Kim Arıyor ?

written by Mert SARICA | 1 August 2015

Kasım 2013 tarihinde bir arkadaşım, CIA (Kim Arıyor?) mobil uygulaması hakkında bilgim olup olmadığını sordu. Bilgim olmadığını söylediğimde, bana arayan kişinin ekranda adını ve soyadını gösterdiğini ve bunu nasıl yaptığını merak ettiğini söyledi. Olsa olsa bu uygulamanın mobil cihaza yüklendiği anda telefon rehberinin bir kopyasını kendi sistemlerine gönderdiğini ve bunun üzerine çağrı geldiğinde rehber havuzda arayan numarayı sorgulayarak gösterebileceğini tahmin ettiğimi söyledim.

Uygulamayı kurup, inceledikten sonra telefon rehberinin aslında bu uygulamayı yükleyen kişinin insiyatifinde paylaşıldığını gördüm ve hemen kendi cep telefonu numaramı bu uygulamada üzerinden arattım. Beklediğim gibi telefon numarama sahip olan kişi veya kişiler, telefon rehberlerini paylaştıkları için benim adım ve soyadım da cep telefonum ile eşleştirilmişti. Yakın çevremdekilerin cep telefonu numaralarını da arattığımda bir arkadaşımın rehbere adı ve soyadı yerine ev adresi ile kaydedildiğini gördüm. Muhtemelen bu arkadaşımın sürekli sipariş verdiği ya bakkal ya çakkal telefon rehberine arkadaşımı bu şekilde kaydetmiş ve telefon rehberini de paylaşmıştı.

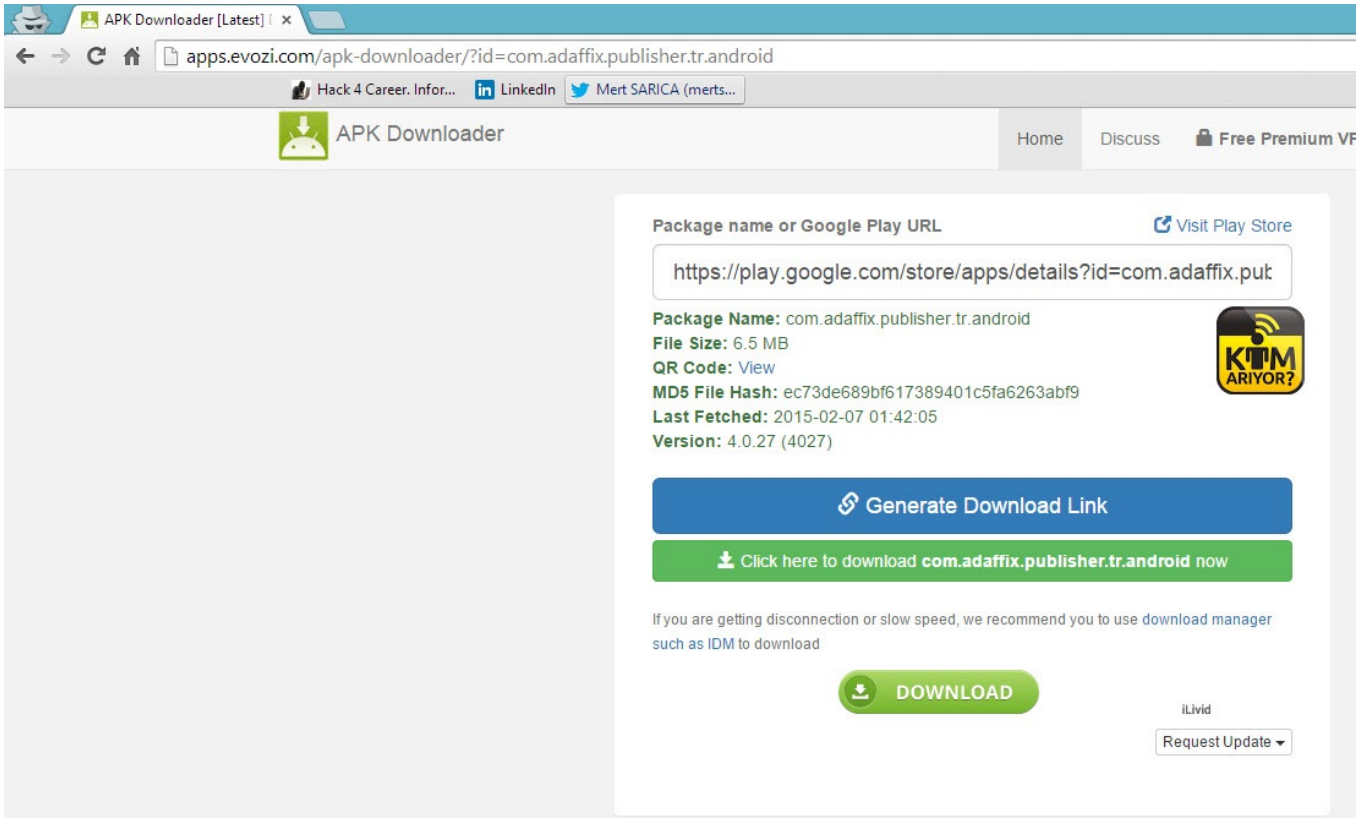
Mahremiyete ve güvenliğe önem verenler için, kendi rızası olmadan karşı tarafın (kişiler veya firmalar) insiyatifinde verilerinin 3. partilerle paylaşılması, satılması bilindiği üzere günümüzün en büyük sorunlarından bir tanesidir. Parayı verip, veriyi satın alan partilerin bu veriyi reklam dışında hangi amaçlarla kullandığını bilemediğimiz için verilerimize sahip çıkmaya çalışarak ileride başımıza gelebilecek potansiyel dolandırıcılık girişimlerinden kendimizi korumaya çalışmaktayız. Onlarca uyarıya rağmen kendini polis, jandarma, savcı olarak tanıtan dolandırıcılara karşı vatandaşlarımızın hala mağdur oluyor olması da, verilerimize neden sahip çıkmamız gerektiğinin önemini anlatıyor.

