Hack 4 Career - 2022

THIS BOOK WAS PRODUCED WITH PRESSBOOKS

Hack 4 Career - 2022

HTTPS://WWW.MERTSARICA.COM

MERTSARICA

Bu kitap Pressbooks (https://pressbooks.com) ile üretilmiş ve Prince ile oluşturulmuştur.

İçindekiler

THIS BOOK WAS PRODUCED WITH PRESSBOOKS

Giriş

2009 yılında "Bilgi güçtür ve paylaşıldıkça artar" mottosuyla oluşturduğum blogumda, bilgi güvenliği farkındalığını arttırma adına çok sayıda teknik yazıya yer vermeye çalıştım. Yıllar içinde okurlarımdan aldığım olumlu geri dönüşler sonucunda, yazılarımı yıllar bazında e-kitap olarak derlemeye ve siber güvenlik meraklıları ile paylaşmaya karar verdim.

Emek, zaman ve kaynak ayırarak yaptığım araştırmalar sonucunda yazdığım bu yazıların, siber güvenlik alanında kendini geliştirmek isteyenler için faydalı olması dileklerimle...

Mert SARICA

This book was produced using

PB PRESSBOOKS

Pressbooks provides educators, authors, & scholars with powerful tools for creating, adapting, & sharing their ideas.

Learn more about how you can use Pressbooks to publish beautiful and accessible books on the web and in print-ready formats at https://pressbooks.com/get-started.

Zararlı Görüntü

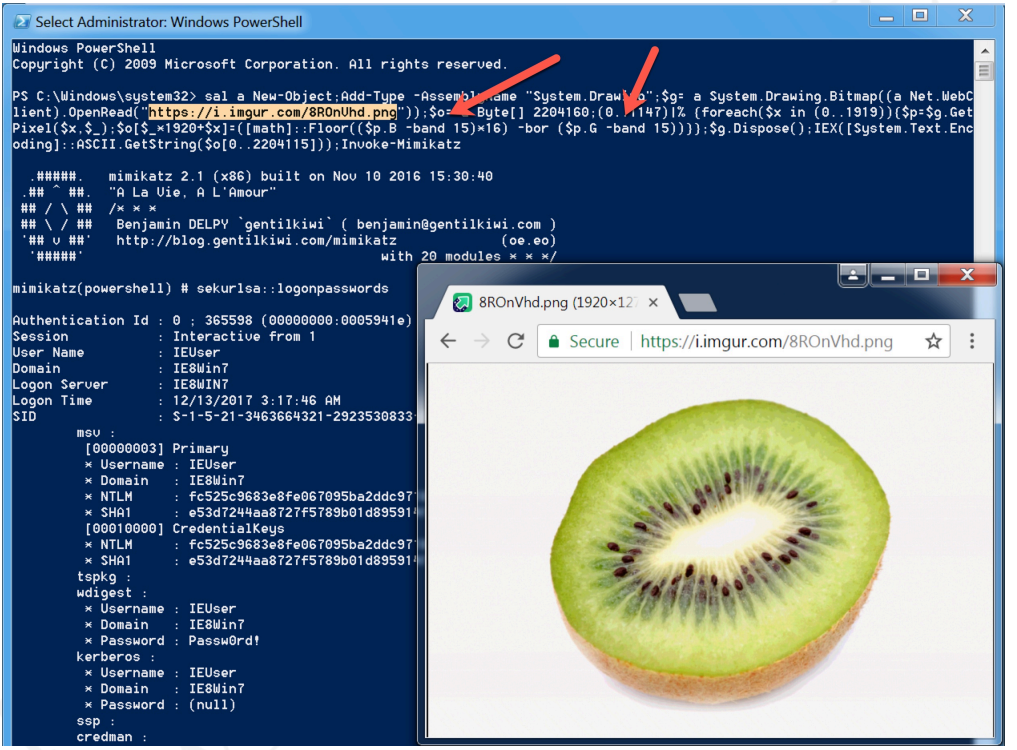
Türkiye'deki kurumları da hedef alan Muddy Water gibi organize siber saldırı gerçekleştiren APT gruplarının son yıllarda gerçekleştirdikleri operasyonlarına baktığımızda, zaman zaman Steganografi tekniğinden faydalandıklarını görüyoruz. Bu teknik sayesinde siber saldırganlar, sosyal mühendislik saldırısı ile sızmaya çalıştıkları hedef son kullanıcı sistemine, gözle ayırt edilemeyecek zararlı kod parçasının görüntü dosyasının içinde indirilmesini ve çalıştırılmasını sağlamaktadırlar.

> Steganografinin ilk kullanımına M.Ö 400'lü yıllarda "Tarihin babası" olarak anılan Herodot'un Historia olarak bilinen eserinde rastlanmaktadır.Bu eserde Demaratus, Yunanistan'a yaklaşan bir saldırıyı tahta bir tabletin üzerine kazıdıktan sonra üzerini balmumu ile kaplar ve mum eritildikten sonra tablette saldırıya dair uyarı ortaya çıkar.

Hem 2018 yılından bu yana haberlere konu olması hem de Mitre'nin T1027 tekniği sayfasında yer alması sebebiyle PNG görüntü dosyasının piksellerine Powershell kodu eklemeye yarayan Invoke-PSImage aracı dikkatimi çekti.

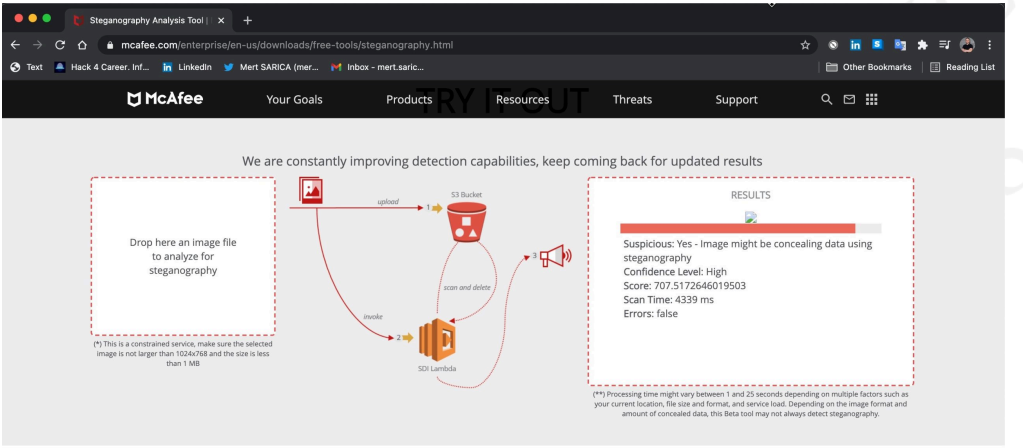
Internette ufak bir araştırma yaptığımda bu araç ile oluşturulmuş PNG dosyasındaki Powershell kodunu ortaya çıkaran bir araç bulamadığım için olay müdahale (IR) uzmanlarına fayda sağlayacak bir araç hazırlamaya karar verdim.

İlk olarak Invoke-PSImage aracının nasıl çalıştığını anlamak için kaynak koduna göz attığımda hedef olarak verile bir PNG dosyasının R (RED), G (GREEN), B (BLUE) renk kodlarından (her biri 8 bayt boyutundadır) G ve B'nin en düşük değerlikli bitleri (Least Significant Bit-LSB) ile oynayıp (bu sayede görüntü kalitesi düşse de insan gözü bu farkı kolay kolay anlayamaz) her defasında aynı aritmetik işlemlere (**[math]::Floor((`$p.B-band15)*16)-bor(`$p.G -band 15))** sokarak gizlenmiş Powershell kodunu çalıştırdığını öğrendim. Hep aynı aritmetik işleme soktuğu için işlemi tersine çevirerek gizli Powershell koduna ulaşmak pratikte mümkün olduğu için amacıma bir adım daha yaklaşmış oldum.

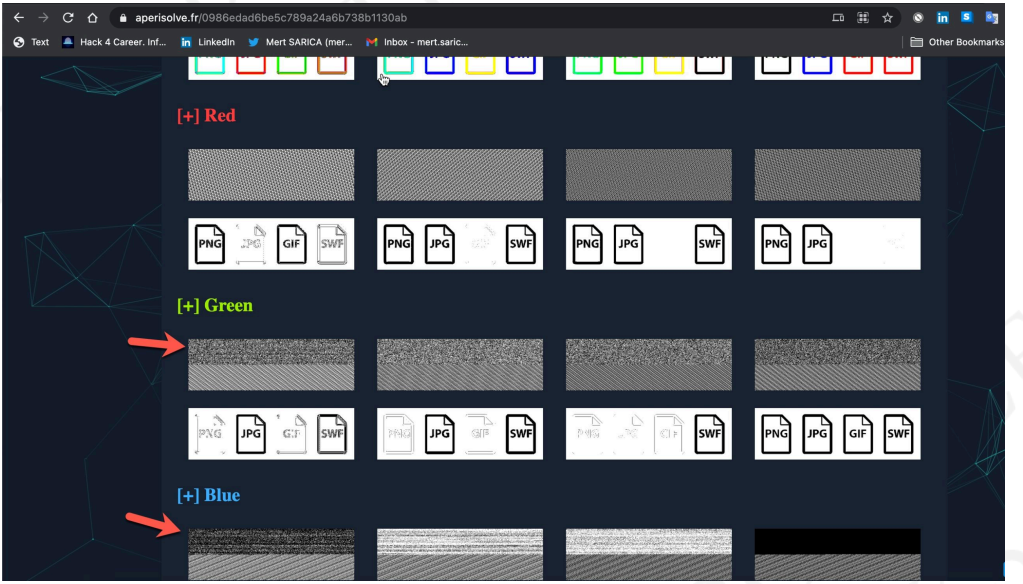


Aracı hazırlamadan önce hedef görüntü dosyasında gizli bir mesaj olup olmadığını anlamanın kolay bir yolu var mı diye araştırırken çok sayıda aracın yanısıra iki tane oldukça faydalı web sitesi ile karşılaştım. İkisinde de Muddy Water APT grubu tarafından bir operasyonda kullanılan EPUWBt3.png dosyasını analiz ettiğimde tatmin edici sonuçlar ile karşılaştım.

Bunlardan ilki olan McAfee'nin web sitesine (FireEye – McAfee birleşmesi sonrasında bu aracı web sitesinden kaldırdılar) **EPUWBt3.png** dosyasını yüklediğimde dosyanın şüpheli olduğuna dair bir uyarı mesajı ile karşılaştım.

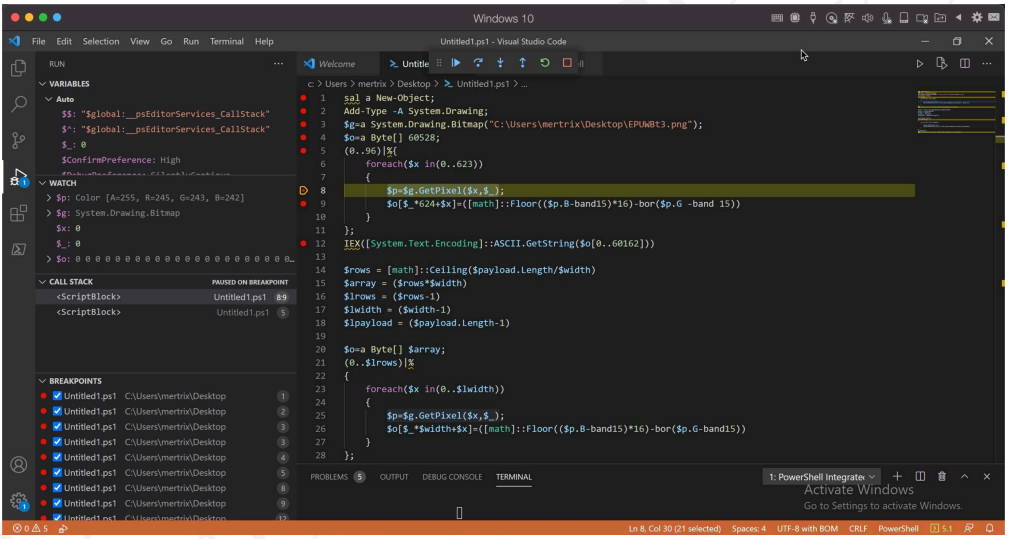


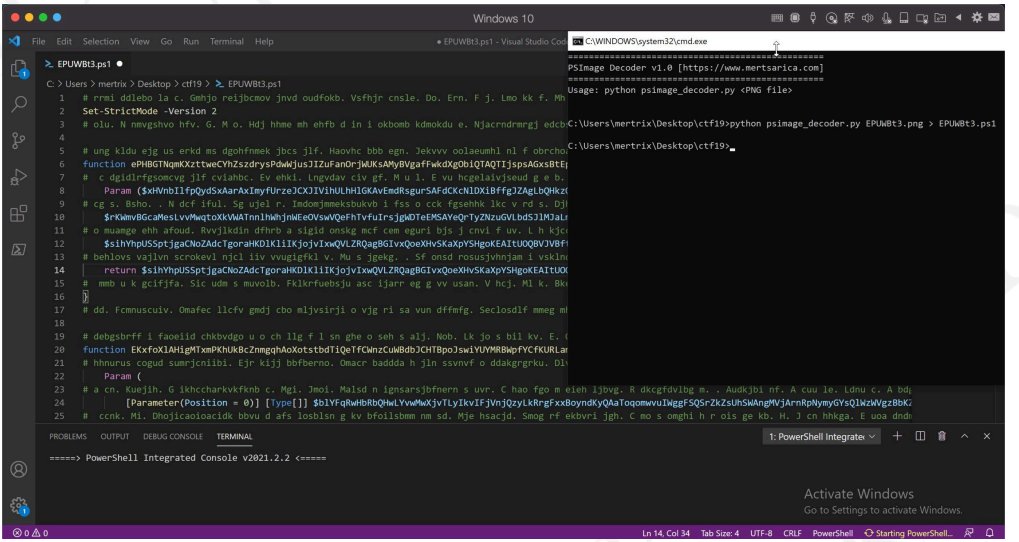
Aperi'Solve isimli diğer web sitesine **EPUWBt3.png** dosyasını yüklediğimde ise özellikle yeşil ve mavi renk kodlarındaki farklılık bu görüntü dosyasında şüpheli bir durum olduğunu ortaya koyuyordu.



