.0/20	Türkiye
195.155.128.0/19	Türkiye
195.155.160.0/19	Türkiye
195.155.192.0/18	Türkiye
195.174.0.0/16	Türkiye
195.175.0.0/16	Türkiye
195.214.128.0/18	Türkiye
195.244.32.0/19	Türkiye
212.2.192.0/19	Türkiye
212.12.128.0/19	Türkiye
212.15.0.0/19	Türkiye
212.29.64.0/18	Türkiye
212.31.0.0/19	Türkiye
212.50.32.0/19	Türkiye
212.57.0.0/19	Türkiye
212.58.0.0/19	Türkiye
212.64.192.0/19	Türkiye
212.65.128.0/19	Türkiye
212.68.32.0/19	Türkiye
212.98.0.0/19	Türkiye
212.98.192.0/18	Türkiye
212.101.96.0/19	Türkiye
212.108.128.0/19	Türkiye
212.109.96.0/19	Türkiye
212.109.224.0/19	Türkiye
212.115.0.0/19	Türkiye
212.125.0.0/19	Türkiye
212.127.96.0/19	Türkiye
212.133.128.0/17	Türkiye
212.146.128.0/17	Türkiye
212.154.0.0/17	Türkiye
212.156.0.0/16	Türkiye
212.174.0.0/16	Türkiye
212.175.0.0/16	Türkiye
212.252.0.0/16	Türkiye
212.253.0.0/16	Türkiye
213.14.0.0/17	Türkiye
213.14.128.0/20	Türkiye

188.56.0.0/14	Türkiye
188.64.208.0/21	Türkiye
188.95.144.0/21	Türkiye
188.119.0.0/18	Türkiye
188.124.0.0/19	Türkiye
188.125.160.0/19	Türkiye
188.132.128.0/17	Türkiye
193.140.0.0/16	Türkiye
193.192.96.0/19	Türkiye
193.243.192.0/19	Türkiye
193.255.0.0/16	Türkiye
194.27.0.0/16	Türkiye
194.54.32.0/19	Türkiye
195.33.192.0/18	Türkiye
195.46.128.0/19	Türkiye
195.87.0.0/16	Türkiye
195.112.128.0/19	Türkiye
195.142.0.0/22	Türkiye
195.142.4.0/22	Türkiye
195.142.8.0/21	Türkiye
195.142.16.0/20	Türkiye
195.142.32.0/19	Türkiye
195.142.64.0/19	Türkiye
195.142.96.0/21	Türkiye
195.142.104.0/21	Türkiye
195.142.112.0/20	Türkiye
195.142.128.0/22	Türkiye
195.142.132.0/22	Türkiye
195.142.136.0/21	Türkiye
195.142.144.0/21	Türkiye
195.142.152.0/22	Türkiye
195.142.156.0/22	Türkiye
195.142.160.0/20	Türkiye
195.142.176.0/21	Türkiye
195.142.184.0/22	Türkiye
195.142.188.0/22	Türkiye
195.142.192.0/22	Türkiye
195.142.196.0/22	Türkiye
195.142.200.0/22	Türkiye
195.142.204.0/22	Türkiye
195.142.212.0/22	Türkiye
195.142.216.0/21	Türkiye
195.142.224.0/20	Türkiye
195.142.240.0/22	Türkiye

185.96.192.0/22	Türkiye
185.97.8.0/22	Türkiye
185.98.60.0/22	Türkiye
185.98.136.0/22	Türkiye
185.98.216.0/22	Türkiye
185.98.252.0/22	Türkiye
185.99.20.0/22	Türkiye
185.102.36.0/22	Türkiye
185.103.196.0/22	Türkiye
185.104.20.0/22	Türkiye
185.105.68.0/22	Türkiye
185.106.20.0/22	Türkiye
185.106.208.0/22	Türkiye
185.107.132.0/22	Türkiye
185.108.124.0/22	Türkiye
185.108.148.0/22	Türkiye
185.108.156.0/22	Türkiye
185.109.28.0/22	Türkiye
185.110.240.0/22	Türkiye
185.111.232.0/22	Türkiye
185.111.244.0/22	Türkiye
185.113.8.0/22	Türkiye
185.113.220.0/22	Türkiye
185.114.20.0/22	Türkiye
185.114.192.0/22	Türkiye
185.115.40.0/22	Türkiye
185.115.208.0/22	Türkiye
185.116.152.0/22	Türkiye
185.117.120.0/22	Türkiye
185.118.140.0/22	Türkiye
185.118.192.0/22	Türkiye
185.119.80.0/22	Türkiye
185.121.124.0/22	Türkiye
185.122.12.0/22	Türkiye
185.122.200.0/22	Türkiye
185.123.0.0/22	Türkiye
185.123.100.0/22	Türkiye
185.123.104.0/22	Türkiye
185.124.84.0/22	Türkiye
185.125.32.0/22	Türkiye
185.126.176.0/22	Türkiye
185.126.216.0/22	Türkiye
188.3.0.0/16	Türkiye
188.38.0.0/16	Türkiye
188.41.0.0/16	Türkiye