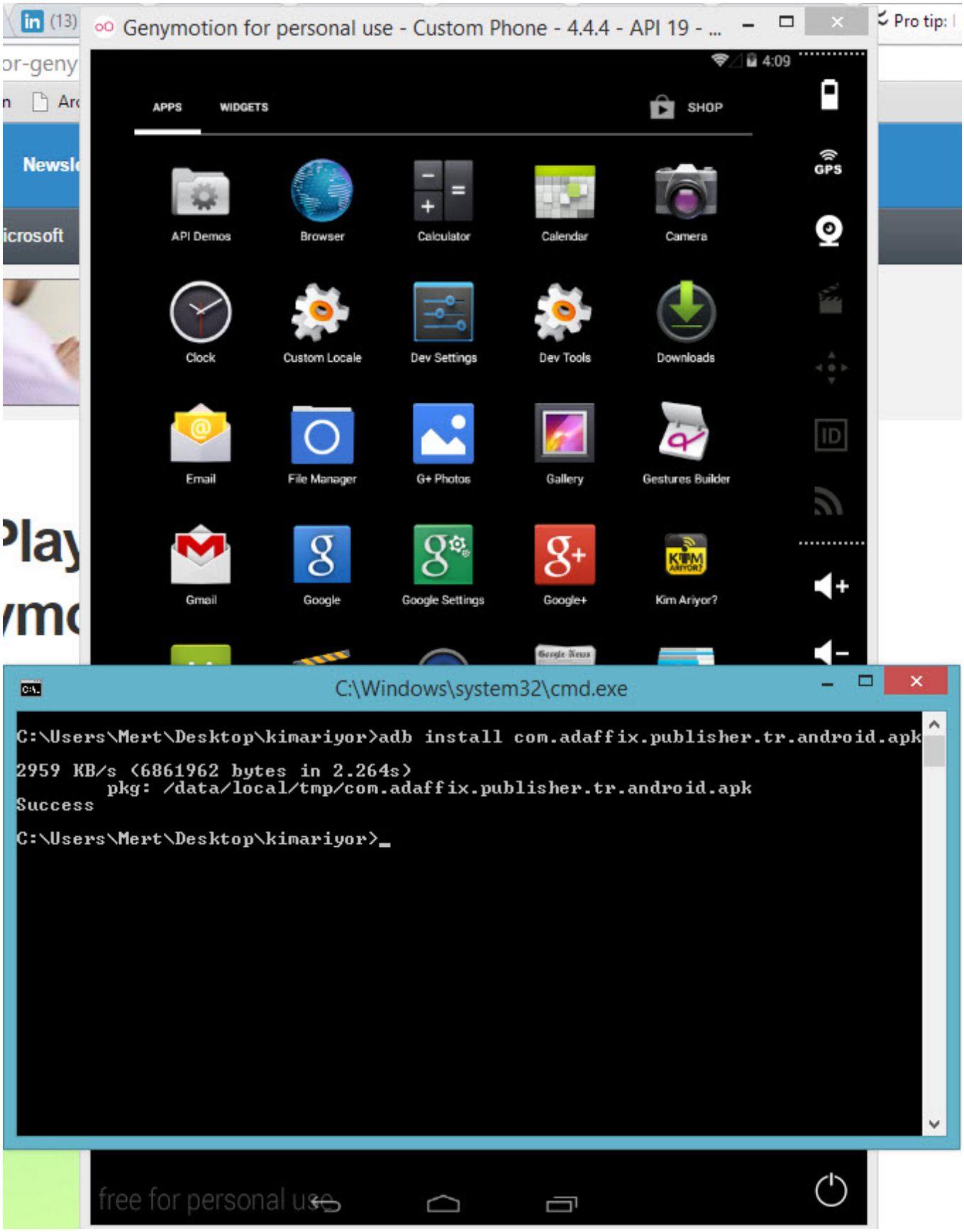
Bu arada 1 Mayıs 2015 tarihinde yürürlüğe giren Elektronik Ticaret yasası ile telefon, kısa mesaj ve e-posta ile izinsiz reklam yapanların 50.000 TL ‘ye varan para cezaları ödeyeceklerini de büyük bir memnuniyetle hatırlatmak isterim. Şikayet için T.C Gümrük ve Ticaret Bakanlığı’nın İleti Şikayet Sistemi‘ni ziyaret edebilirsiniz.