Sıra aracı hazırlamaya geldiğinde **EPUWBt3.png** görüntü dosyasını çözen

Powershell kodunu Visual Studio Code ile hata ayıklama ile adım adım analiz ettikten sonra Invoke-PSImage aracı ile görüntü dosyalarına gizlenen Powershell kodlarını ortaya çıkaran psimage_decoder.py isimli yeni aracım, siber güvenlik uzmanlarının kullanımı için hayata merhaba demiş oldu.





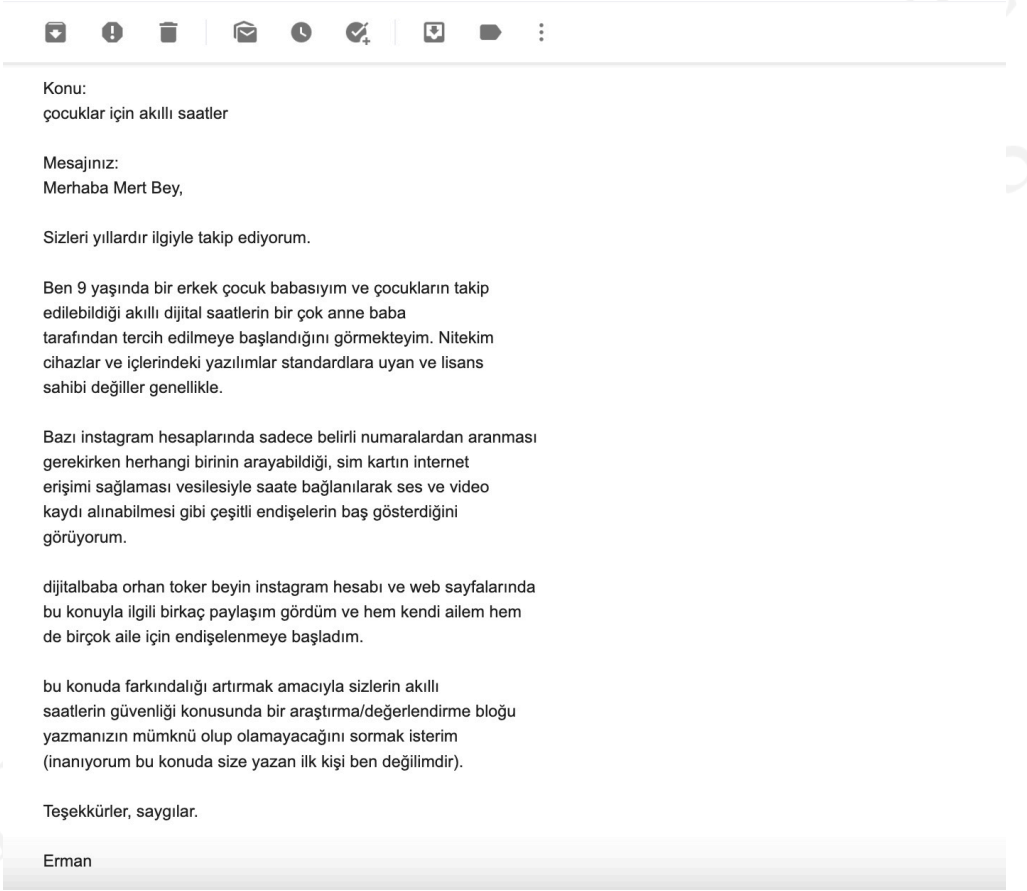
Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

Bu yazı ayrıca Pi Hediyem Var #19 oyununun çözüm yolunu da içermektedir.

Akıllı Çocuk Saatleri

Bu hikaye, 4 Mayıs 2022 tarihinde Erman ATEŞ isimli bir okurumdan aldığım e-posta ile başladı. Bilinçli ve duyarlı bir baba olan Erman Bey göndermiş olduğu e-postada, akıllı çocuk saatlerinin bir çok ebeveyn tarafından haklı gerekçelerle tercih edilmeye başlandığını ancak yazılım, güvenlik ve mahremiyet açısından hem bir standarda tabi olmamaları hem de Instagram'da gördüğü bir mesaj nedeniyle tüm ebeveynler adına endişe duymaya başladığını ve bu nedenle de bu konuya mercek tutmamı rica etmişti. Instagram Dolandırıcıları, Arka Kapı Avı, Tuzak Sistem ile Hacker Avı blog yazılarımda olduğu gibi okurlarına her daim kulak veren bir güvenlik araştırmacısı olarak toplumsal fayda ve bilgi güvenliği farkındalığı adına bu konuya eğilmeye karar verdim.



Konu:
çocuklar için akıllı saatler

Mesajınız:
Merhaba Mert Bey,

Sizleri yıllardır ilgiyle takip ediyorum.

Ben 9 yaşında bir erkek çocuk babasıyım ve çocukların takip edilebildiği akıllı dijital saatlerin bir çok anne baba tarafından tercih edilmeye başlandığını görmekteyim. Nitekim cihazlar ve içlerindeki yazılımlar standardlara uyan ve lisans sahibi değiller genellikle.

Bazı instagram hesaplarında sadece belirli numaralardan aranması gerekirken herhangi birinin arayabildiği, sim kartın internet erişimi sağlaması vesilesiyle saate bağlanılarak ses ve video kaydı alınabilmesi gibi çeşitli endişelerin baş gösterdiğini görüyorum.

dijitalbaba orhan toker beyin instagram hesabı ve web sayfalarında bu konuyla ilgili birkaç paylaşım gördüm ve hem kendi ailem hem de birçok aile için endişelenmeye başladım.

bu konuda farkındalığı artırmak amacıyla sizlerin akıllı saatlerin güvenliği konusunda bir araştırma/değerlendirme bloğu yazmanızın mümknü olup olamayacağını sormak isterim (inanıyorum bu konuda size yazan ilk kişi ben değilimdir).

Teşekkürler, saygılar.

Erman

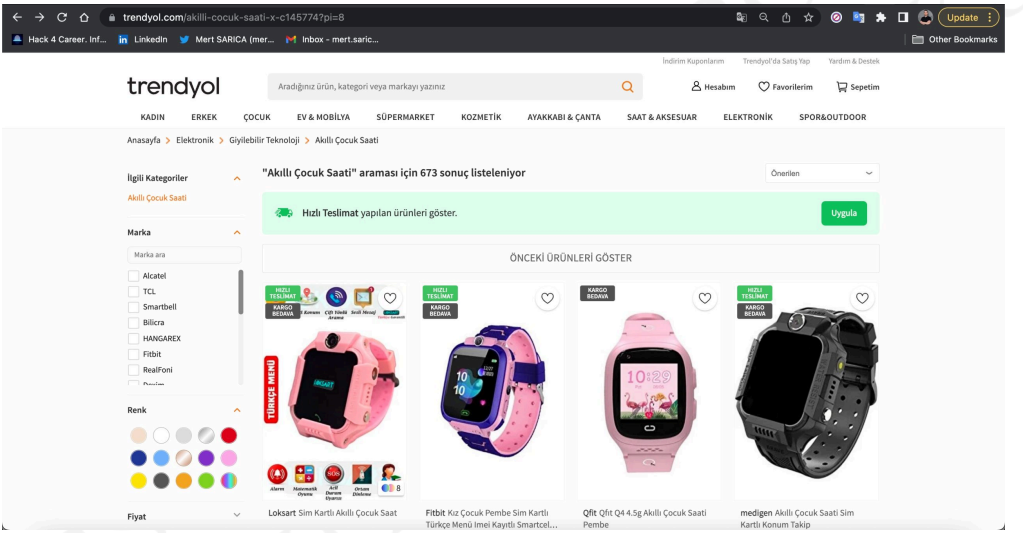
Aşağıdaki fotoğrafa bakıldığında akıllı çocuk saatleri gerçekten ebeveynler için çocuklarını gözetim altında tutmak için faydalanabilecekleri büyük bir teknolojik nimet mi ?

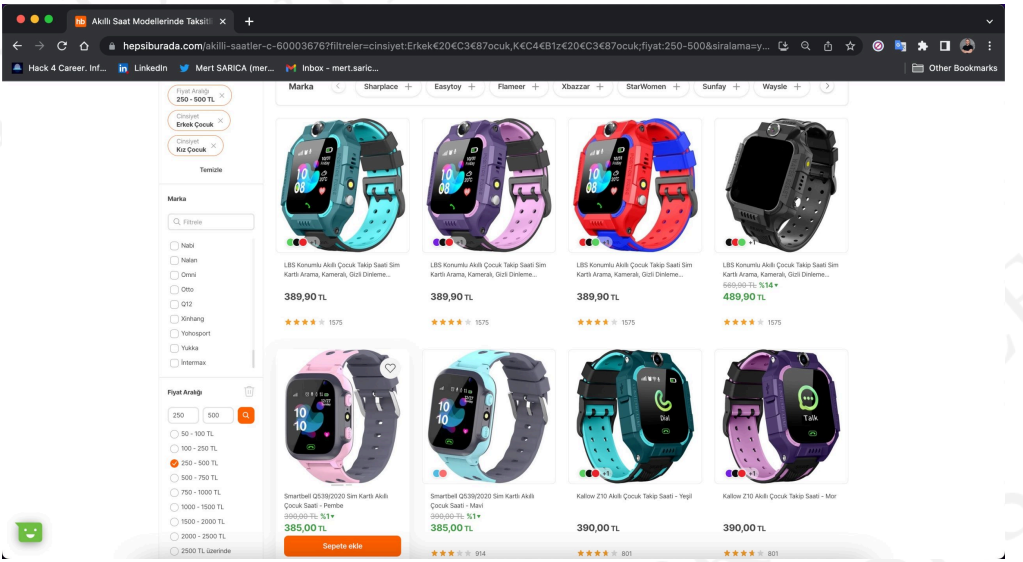

09:5
17/08

Yoksa aşağıdaki diğer bir fotoğrafa bakıldığında ebeveynlerin, kendilerinin ve çocuklarının mahremiyetini, özel hayatlarının gizliliğini istemeden de olsa tehlikeye attıkları, ortam dinlemeye imkan tanıyan saat görünümlü potansiyel casus bir cihaz mı ?

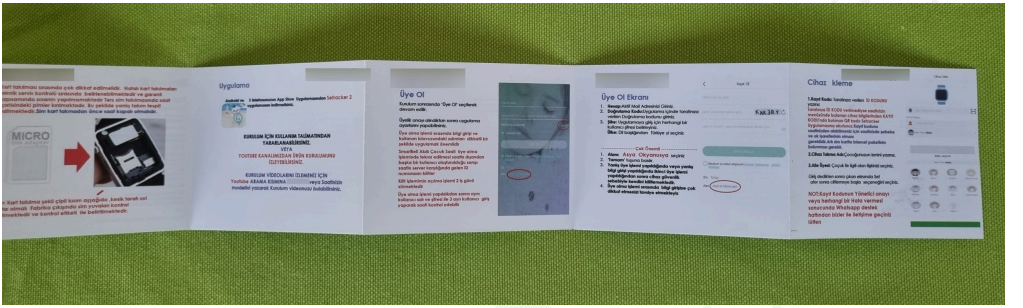
Bu sorulara yanıt bulmak için ilk olarak güvenlik araştırmamda kullanmak üzere fiyat açısından uygun olan bir çocuk saati satın almaya karar verdim.

Bunun için Hepsiburada, Trendyol gibi alışveriş sitelerindeki **Akıllı Çocuk Saatleri** kategorilerini incelemeye başladım. En çok satılan, yorum ve değerlendirme yapılan saatlere baktıktan sonra **1000**'e yakın değerlendirmesi olan bir marka ve modelde karar kılıp, satın aldım.