91.235.104.0/23	Türkiye
91.237.216.0/23	Türkiye
91.239.204.0/24	Türkiye
91.239.242.0/24	Türkiye
91.240.26.0/24	Türkiye
91.240.37.0/24	Türkiye
91.240.108.0/24	Türkiye
91.244.116.0/24	Türkiye
91.244.226.0/24	Türkiye
91.244.227.0/24	Türkiye
139.179.0.0/16	Türkiye
144.122.0.0/16	Türkiye
155.223.0.0/16	Türkiye
160.75.0.0/16	Türkiye
161.9.0.0/16	Türkiye
168.139.0.0/16	Türkiye
176.117.96.0/21	Türkiye
192.70.133.0/24	Hollanda
192.70.134.0/24	Hollanda
192.129.87.0/24	Türkiye
192.160.21.0/24	Türkiye
193.23.156.0/24	Türkiye
193.25.124.0/23	Türkiye
193.28.225.0/24	Türkiye
193.32.53.0/24	Türkiye
193.32.55.0/24	Türkiye
193.34.132.0/23	Türkiye
193.34.205.0/24	Türkiye
193.36.0.0/24	Türkiye
193.36.39.0/24	Türkiye
193.36.184.0/24	Türkiye
193.37.135.0/24	Türkiye
193.37.154.0/24	Türkiye
193.41.2.0/23	Türkiye
193.41.225.0/24	Türkiye
193.42.216.0/24	Türkiye
193.58.236.0/24	Türkiye
193.104.13.0/24	Türkiye
193.104.109.0/24	Türkiye
193.104.124.0/24	Türkiye
193.104.130.0/24	Türkiye
193.104.138.0/24	Türkiye
193.104.201.0/24	Türkiye
193.105.208.0/24	Türkiye
193.105.211.0/24	Türkiye

91.199.73.0/24	Türkiye
91.199.111.0/24	Türkiye
91.199.166.0/24	Türkiye
91.199.191.0/24	Türkiye
91.208.61.0/24	Türkiye
91.208.70.0/24	Türkiye
91.208.199.0/24	Türkiye
91.212.126.0/24	Türkiye
91.212.178.0/24	Türkiye
91.213.1.0/24	Türkiye
91.213.245.0/24	Türkiye
91.213.253.0/24	Türkiye
91.213.254.0/24	Türkiye
91.216.98.0/24	Türkiye
91.216.119.0/24	Türkiye
91.216.148.0/24	Türkiye
91.216.170.0/24	Türkiye
91.216.201.0/24	Türkiye
91.216.223.0/24	Türkiye
91.217.147.0/24	Türkiye
91.217.193.0/24	Türkiye
91.217.238.0/24	Türkiye
91.220.50.0/24	Türkiye
91.220.65.0/24	Türkiye
91.220.182.0/24	Türkiye
91.220.242.0/24	Türkiye
91.223.0.0/24	Türkiye
91.223.8.0/24	Türkiye
91.223.157.0/24	Türkiye
91.227.4.0/23	Türkiye
91.227.6.0/24	Türkiye
91.228.169.0/24	Türkiye
91.228.255.0/24	Türkiye
91.229.34.0/24	Türkiye
91.229.35.0/24	Türkiye
91.229.44.0/23	Türkiye
91.229.155.0/24	Türkiye
91.229.184.0/24	Türkiye
91.230.73.0/24	Türkiye
91.230.81.0/24	Türkiye
91.230.85.0/24	Türkiye
91.232.174.0/24	Türkiye
91.233.80.0/24	Türkiye
91.235.64.0/24	Türkiye