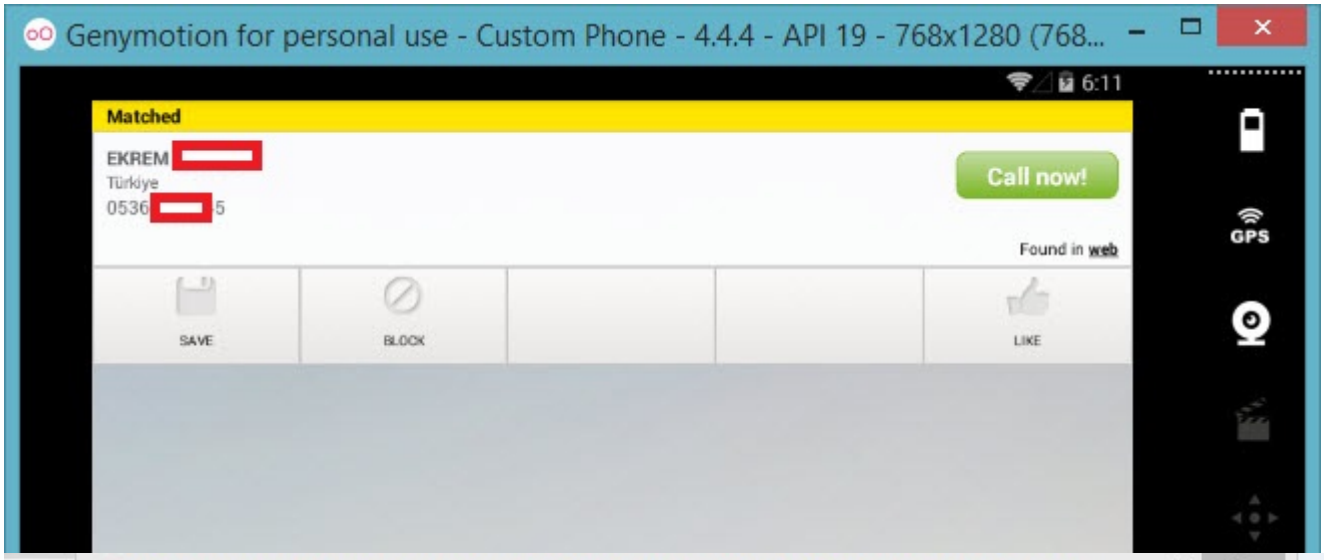
İyi, güzel de Mert, telefon rehberi paylaşımı ile telefon dolandırıcılığının