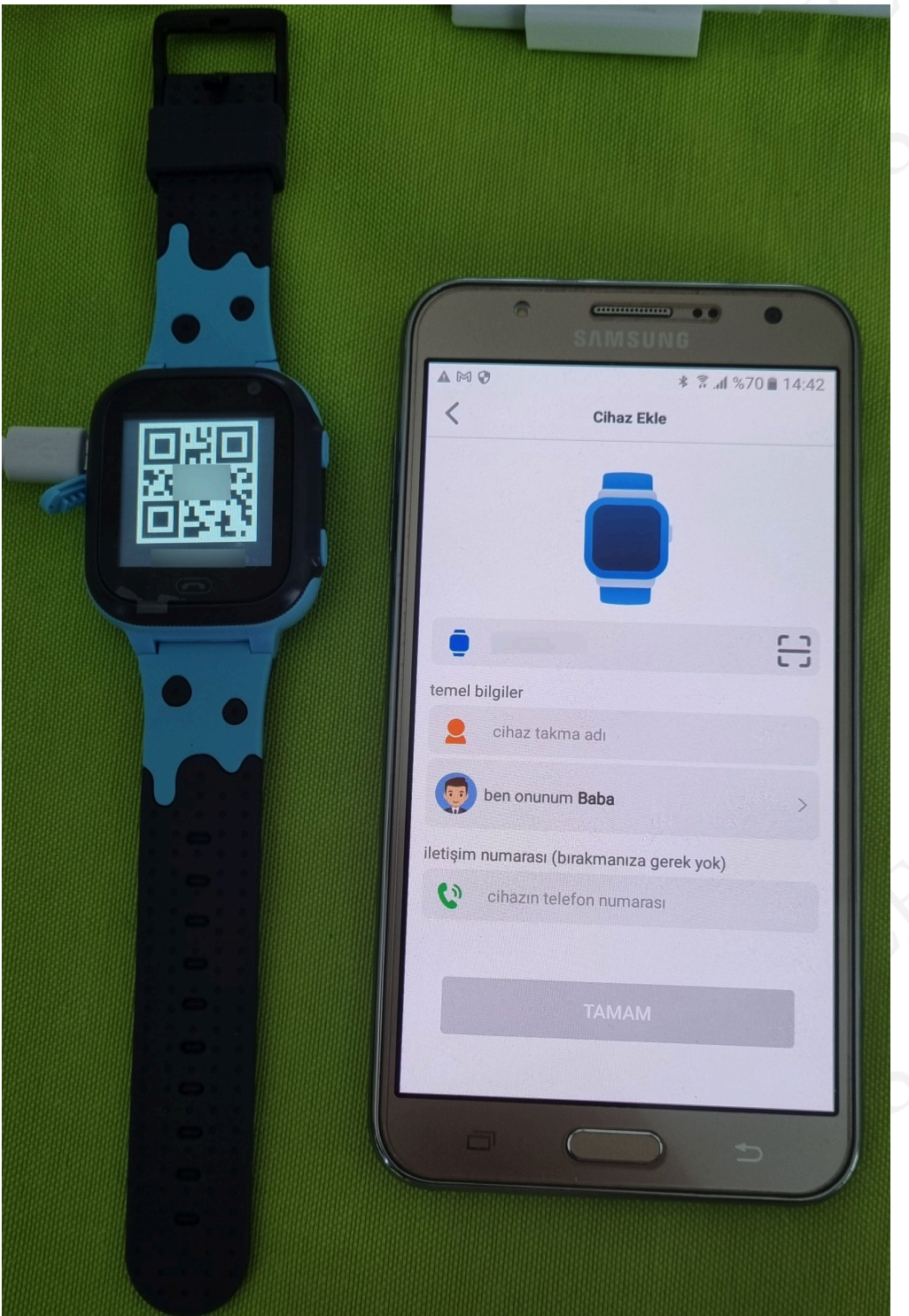


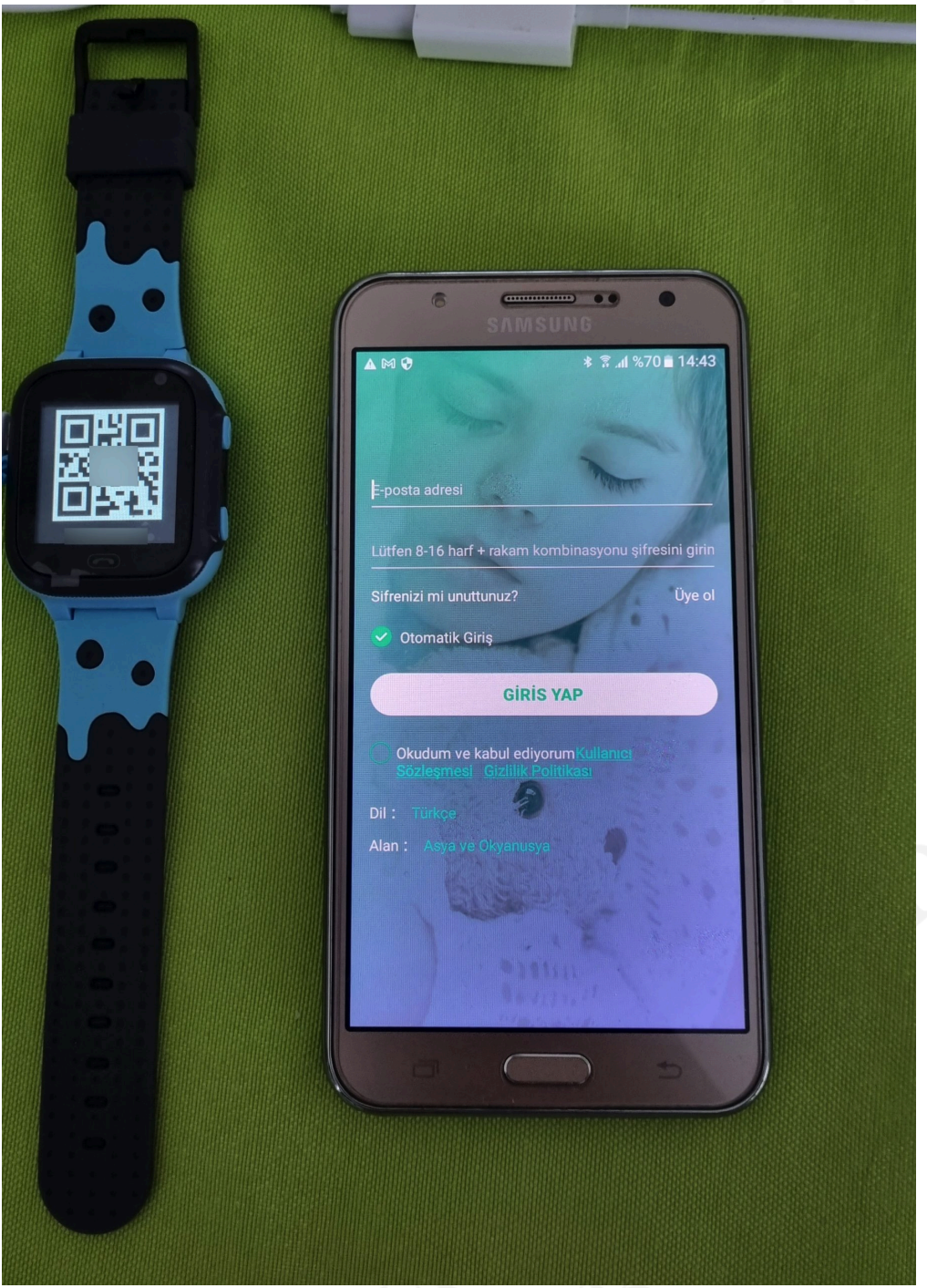
Saati kutusundan çıkarıp, kurulum kılavuzunu incelediğimde, saati uzaktan yönetebilmek için Çinli 3G Electronics isimli bir şirket tarafından geliştirilen Android veya iOS mobil uygulamasının kurulmasının gerektiği belirtiliyordu.

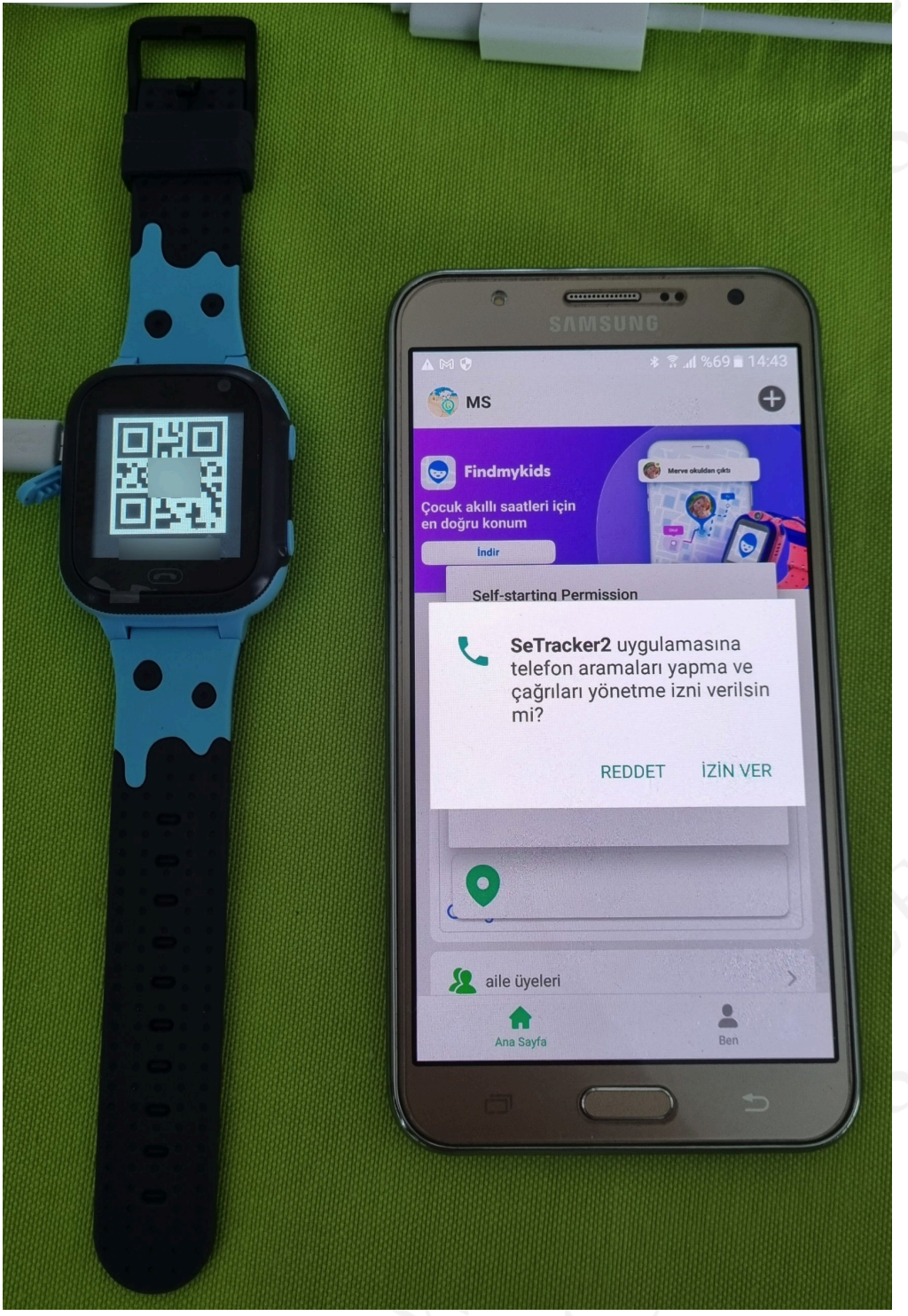


SeTracker2 isimli uygulamanın topladığı bilgilere baktığımızda lokasyon, ses ve görüntü kaydından, rehbere, isim, cep telefonu ve e-posta adresine kadar kişiye özel, hassas, mahrem sayılabilecek bilgiler olduğunu gördüm.

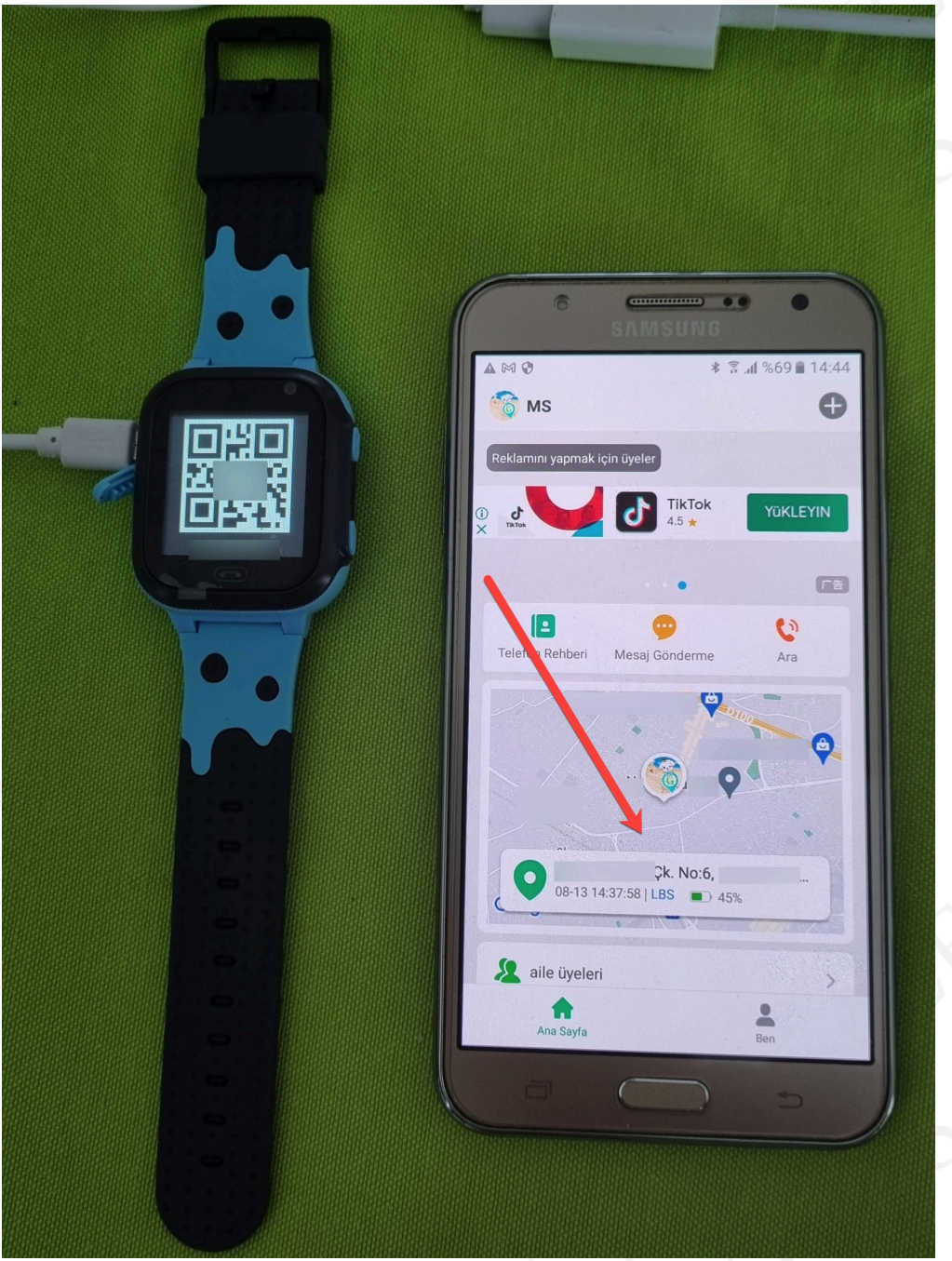
Saate SIM kartı takıp, çalıştırdıktan sonra SeTracker2 uygulamasını açıp, kayıt oldum. Daha sonra uygulamaya ile saati eşleştirdikten sonra uygulamayı ve menü adımlarını incelemeye başladım.