213.14.144.0/20	Türkiye
213.14.160.0/19	Türkiye
213.14.192.0/18	Türkiye
213.43.0.0/16	Türkiye
213.74.0.0/16	Türkiye
213.128.64.0/19	Türkiye
213.139.192.0/19	Türkiye
213.139.224.0/19	Türkiye
213.142.128.0/19	Türkiye
213.143.224.0/19	Türkiye
213.144.96.0/19	Türkiye
213.148.64.0/19	Türkiye
213.153.128.0/19	Türkiye
213.153.160.0/19	Türkiye
213.153.192.0/18	Türkiye
213.155.96.0/19	Türkiye
213.159.28.0/22	Türkiye
213.161.128.0/19	Türkiye
213.186.128.0/19	Türkiye
213.194.64.0/18	Türkiye
213.211.0.0/19	Türkiye
213.232.0.0/18	Türkiye
213.238.128.0/18	Türkiye
213.243.0.0/19	Türkiye
213.243.32.0/19	Türkiye
213.248.128.0/18	Türkiye
213.254.128.0/19	Türkiye
217.17.144.0/20	Türkiye
217.31.224.0/20	Türkiye
217.31.240.0/20	Türkiye
217.64.208.0/20	Türkiye
217.65.176.0/20	Türkiye
217.68.208.0/20	Türkiye
217.74.24.0/21	Türkiye
217.78.96.0/20	Türkiye
217.116.192.0/20	Türkiye
217.131.0.0/16	Türkiye
217.169.192.0/20	Türkiye
217.174.32.0/20	Türkiye
217.195.192.0/20	Türkiye
91.142.142.0/24	Türkiye
91.195.138.0/23	Türkiye
91.198.49.0/24	Türkiye
91.198.61.0/24	Türkiye
91.198.124.0/24	Türkiye