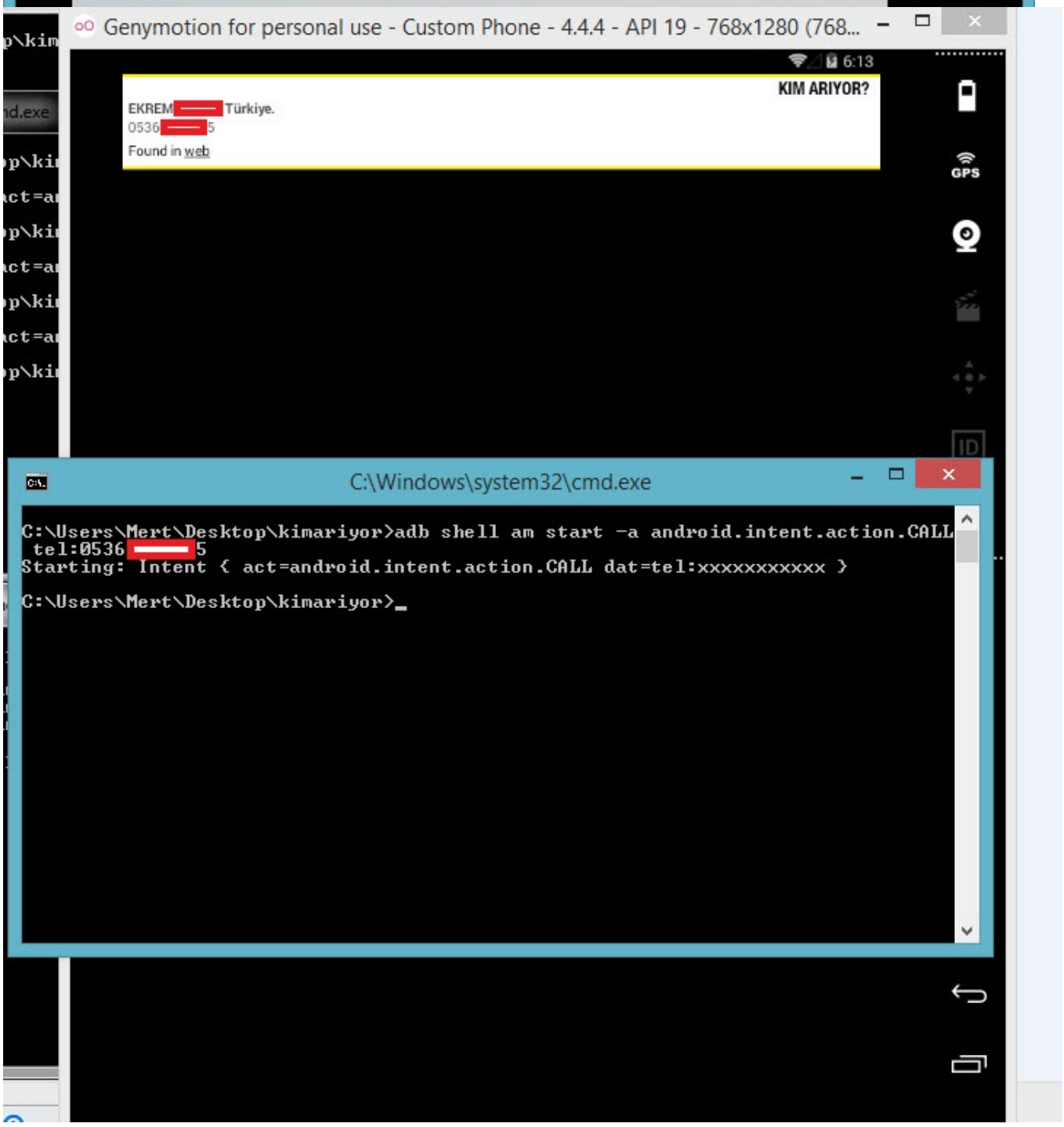
ne tür bir bağlantısı var diye soruyor olabilirsiniz. En basitinden sosyal mühendislik testinde olduğu gibi test öncesinde karşı taraf hakkında ne kadar çok bilgiye sahip olursanız, test esnasında karşı tarafı ikna etmeniz ve değerli bilgilere ulaşmanız o kadar kolay olur. Bundan yola çıkacak olursanız, size telefon açan bir dolandırıcı, size adınız ve soyadınız ile hitap ettiği zaman, sizi ikna etme ihtimali çok daha yüksek olacaktır. Bundan yola çıkarak art niyetli kişilerin, dolandırıcıların kısa bir sürede kim arıyor ve benzeri mobil uygulamaların, telefon rehberi havuzundan kısa sürede nasıl isim ve soyad bilgilerini temin edebileceğini öğrenmeye ve buna karşı sizleri ve yakınlarınızı bu konuda uyarmaya karar verdim.