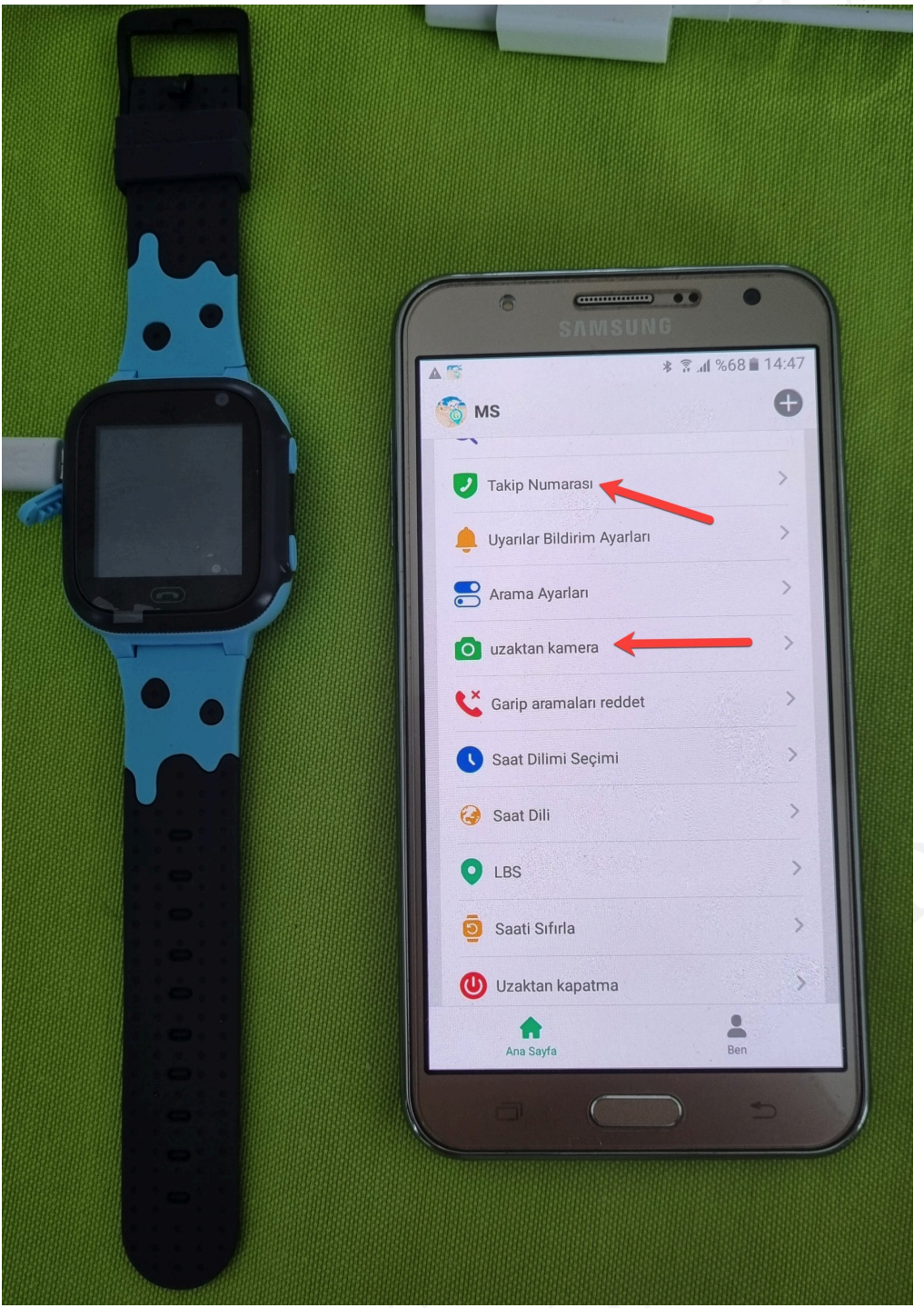

SAMSUNG
%70 14:42
Cihaz Ekle
temel bilgiler
cihaz takma adı
ben onunum Baba
iletişim numarası (bırakmanıza gerek yok)
cihazın telefon numarası
TAMAM

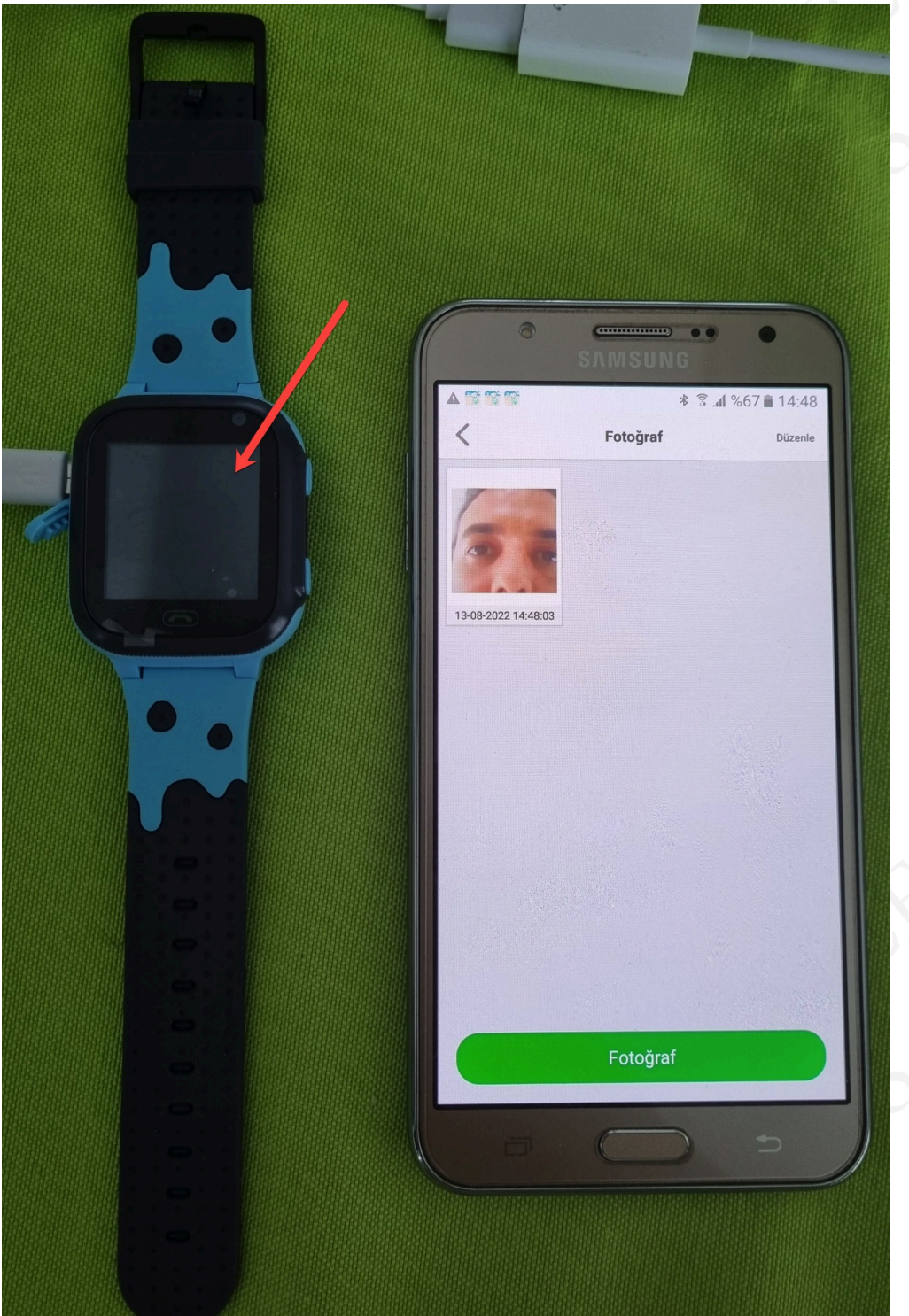

SAMSUNG
%70 14:43
E-posta adresi
Lütfen 8-16 harf + rakam kombinasyonu şifresini girin
Sifrenizi mi unuttunuz?
Üye ol
Otomatik Giriş
GİRİS YAP
Okudum ve kabul ediyorum Kullanıcı Sözleşmesi Gizlilik Politikası
Dil : Türkçe
Alan : Asya ve Okyanusya


SAMSUNG
%69 14:43
MS
Findmykids
Çocuk akıllı saatleri için
en doğru konum
İndir
Merve okuldan çıktı
Self-starting Permission
SeTracker2 uygulamasına telefon aramaları yapma ve çağrıları yönetme izni verilsin mi?
REDDET
İZİN VER
aile üyeleri
Ana Sayfa
Ben

Uygulamada öncelikle dikkatimi çeken nokta, saatin harita üzerinden anlık olarak izlenebilmesi daha sonra ise **Takip Numarası** ve **uzaktan kamera** menü adımları oldu. **Uzaktan kamera** menüsü üzerinden saatteki kamera ile istediğiniz zaman fotoğraf çekilebiliyorsunuz. Bu esnada saat herhangi bir görsel veya işitsel bir uyarı oluşturmuyor. **Takip numarası** menüsü ile ise saatin girilen cep telefonu numarasını aramasını sağlayabiliyorsunuz ve saatteki mikrofon sayesinde de ortam dinlemesi yapılabiliyor. Bu esnada yine uzaktan kamera adımında olduğu gibi telefon, ortam dinlemesi yapıldığına dair herhangi bir uyarı vermiyor.


SAMSUNG
%69 14:44
MS
Reklamını yapmak için üyeler
TikTok
4.5
YÜKLEYIN
Mesaj Gönderme
Ara
08-13 14:37:58 | LBS
45%
aile üyeleri
Ana Sayfa
Ben


SAMSUNG
%68 14:47
MS
Takip Numarası
Uyarılar Bildirim Ayarları
Arama Ayarları
uzaktan kamera
Garip aramaları reddet
Saat Dilimi Seçimi
Saat Dili
LBS
Saati Sıfırla
Uzaktan kapatma
Ana Sayfa
Ben


SAMSUNG
%67 14:48
Fotoğraf
Düzenle
13-08-2022 14:48:03
Fotoğraf

Bir veya daha fazla etkileşimli öğe, metnin bu sürümünde yer almadı. Bunları çevrimiçi olarak burada görüntüleyebilirsiniz: https://pressbooks.pub/mertrix/?p=68#oembed-1

"E ne güzel işte Mert, çocuğumuzu anlık olarak izleyebilir ve dinleyebiliriz" diye düşünüyor olabilirsiniz. Peki **SeTracker2** uygulamasına giriş için kullandığınız e-posta adresinizi ve içinde özel karakter bile kullanarak güçlendiremediğiniz parolanızın bir an olsun art niyetli kişiler tarafından çalındığını veya tahmin edildiğini düşünelim. Art niyetli kişi, çocuğunuzun kolundaki saate uygulama üzerinden bağlanarak konumunu anlık olarak izleyebilir, fotoğrafını çekebilir, mesaj gönderebilir, gönderdiği mesajı silip geride iz bırakmayabilir, saatin belirttiği telefon numarasını aramasını sağlayarak ortam dinlemesi yaparak mahremiyetinizi, özel hayatınızın gizliliğini ihlal edebilir. Ayrıca art niyetli kişi tarafından gerçekleştirilen tüm bu işlemlerin iz kaydına (log) SeTracker2 uygulaması üzerinden ulaşma şansınızın olmadığının da altını çizeyim!

"Mert ben çok dikkatliyim, temkinliyim, kolay kolay dolandırıcıların ağına düşmem" de diyebilirsiniz. Aynı parolayı birden fazla web sitesine giriş esnasında kullanıyorsanız, o web sitelerinden biri çoktan hacklenmiş ve kullanıcı adınız/e-posta ve parolanız ele geçirilmiş olabilir. **Çok Faktörlü Kimlik Doğrulaması (MFA)** kullanmadığınız durumda (SeTracker2 uygulaması MFA desteklemiyor!) art niyetli kişilerin elde ettiği bu bilgilerle hesabınızın olduğu web sitelerine, mobil uygulamalara (SeTracker2 uygulaması gibi) rahatlıkla giriş yapılabileceğini unutmayın!

> Çok faktörlü kimlik doğrulaması (MFA), kullanıcıların yalnızca bir paroladan daha fazla bilgi girmesini gerektiren, hesapta çok adımlı oturum açma sürecidir. Örneğin, kullanıcılardan parolanın yanı

> sıra e-posta adreslerine, cep telefonlarında gönderilen bir kodu (internet şubeye girişte olduğu gibi) girmeleri, mobil uygulamaya gönderilen bir isteği kabul etmeleri, gizli bir soruyu yanıtlamaları ya da parmak izlerini taratmaları istenebilir. İkinci bir doğrulama yöntemi, art niyetli kişilerin parolasını ele geçirildiği kullanıcıların hesaplarına yetkisiz erişmesini önlemeye yardımcı olmaktadır.