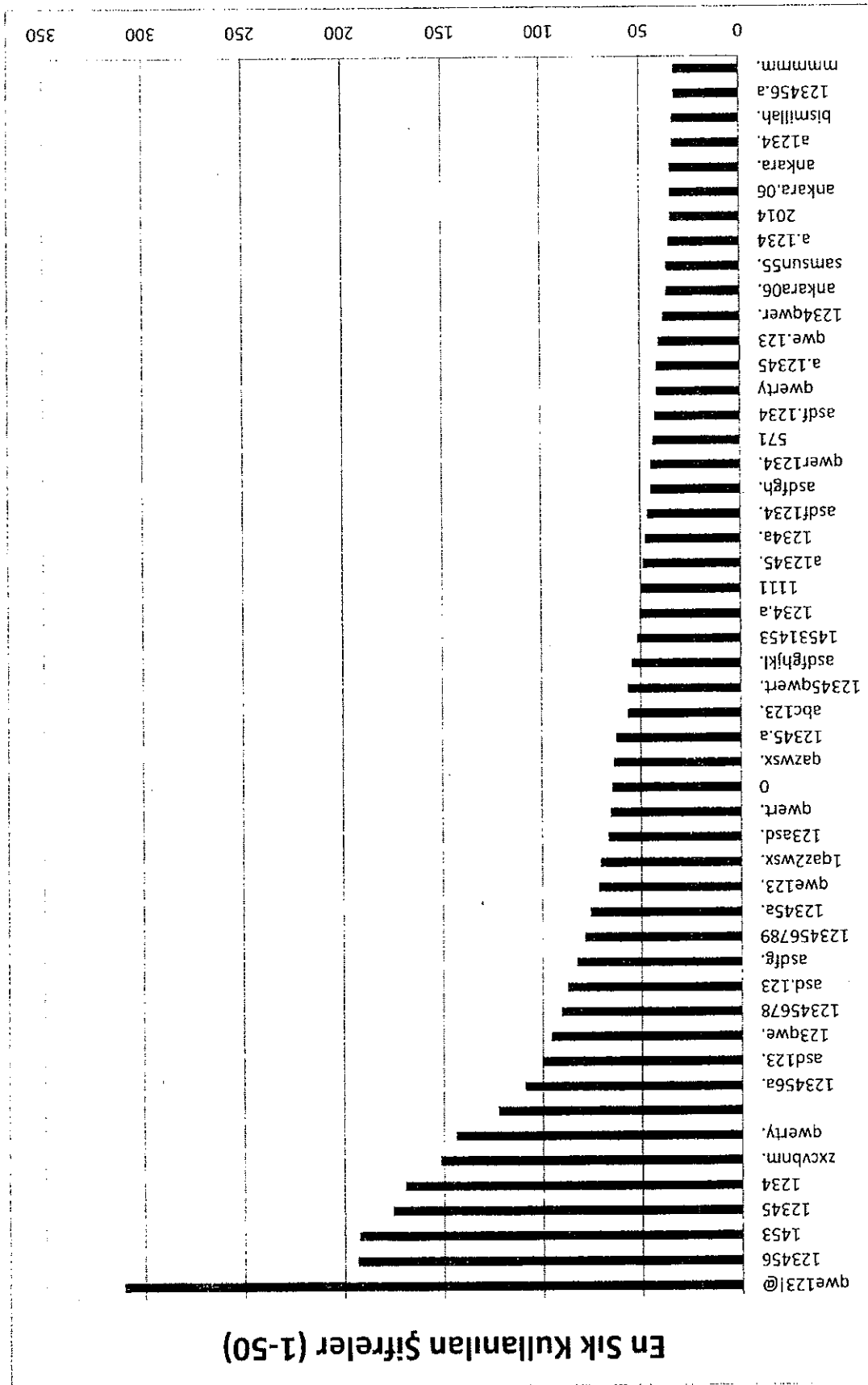
193.105.234.0/24	Türkiye
193.105.243.0/24	Türkiye
193.108.213.0/24	Türkiye
193.109.134.0/23	Türkiye
193.110.170.0/23	Türkiye
193.110.208.0/21	Türkiye
193.138.116.0/24	Türkiye
193.143.226.0/24	Türkiye
193.164.9.0/24	Türkiye
193.169.50.0/24	Türkiye
193.186.208.0/24	Türkiye
193.189.142.0/24	Türkiye
193.200.170.0/24	Türkiye
193.200.180.0/24	Türkiye
193.200.188.0/24	Türkiye
193.202.18.0/24	Türkiye
193.202.18.0/24	Türkiye
193.202.120.0/24	Türkiye
193.218.113.0/24	Türkiye
193.223.76.0/24	Türkiye
193.238.25.0/24	Türkiye
193.254.228.0/23	Türkiye
193.254.252.0/23	Türkiye
194.0.130.0/24	Türkiye
194.0.142.0/24	Türkiye
194.0.178.0/24	Türkiye
194.0.202.0/24	Türkiye
194.24.168.0/23	Türkiye
194.24.224.0/23	Türkiye
194.29.208.0/21	Türkiye
194.32.84.0/23	Türkiye
194.36.160.0/24	Türkiye
194.49.126.0/24	Türkiye
194.50.84.0/24	Türkiye
194.50.179.0/24	Türkiye
194.60.73.0/24	Türkiye
194.107.22.0/24	Türkiye
194.110.150.0/24	Türkiye
194.110.213.0/24	Türkiye
194.125.232.0/22	Türkiye
194.126.230.0/24	Türkiye
194.140.227.0/24	Türkiye
194.156.165.0/24	Türkiye
194.242.32.0/24	Türkiye
194.247.59.0/24	Türkiye
195.8.109.0/24	Türkiye

195.39.224.0/23	Türkiye
195.49.216.0/21	Türkiye
195.62.35.0/24	Türkiye
195.85.242.0/24	Türkiye
195.85.255.0/24	Türkiye
195.95.149.0/24	Türkiye
195.95.160.0/24	Türkiye
195.95.179.0/24	Türkiye
195.128.32.0/21	Türkiye
195.137.222.0/23	Türkiye
195.140.196.0/22	Türkiye
195.149.85.0/24	Türkiye
195.149.116.0/24	Türkiye
195.177.206.0/23	Türkiye
195.182.25.0/24	Türkiye
195.182.42.0/24	Türkiye
195.190.20.0/24	Türkiye
195.191.118.0/23	Türkiye
195.200.222.0/24	Türkiye
195.216.232.0/24	Türkiye
195.226.196.0/24	Türkiye
195.226.221.0/24	Türkiye
195.234.52.0/24	Türkiye
195.234.165.0/24	Türkiye
195.245.227.0/24	Türkiye