Bunun için ilk işim, GenyMotion Android öykünücüsüne uygulamayı yüklemek oldu. Uygulamayı yükledikten sonra aklıma gelen rastgele bir cepe telefonu numarasını arattım ve karşıma o kişinin adı ve soyadı çıktı. Bir dolandırıcı olsa ve elinde yüzlerce belki de binlerce cep telefonu numarası olsa, bu uygulama üzerinden bu cep telefonlarına ait isim ve soyad bilgilerini toplu halde nasıl alabilirdi diye düşünürken, öykünücüye dışarıdan çağrı gönderilebildiği geldi.

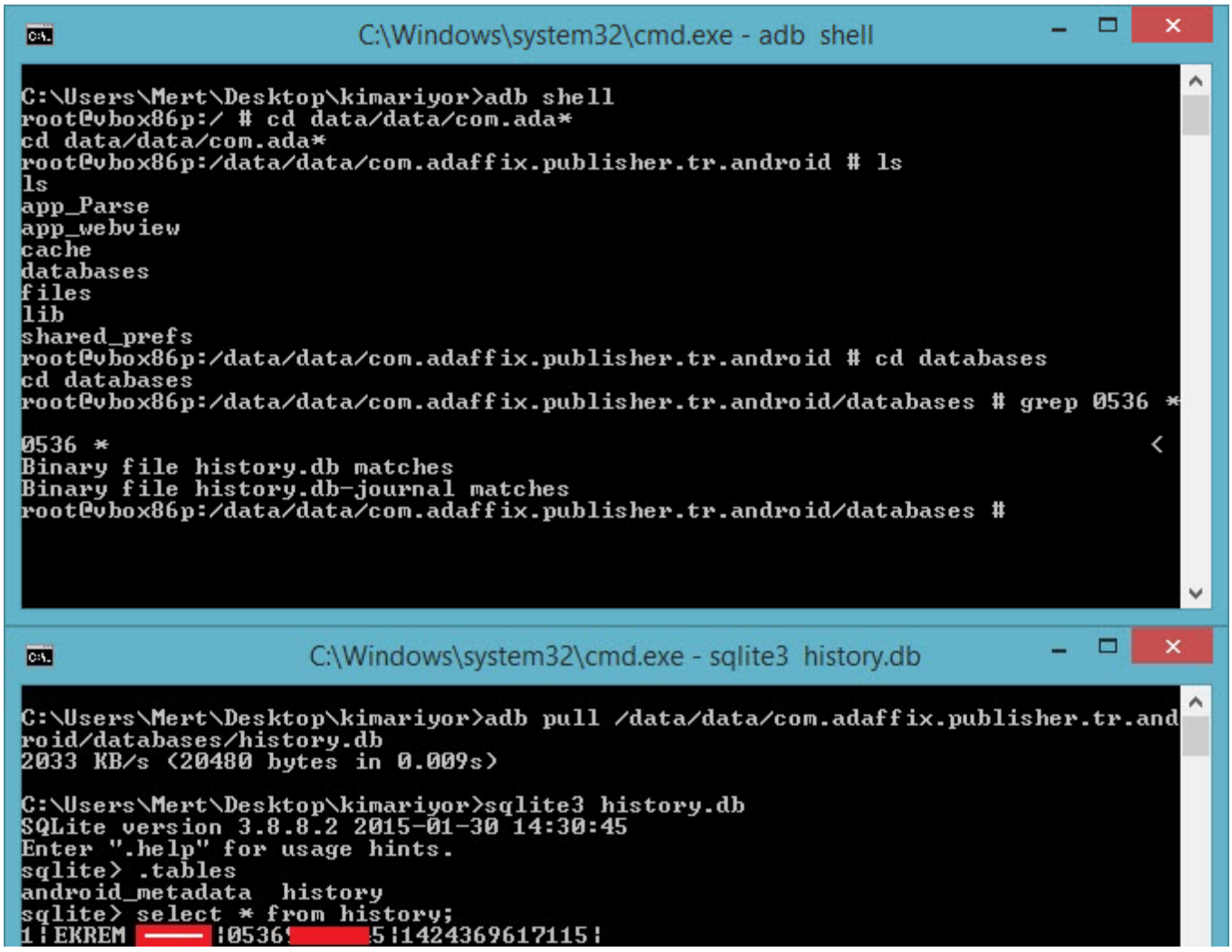



Genymotion for personal use - Custom Phone - 4.4.4 - API 19 - ...
4:09
APPS
WIDGETS
SHOP
API Demos
Browser
Calculator
Calendar
Camera
Clock
Custom Locale
Dev Settings
Dev Tools
Downloads
Email
File Manager
G+ Photos
Gallery
Gestures Builder
Gmail
Google
Google Settings
Google+
Kim Ariyor?
GPS
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\kimariyor>adb install com.adaffix.publisher.tr.android.apk
2959 KB/s (6861962 bytes in 2.264s)
pkg: /data/local/tmp/com.adaffix.publisher.tr.android.apk
Success
C:\Users\Mert\Desktop\kimariyor>_
free for personal use