Bir diğer önemli konu ise ortam dinlemesi özelliğine sahip saatler kullanarak istemeden de olsa çocuğunuz üzerinden suç işliyor olabilirsiniz. Hukukçu olmasam da **5237 Sayılı Türk Ceza Kanunu**'nun "Kişiler Arasındaki Konuşmaların dinlenmesi ve kayda alınması" başlıklı **133. maddesine** dikkatinizi çekmek isterim:

> (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.
>
> (2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.
>
> (3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

Tahminimce başta Koş Mert Koş başlıklı blog yazım olmak üzere, güvenlik araştırmalarıma aşina olanlarınızın bu yazımda tersine mühendislikle, statik ve dinamik kod analizi ile SeTracker2 uygulamasını analiz edip tespit ettiğim

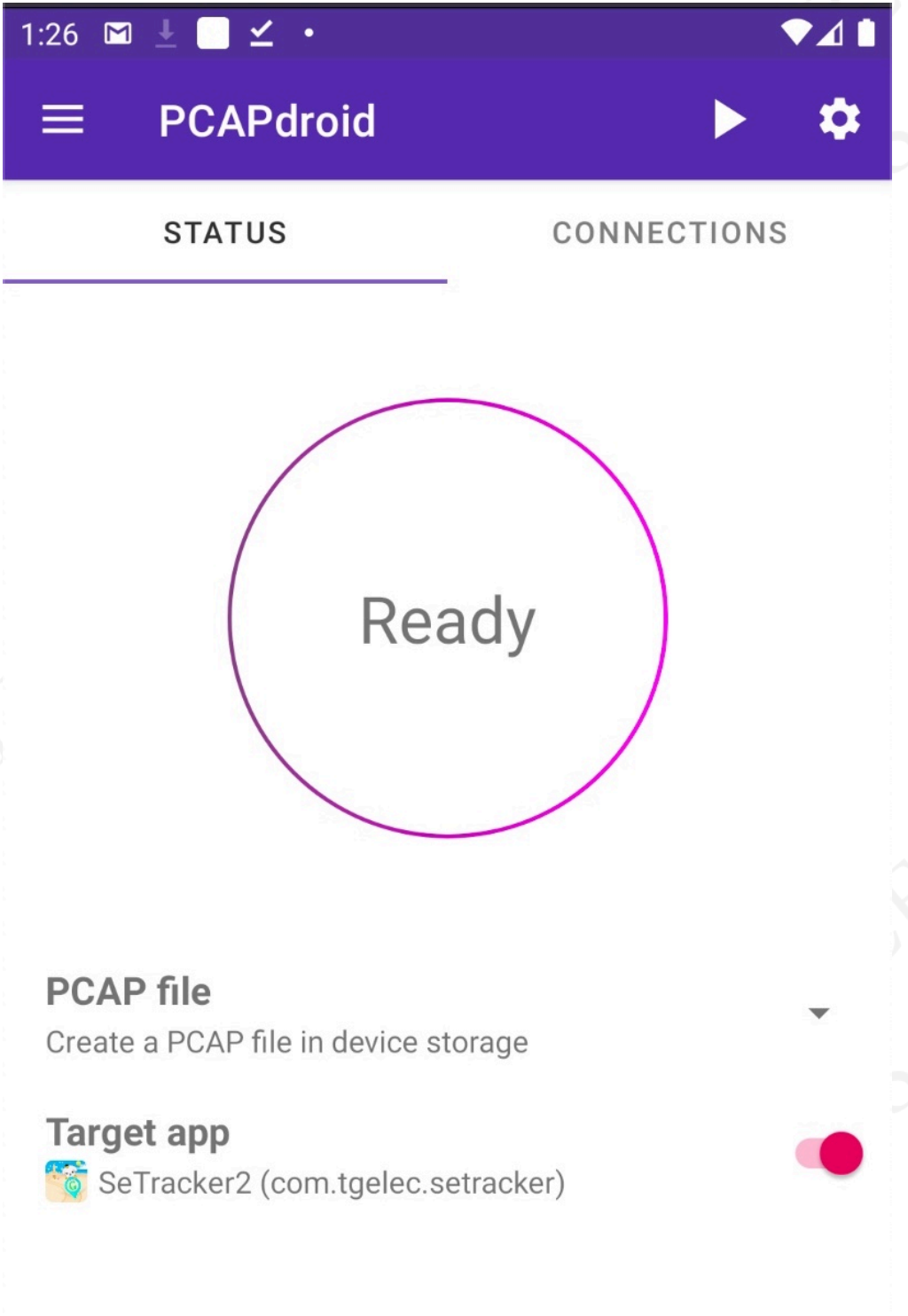
zafiyetlerin nasıl kötüye kullanılabileceğini göstermemi veya saatte keşfettiğim donanımsal bir zafiyet ile saatin nasıl casus bir cihaza dönüştürebildiğini görmeyi umuyorlardı. Tüm bu anlattıklarımdan sonra bunca zahmete girmeden bu saatin, SeTracker2 uygulaması sayesinde art niyetli kişilere kötüye kullanım için davetiye çıkardığını, ebeveynler ve çocukları için büyük bir tehlike oluşturduklarını net olarak aktarabildiğimi düşünüyorum. 🙂 Yine de uygulama ile ilgili teknik bilgi edinmek isteyenler var ise önceki yıllarda yapılmış olan çalışmalar için buraya ve de buraya göz atabilirler.

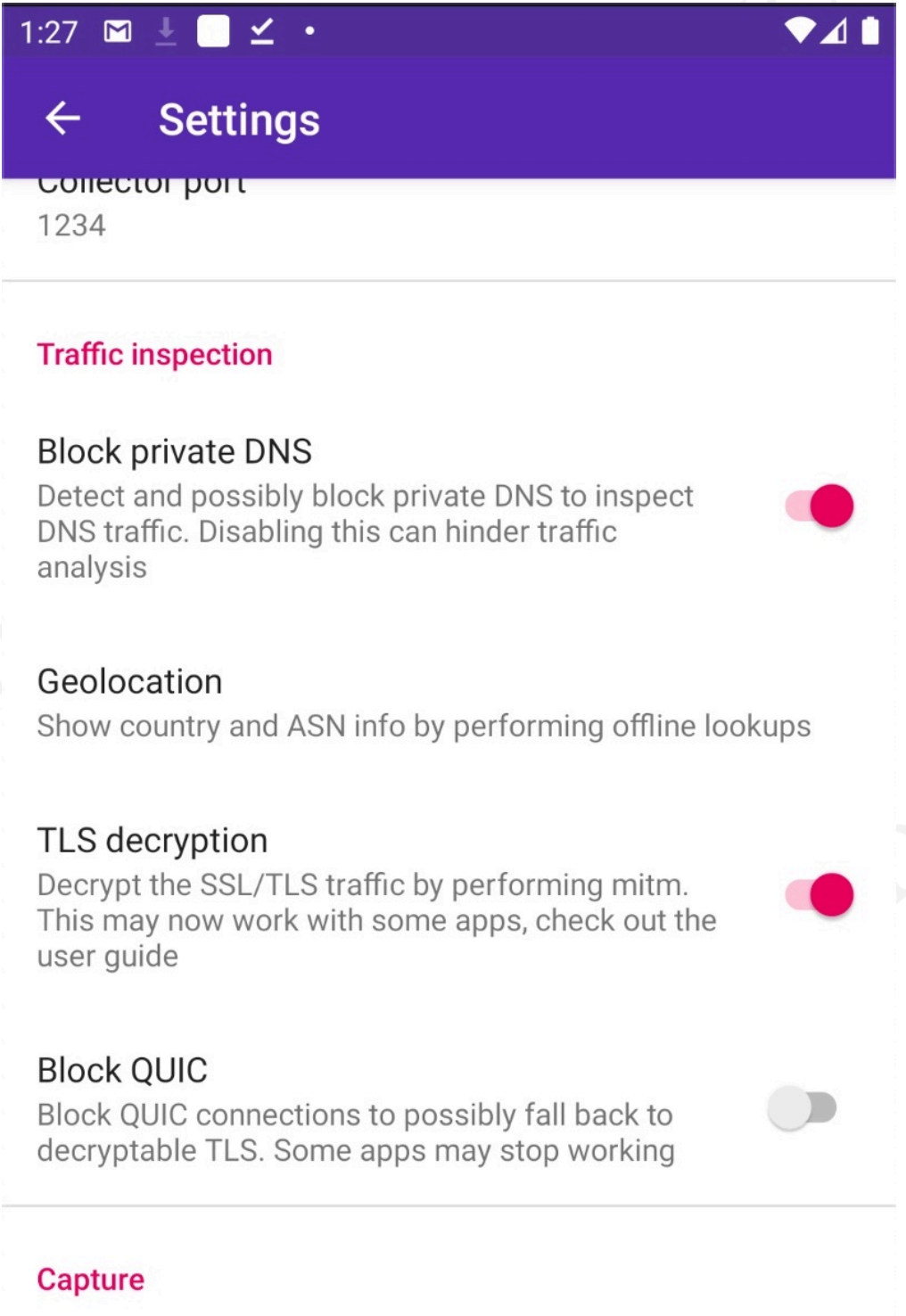
Umuyorum ki 2017 yılında Almanya'nın aldığı bu örnek karar gibi otoritelerimiz de benzer bir karar alarak, yasa dışı ortam dinlemesi yapma özelliğine sahip olan bu saat görünümlü potansiyel casus cihazların alışveriş sitelerinde satışını engelleyerek, ebeveynleri ve çocukları bu tür tehlikelerden korumak için önemli bir adım atarlar.

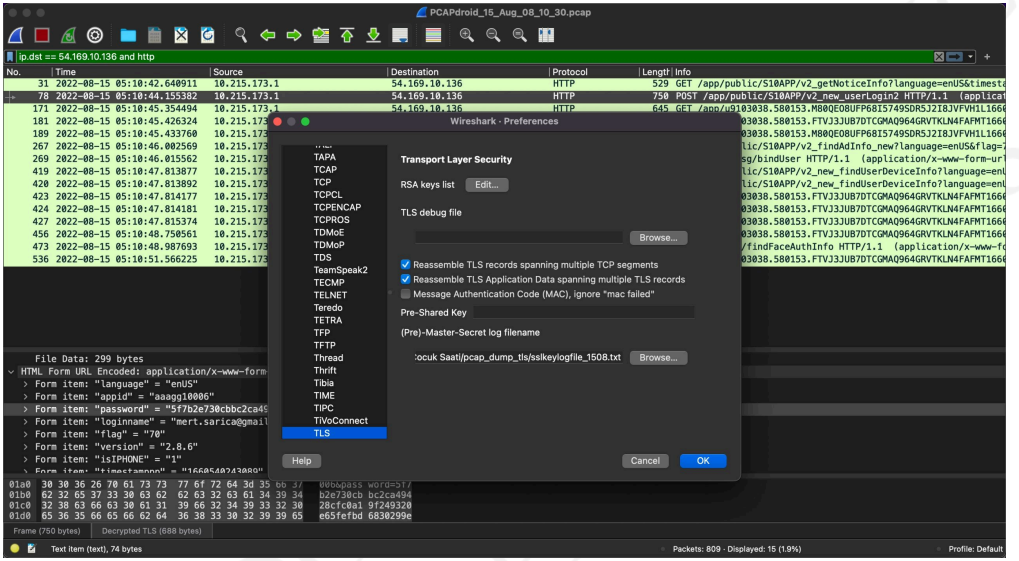
Bu bilgiler ışığında, ortam dinlemesi yapabilen akıllı çocuk saatleri kullanacaklara risklerini bilerek kullanmalarını tavsiye ettikten sonra siz sevgili okurlarımdan farkındalık yaratma adına bu yazıyı ebeveyn olan arkadaşlarınızla, dostlarınızla ve sevdiklerinizle paylaşmanızı önemle rica ederim.

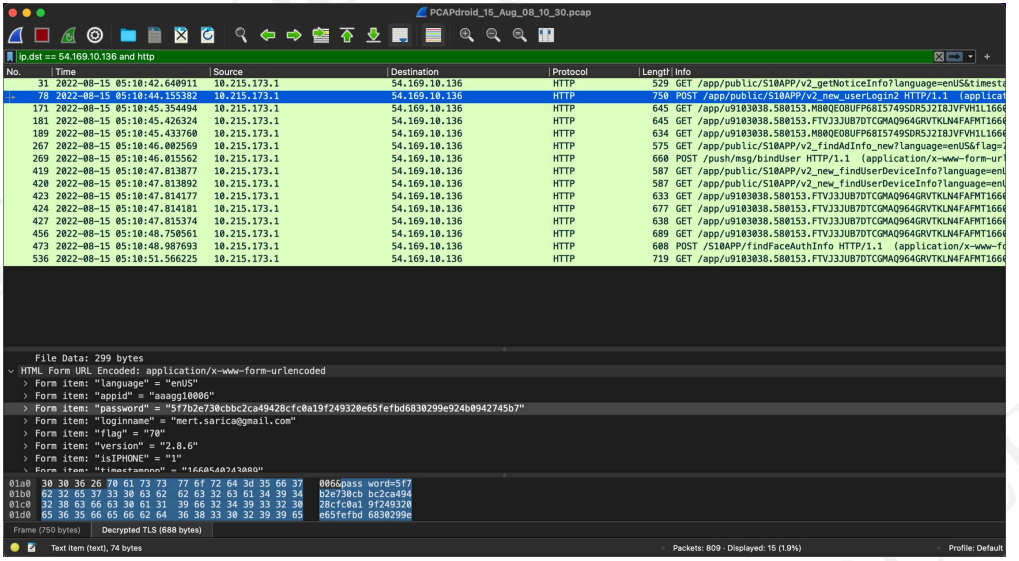
Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Teknik okurlarım için de SeTracker2 uygulamasında SSL Pinning yönteminin kullanıldığını, HTTPS trafiğini analiz etmek için PCAPdroid isimli bir Android uygulaması sayesinde basit bir şekilde trafiği kayıt altına aldığımı ve daha sonrasında da Wireshark aracı ile analiz edebildiğimi de paylaşayım.