## Ek-11: Çözümlenen Şifrelere İlişkin İstatistikî Veriler

215.092 adet kriptografik MD5 özetinden yaklaşık %85'i çözülenmiş olup en sık görülen 50 şifreye aşağıda yer verilmiştir:

Sıra no:	Şifre:	Sıra no:	Şifre:
1	qwe123!@	26	asdfghjkl.
2	123456	27	14531453
3	1453	28	1234.a
4	12345	29	1111
5	1234	30	a12345.
6	zxcvbnm.	31	1234a.
7	qwerty.	32	asdf1234.
8		33	qwer1234.
9	123456a.	34	asdfgh.
10	asd123.	35	571
11	123qwe.	36	asdf.1234
12	12345678	37	a.12345
13	asd.123	38	qwerty
14	asdfg.	39	qwe.123
15	123456789	40	1234qwer.
16	12345a.	41	samsun55.
17	qwe123.	42	ankara06.
18	1qaz2wsx.	43	a.1234
19	123asd.	44	ankara.
20	qwert.	45	ankara.06
21	0	46	2014
22	qazwsx.	47	bismillah.
23	12345.a	48	a1234.
24	12345qwert.	49	mmmmmm.
25	abc123.	50	123456.a

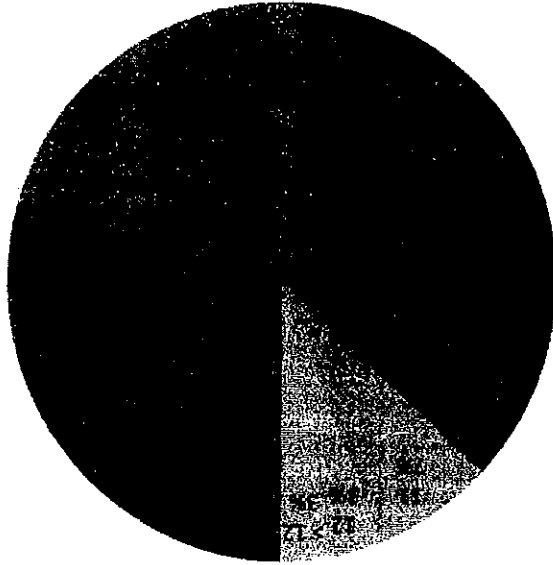


En Sık Kullanılan Şifreler (51-100)

qaz.wsx	0
qwert12345.	0
20022010	0
izmir.35	0
1qaz.2wsx	0
123abc.	0
qwel23@	0
1234567890	0
13579	0
1234asd.	0
qawsed.	0
fb.1907	0
bylock.	0
1qzW3e4r.	0
izmir35.	0
erzurum25.	0
123456789a.	0
5555	0
ahmet.	0
123456qwerty.	0
qazwsx	0
qwel23!	0
1453a.	0
123	0
istanbul34.	0
qaz123.	0
a.123456	0
fatih1453.	0
fatih.1453	0
Ankara06.	0
9999p.	0
feth1453.	0
qwer.1234	0
a123456.	0
1234.qwer	0
571632	0
yusuf.	0
12345s.	0
istanbul.34	0
1234asdt.	0
1234567	0
erzurum.25	0
12345.s	0
gs1905.	0
bjk1903.	0
adem1\$	0
mehmet.	0
manisa45.	0
mustafa.	0
123.abc	0
35	35

Çözümlenen şifrelerin yaklaşık yarısının uzunluğu 9 karakterden fazladır. Şifre uzunluklarına göre dağılım grafiği aşağıda sunulmuştur:

### Şifrelerin Uzunluklara Göre Dağılımı



Bu uzun şifre örnekleri:

- lqaz2wsx3edc4rfv5tgb6yhn7ujm8ik,9ol.0p
- Selam.2010-Selam.2010-
- tedbirleidenbirkakma.01
- qwertyuio1234567890@#\$
- asdfghjkl1234567890.....
- Pass.111111111111111111111111
- OlmakyadaoImamak123.
- YahafIz99.YahafIz99.