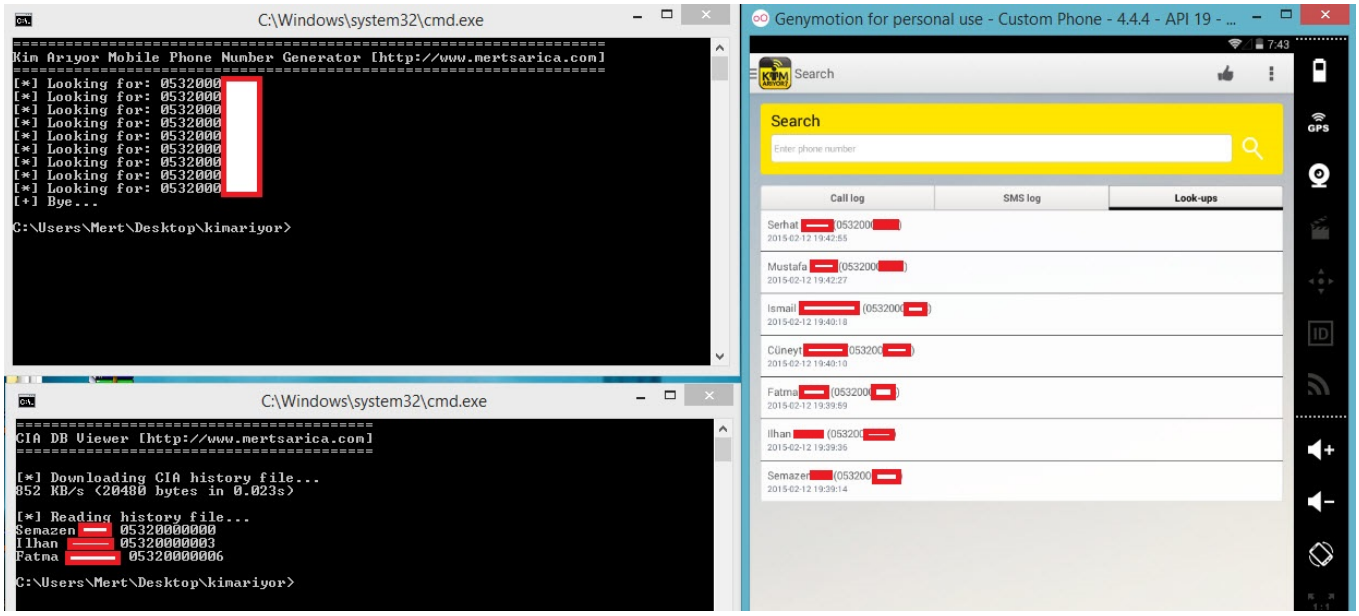

Genymotion for personal use - Custom Phone - 4.4.4 - API 19 - 768x1280 (768...
6:11
Matched
EKREM
Türkiye
0536 5
Call now!
Found in web
SAVE
BLOCK
LIKE
GPS


Genymotion for personal use - Custom Phone - 4.4.4 - API 19 - 768x1280 (768...
6:13
KIM ARIYOR?
EKREM Türkiye.
0536 5
Found in web
GPS
C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\kimariyor>adb shell am start -a android.intent.action.CALL
tel:0536 5
Starting: Intent { act=android.intent.action.CALL dat=tel:xxxxxxxxxx }
C:\Users\Mert\Desktop\kimariyor>

Çağrı gönderdikten sonra rehber havuzu üzerinde yapılan sorgulamanın, uygulama tarafından dosya sistemi üzerinde herhangi bir yere kaydedilip kaydedilmediğini adb shell komutu ile öykünücüye bağlanıp araştırmaya başladım. Çok geçmeden uygulama tarafından yapılan sorguların ve yanıtlarının uygulamaya ait databases klasörü altında history.db isimli sqlite veritabanı dosyasında tutulduğunu tespit ettim.



Ardından Python ile iki araç hazırladım. Bir tanesi mobil operatörlerin alan koduna göre numara üreterek öykünücüye çağrı gönderirken diğeri ise history.db veritabanı dosyasını okuyarak yeni oluşturulan kayıtları gösteriyordu. Araçları kısa bir süre çalıştırdıktan sonra çalışmamı tamamladım.



Bu çalışma sonucunda art niyetli kişilerin ellerinde bulunan veya bulunmayan (anlık olarak üretilen) cep telefonu numaraları ile isim ve soyad bilgilerini kısa bir sürede eşleştirebileceklerini öğrenmiş oldum. Siz de benim gibi, rızanız olmadan yakınlarınızın veya sizin cep telefonu numaranızı paylaşan arkadaşlarınız olduğundan şüphe ediyor ve Kim Arıyor? uygulamasının rehber havuzundan numaranızı silmek istiyorsanız, buradaki adresi ziyaret ederek numaranızı bu listeden sildirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.