1:26
PCAPdroid
STATUS
CONNECTIONS
Ready
PCAP file
Create a PCAP file in device storage
Target app
SeTracker2 (com.tgelec.setracker)

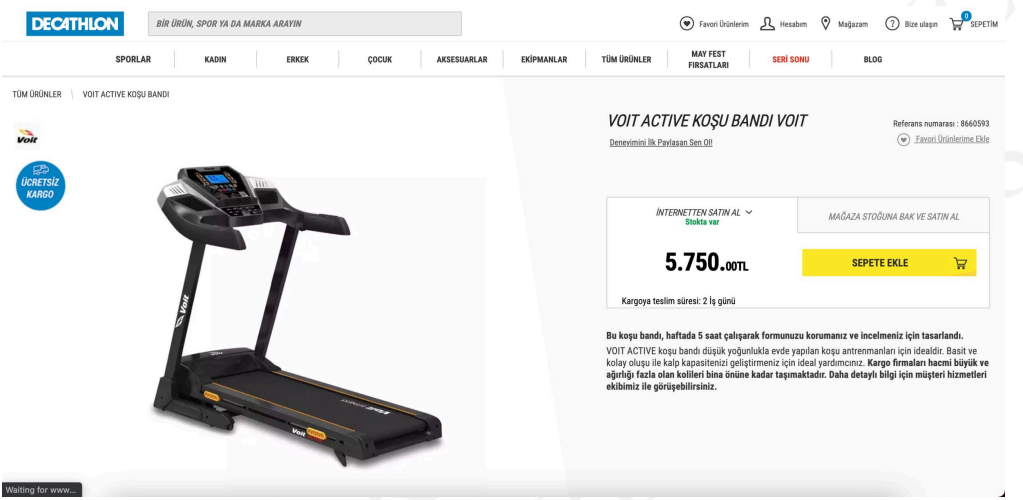

1:27
Settings
Collector port
1234
Traffic inspection
Block private DNS
Detect and possibly block private DNS to inspect DNS traffic. Disabling this can hinder traffic analysis
Geolocation
Show country and ASN info by performing offline lookups
TLS decryption
Decrypt the SSL/TLS traffic by performing mitm. This may now work with some apps, check out the user guide
Block QUIC
Block QUIC connections to possibly fall back to decryptable TLS. Some apps may stop working
Capture


PCAPdroid_15_Aug_08_10_30.pcap
ip.dst == 54.169.10.136 and http
Wireshark · Preferences
Transport Layer Security
RSA keys list
Edit...
TLS debug file
Browse...
Reassemble TLS records spanning multiple TCP segments
Reassemble TLS Application Data spanning multiple TLS records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared Key
(Pre)-Master-Secret log filename
Browse...
Help
Cancel
OK
Frame (750 bytes)
Decrypted TLS (688 bytes)
Text item (text), 74 bytes
Packets: 809 · Displayed: 15 (1.9%)
Profile: Default


PCAPdroid_15_Aug_08_10_30.pcap
ip.dst == 54.169.10.136 and http
File Data: 299 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "language" = "enUS"
Form item: "appid" = "aaagg10006"
Form item: "password" = "5f7b2e730cbbc2ca49428cfc0a19f249320e65fefbd6830299e924b0942745b7"
Form item: "loginname" = "mert.sarica@gmail.com"
Form item: "flag" = "70"
Form item: "version" = "2.8.6"
Form item: "isIPHONE" = "1"
Frame (750 bytes)
Decrypted TLS (688 bytes)
Text item (text), 74 bytes
Packets: 809 · Displayed: 15 (1.9%)
Profile: Default

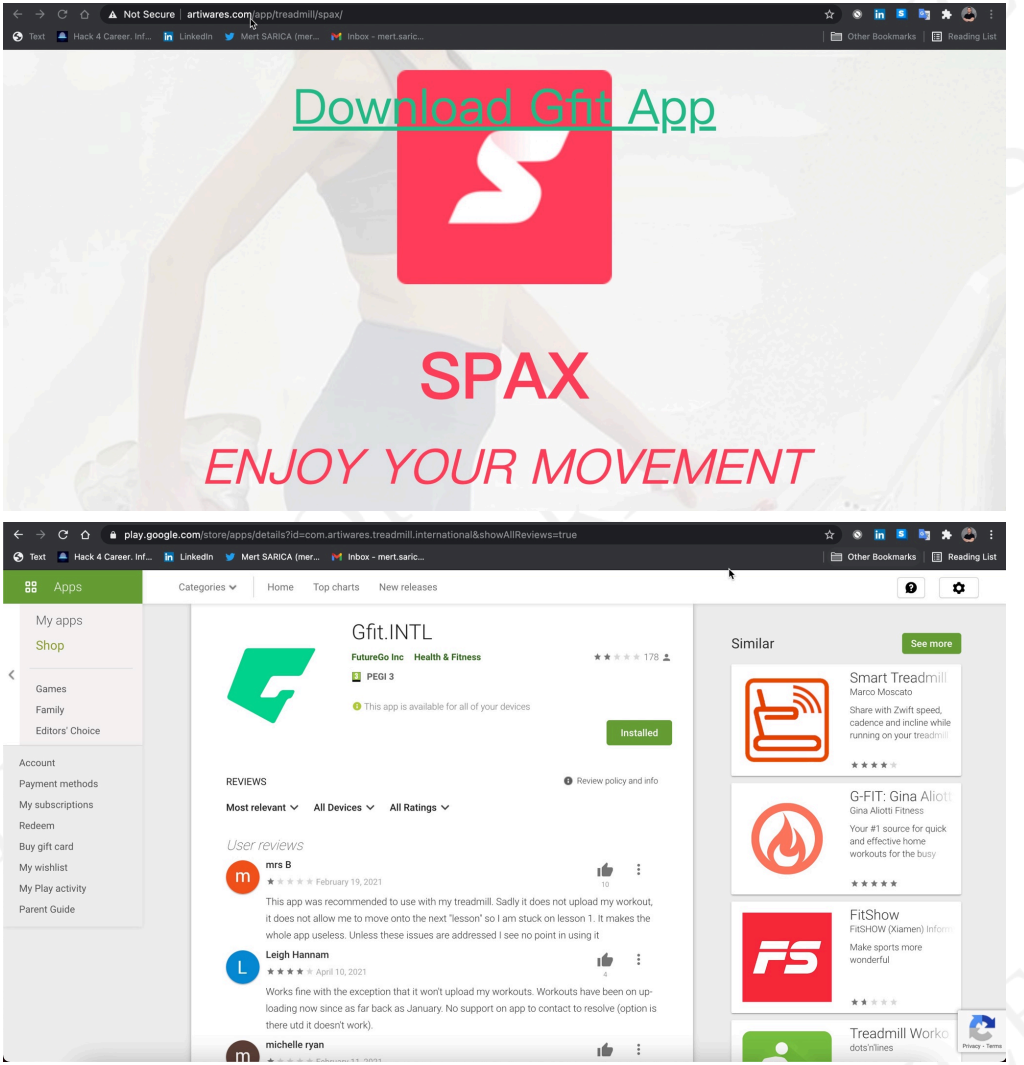
Koş Mert Koş

2020 yılı itibariyle ülkemizde etkisini arttıran Covid-19 salgını sebebiyle spor antrenörüm ile spor salonu yerine WhatsApp üzerinden spor yapmaya başladım. Zaman içinde antrenörümün yönlendirmesiyle satın almaya başladığım barfiks barı, ağırlık seti ve sehpası gibi spor aletleri, salgının pek de sona erecek gibi görünmemesi nedeniyle koşu bandı ile genişlemek durumunda kaldı ve son olarak Bluetooth fonksiyonuna Voit Active koşu bandı, spor aletlerimin arasındaki yerini almış oldu.



Açıkçası bu zamana dek satın aldığı elektronik aletleri hacklemeye çalışan (Yazıcı Deyip Geçmeyin!, Bir Drone Gördüm Sanki, Et tu, CPCR-505 ?, Casus Fare, Esaretten Kaçış gibi gibi) bir güvenlik araştırmacısı olarak masum koşu bandına orantısız güç uygulamak pek aklımın ucundan geçmiyordu. Ne zaman ki koşu bandında geçen yürüyüş sürem artmaya başladı işte o zaman koşu bandının panelindeki QR kod da daha fazla dikkatimi çekti.

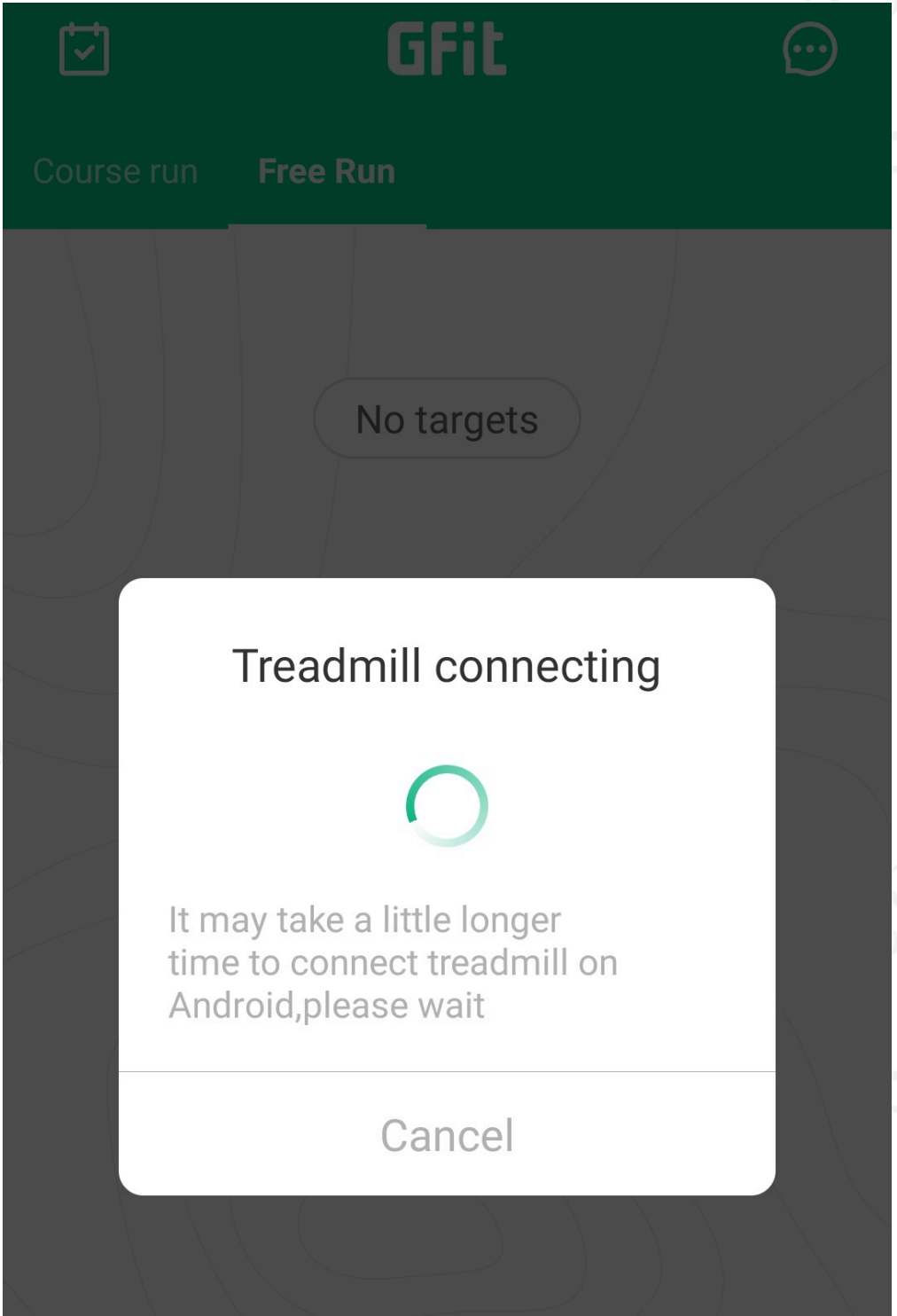
QR kodu bir uygulama yardımı ile okuttuğumda beni http://www.artiwares.com/app/treadmill/spax/ adresine oradan da çok sayıda olumsuz yoruma sahip olan ve ne idüğü belirsiz Çinli bir firma tarafından geliştirilen Google Play'deki
Gfit.INTL uygulamasının sayfasına yönlendirdiğini gördüm. Koşu bandı Bluetooth desteklediği için bu uygulamayı kurup ne tür komutlar gönderilebildiğini incelemeye ve kendimce kötüye kullanım senaryolarını ortaya çıkarmaya karar verdim.

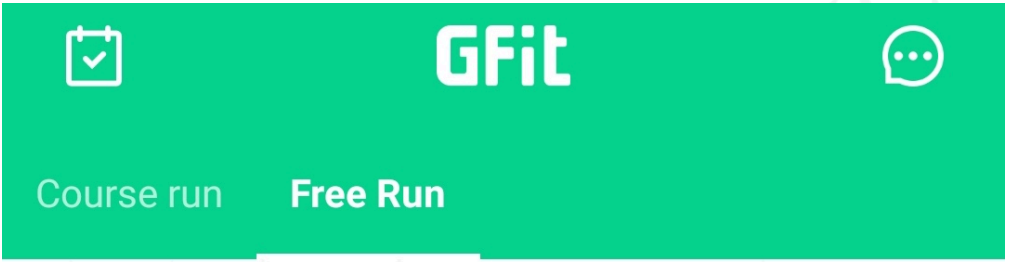


Bu araştırmayı yaptığımda favori araçlarımdan olan Genymotion öykünücüsü (emulator) Apple M1 işlemcili macOS desteklemediği için Android'de Kanca Atmak yazımda olduğu gibi öykünücü tabanlı dinamik analizden ve türlü imkanlarından faydalanamayacağımı iyi biliyordum.

Gfit uygulamasını cep telefonuma kurup **RunnerT** Bluetooth ismine

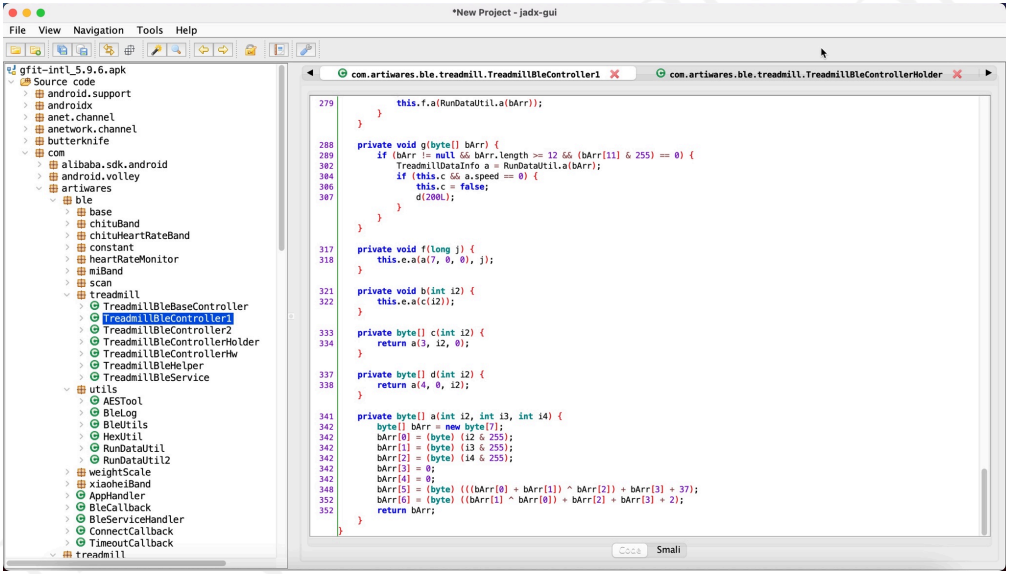
sahip koşu bandım ile eşleştirdikten sonra uygulama üzerinden koşu bandının temel fonksiyonları olan başlatma (start), hız arttırma, hız azaltma ve durdurma işlemlerini rahatlıkla gerçekleştirebildiğimi gördüm.


GFit
Course run
Free Run
No targets
Treadmill connecting
It may take a little longer time to connect treadmill on Android,please wait
Cancel



free run

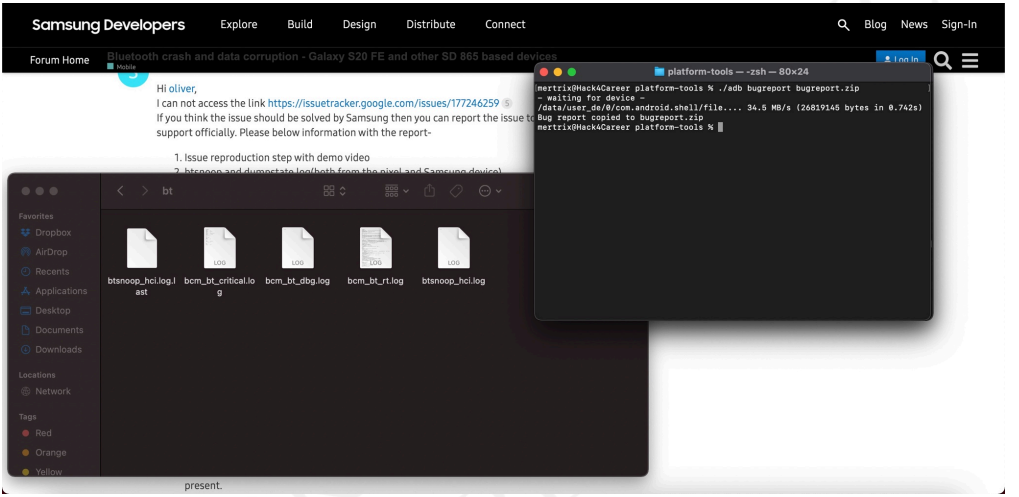
Uygulama tarafından koşu bandına gönderilen komutları öğrenmek istediğim için ya statik kod analizini tercih edecektim ya da uygulamanın yüklü olduğu cep telefonundan faydalanacaktım. Statik kod analizi ile ilerlemek daha pratik geldiği için jadx aracı ile Gfit uygulamasını incelemeye başladım.



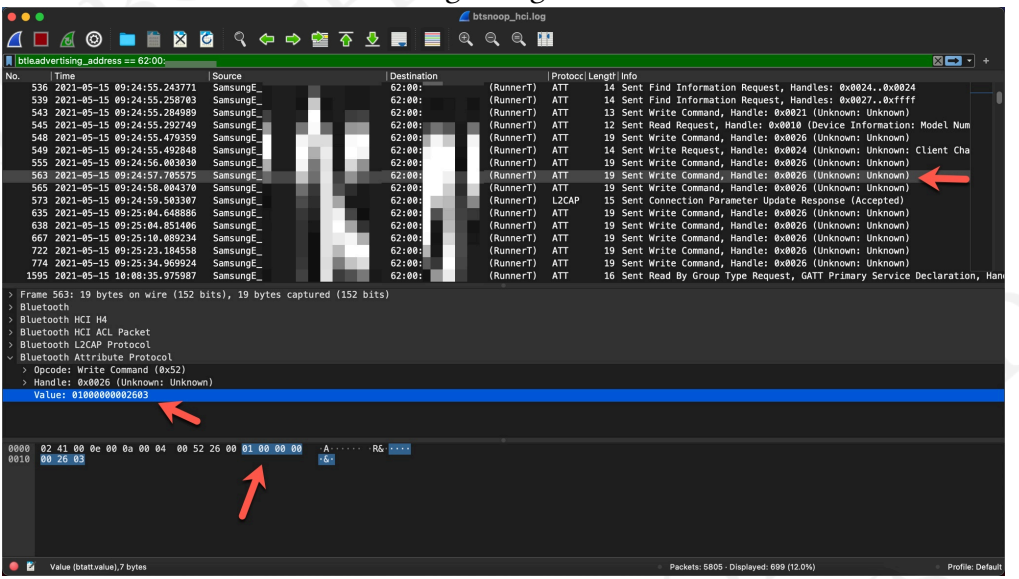
Uygulama genelinde kodlar gizlendiği (obfuscation) ve mevcut şartlar ve koşullarda öykünücü üzerinde dinamik kod analizi yapma şansım olmadığı için hemen pes edip telefon üzerinden neler yapabileceğime bakmaya karar verdim.

Samsung'un destek sayfasında Bluetooth paketleri kaynaklı problem yaşayan bir kişinin mesajına yazılan yanıttaki adımları takip etmeye başladım.

6. adıma geldiğimde Gfit uygulaması üzerinden koşu bandına başlatma, hız arttırma, hız azaltma, koşu bandını durdurma komutlarını gönderdim ve diğer adımlara **geçip btsnoop_hci.log** dosyasını Wireshark ile analiz etmeye başladım.



WireShark üzerinde **btle.advertising_address == 62:00:a1:18:b5:22** filtresi ile koşu bandına ulaşan ilk komuta baktığımda koşu bandını başlatma komutu olan **01000000002603** değerini gördüm.



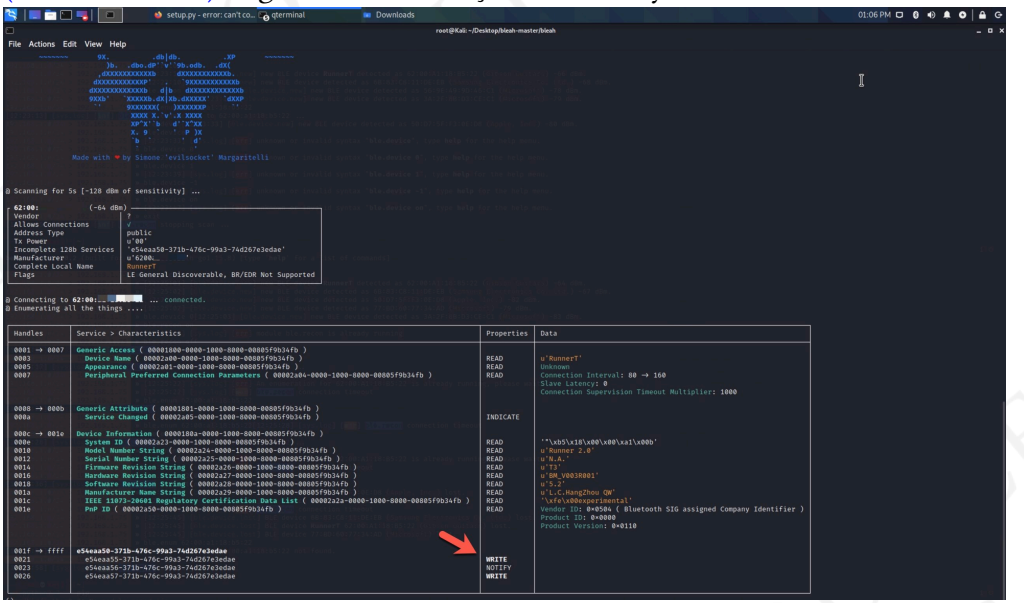
Daha sonra koşu bandına sırasıyla Bekletme/Pause (**05000000002a07**), hızı saatte 9 KM'ye ayarlama (**035a000000825b**), hızı saatte 5.2 KM'ye ayarlama

(**03340000005c39**) ve Durdurma (**02000000002704**) komutlarını gönderip WireShark üzerinde parantez içindeki diğer değerleri gördüm.

İlk olarak koşu bandının tekrarlama (replay) saldırısına açık olup olmadığını öğrenmeye karar verdim. Bunun için de öncelike BLE destekli koşu bandına elde ettiğim Bluetooth paketlerini gönderecek aygıtta ve araçta karar kılmam gerekti. Aygıt olarak Mavi Tehlike başlıklı blog yazımda da kullandığım Parani-UD100 imdadıma yetişti.

Sıra paket göndermek için araç bulmaya geldiğinde gatttool, bleah ve nRF Connect araçları arasından **bleah** ile ilerlemeye karar verdim.

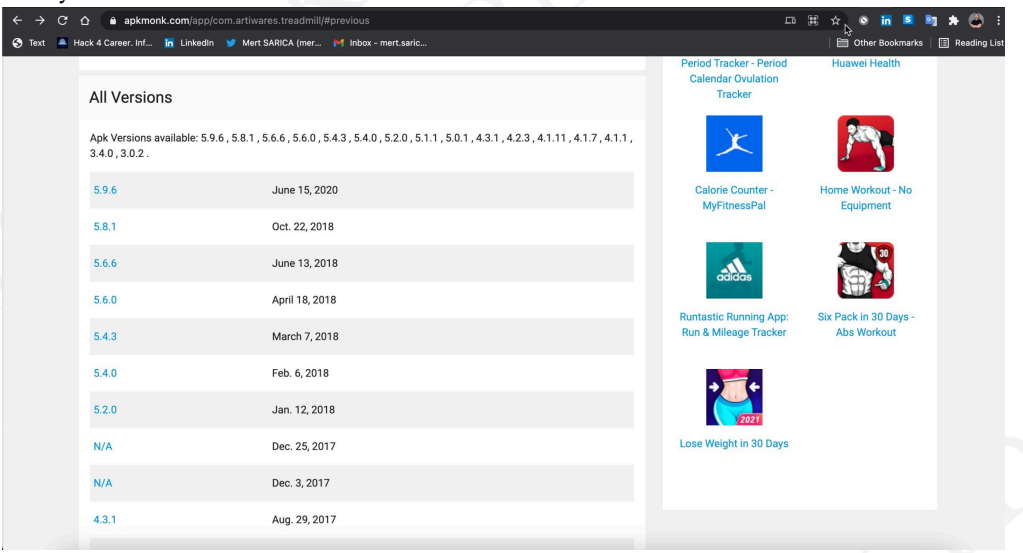
Kali işletim sistemi üzerinde **bleah -b "62:00:xx:xx:xx:xx" -e** komutu ile Generic Attribute Protocol (GATT) ile koşu bandına paket gönderebilmek için ihtiyaç duyacağım Servisler (Services) ve Karakteristikler (Characteristics) bilgilerine hızlı bir şekilde listeleyebildim.

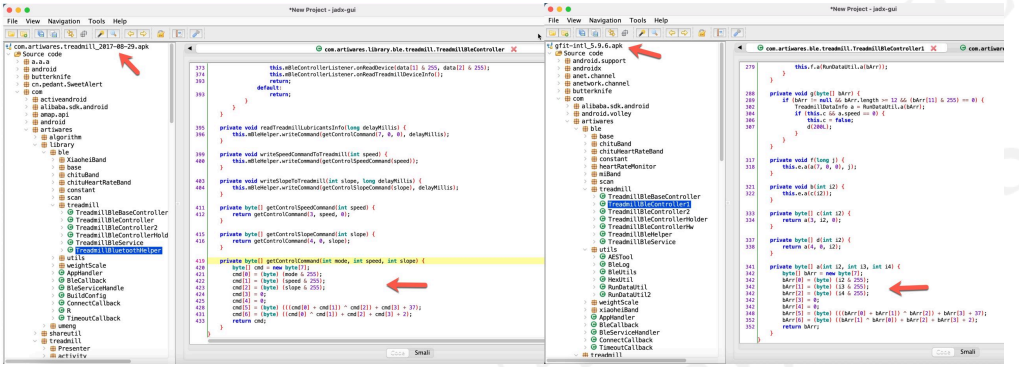


e54eaa57-371b-476c-99a3-74d267e3edae karakteristik bilgisinde **WRITE** özelliğini gördükten sonra bleah ile koşu bandına **bleah -b "62:00:xx:xx:xx:xx" -u "e54eaa57-371b-476c-99a3-74d267e3edae" -d**

“0x01000000002603” komutunu gönderdikten sonra koşu bandının başladığını gördüm!

Bu noktada koşu bandının tekrarlama saldırısına açık olduğunu öğrendikten sonra sıra bu komutların nasıl oluşturulduğunu öğrenmeye karar verdim. Kaynak kodu seviyesinde gizleme (obfuscation) tekniği kullanıldığı ve dinamik kod analizi de yapamadığım için Gfit uygulamasının eski sürümlerini indirip teker teker incelemeye başladım ve çok geçmeden 2017 sürümünde gizleme (obfuscation) tekniği kullanılmadığını gördüm. 2020 ve 2017 kaynak kodlarını yan yana koyduğumda Gfit uygulamasından koşu bandına gönderilen komutların nasıl oluşturulduğunu öğrenmem oldukça kolay oldu.



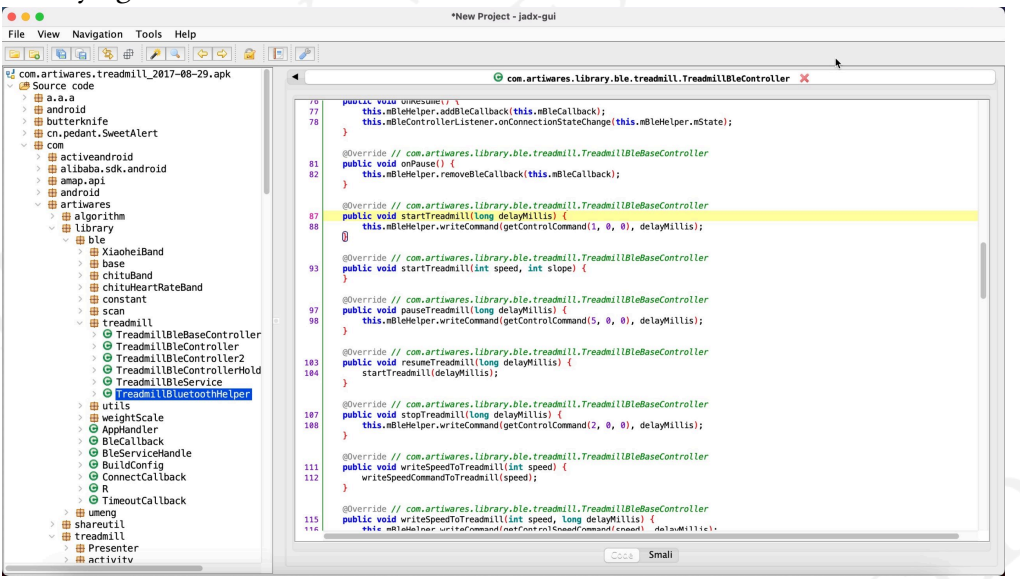


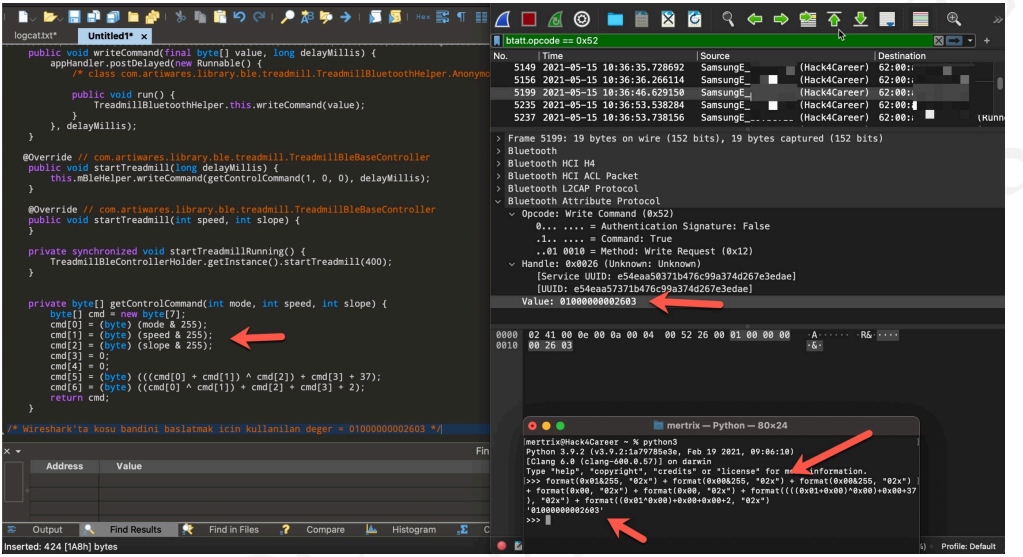
Örnek olarak kaynak koduna hızlıca göz attığımda, koşu bandını başlatmak (start) için **startTreadmill(long delayMillis)** fonksiyonu çağrılmakta ardından **mBleHelper.writeCommand(getControlCommand(1, 0, 0), delayMillis)** fonksiyonu ve son olarak koşu bandına gönderilecek 7 bayt değerindeki paketi oluşturan aşağıdaki **getControlCommand(int mode, int speed, int slope)** fonksiyonu çağrılmaktaydı.

```
private byte[] getControlCommand(int mode, int speed,
int slope) {
byte[] cmd = new byte[7];
cmd[0] = (byte) (mode & 255);
cmd[1] = (byte) (speed & 255);
cmd[2] = (byte) (slope & 255);
cmd[3] = 0;
cmd[4] = 0;
cmd[5] = (byte) (((cmd[0] + cmd[1]) ^ cmd[2]) +
cmd[3] + 37);
cmd[6] = (byte) ((cmd[0] ^ cmd[1]) + cmd[2] + cmd[3]
+ 2);
```

```
return cmd;
}
```

Koşu bandını başlatmak için **mode = 1**, **speed = 0**, **slope = 0** değişkenleri ile çağrılan yukardaki **getControlCommand** fonksiyonunda yer alan işlemleri Python ile gerçekleştirdiğimde **01000000002603** çıktısını oluşturabildim. Bu sayede artık Gfit uygulaması olmadan koşu bandını başlatacak komuttan **(getControlCommand(1, 0, 0))** hız arttırmaya **(getControlCommand(3, 5, 0))** kadar tüm komutları Python ile oluşturup **Parani-UD100** sayesinde **bleah** aracı ile koşu bandına gönderebilecek noktaya geldim.





Son olarak sıra aklıma gelen kötüye kullanım senaryolarını pratikte denemeye geldiğinde;

İlk olarak koşu bandının hız sınırı olan saatte 14 KM'yi 20 KM'ye yükseltmeye çalıştığımda (**bleah -b "62:00:xx:xx:xx:xx" -u "e54eaa57-371b-476c-99a3-74d267e3edae" -d "0x03c8000000f0cd"**) maksimum 14 KM'ye ayarlanabildiğini gördüm. (iyi haber)

İkinci olarak koşu bandına saatte 14 KM hızla giderken koşu bandına durdurma komutu gönderdiğimde (**bleah -b "62:00:xx:xx:xx:xx" -u "e54eaa57-371b-476c-99a3-74d267e3edae" -d "0x02000000002704"**) koşu bandının mevcut hızdan 0 KM'ye mevcut hız süresinde (Saatte 14 KM hızla koşuluyorsa 14 saniyede duruyor) saniyede düştüğünü gördüm fakat aynı paketi iki defa, peşpeşe gönderdiğimde bu defa 4-5 saniyede düştüğünü ve yüksek hızda koşarken kontrolsüz bir şekilde bu denli azalmasının koşan kişinin kaza yaşamasına imkan tanıyabileceğini düşündüm. (kötü haber)

Son olarak düşük hızda yürüyen veya koşan bir kişinin koşu bandına, sınırsız bir döngüde hızı satte 14 KM'ye yükselten komut gönderdiğimde aşağıdaki videoda olduğu üzere kişinin panik halinde hızı azaltmaya çalışsa

da başaramadığını bu nedenle kaza yaşama ihtimalinin ortaya çıktığını görmüş oldum. Bir de bu koşu bantlarından satın almış ve kullanıma sunmuş bir spor salonuna kötü niyetli bir kişinin gidip tüm koşu bantlarına sırasıyla bu komutu gönderdiğini düşündüğümde yaşanacak krizi gözümün önüne getirmek bile istemedim. (kötü haber)

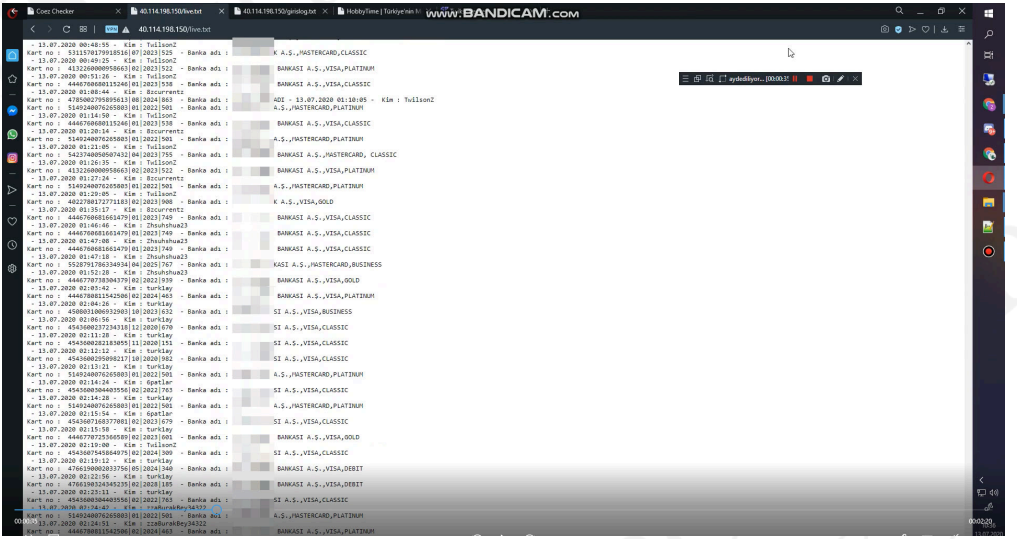
Bir veya daha fazla etkileşimli öğe, metnin bu sürümünde yer almadı. Bunları çevrimiçi olarak burada görüntüleyebilirsiniz: https://pressbooks.pub/mertrix/?p=49#oembed-1

Sonuç itibariyle Bluetooth fonksiyonunu kapatamadığınız ve yazılımı ne idüğü belirsiz Çinli bir firma tarafından geliştirilen bu koşu bandını satın almadan önce veya kullanırken risklerini göz önünde bulundurmanızı şiddetle tavsiye ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Çalıntı Kart Avı

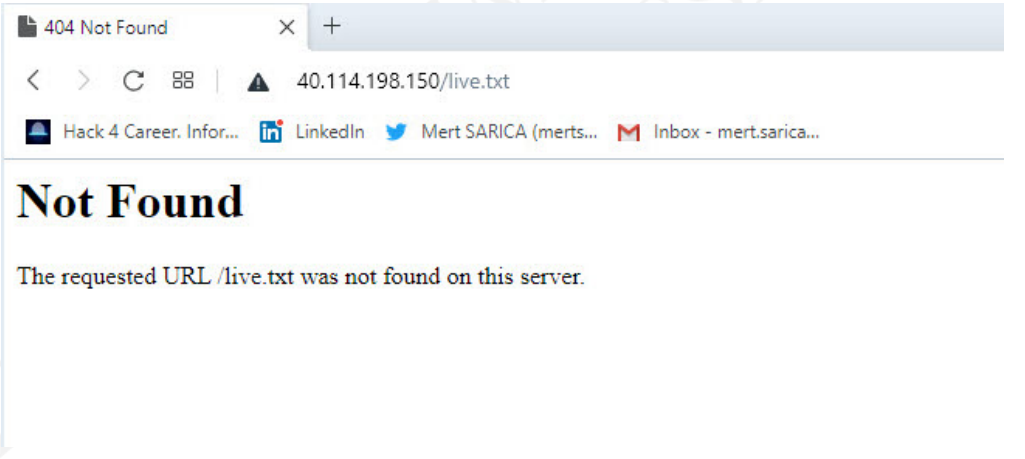
Sosyal medyayı oldukça etkin kullanan bir güvenlik araştırmacısı olarak bu zamana dek sosyal ağlar, e-postalar üzerinden aldığım mesajları güvenlik araştırmalarına ve ardından blog yazılarına, sunumlara çevirdiğimi biliyorsunuzdur. Çıkış noktası diğerleri ile aynı olan bu hikayede ise müşteri güvenliğini sağlamak amacıyla sosyal ağ üzerinden gelen bir siber tehdit istihbaratından nasıl faydalandığımı görebilirsiniz.

Her sabah olduğu gibi **17 Temmuz 2020** sabahı da uyandıktan hemen sonra telefonumu elime alıp siber güvenlik haberlerine göz atmak için sosyal medya hesaplarıma göz atmaya başladım. LinkedIn üzerinde Ebubekir BASTAMA isimli bir kişinin bankalar dışında beni de etiketlediği bir mesaj dikkatimi çekti. Mesajında bir videoda yer alan ve açık halde görülen kredi kartı bilgilerinin yer aldığını ve müşteri güvenliği adına bunların iptal edilip edilmediğini merak ediyordu.



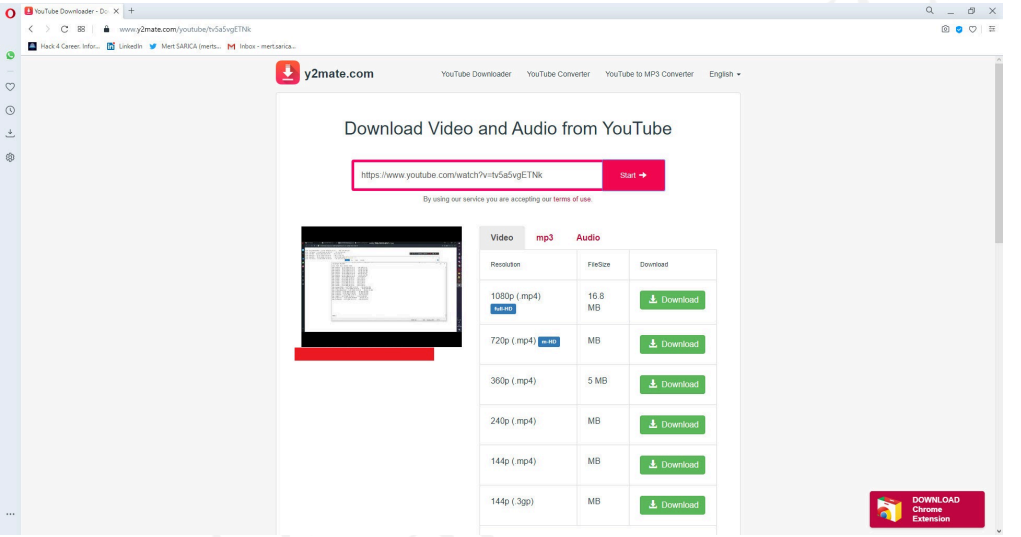
Videoyu izlemeye başladığımda Coez Checker isimli çalıntı kartları kontrol

etmek amacıyla kullanılan bir servisin dolandırıcılar tarafından diğer dolandırıcılara mesaj vermek amacıyla hacklendiği anlaşılıyordu. Dolandırıcı, yaklaşık 3 dakikalık videonun 30 saniyesi boyunca sistem üzerinde kayıtlı olan **13 Temmuz** tarihli çalıntı kart bilgilerini gösteriyor ve ardından diğer dolandırıcılara mesajını ilettikten sonra video kaydı sonlanıyordu. Videoda görünen çalıntı kart bilgilerinin yer aldığı **http://40[.]114.198.150/live.txt** adresine ulaşmak istediğimde ise tahmin ettiğim üzere dosya çoktan yayından kaldırılmıştı ve elimde sadece bu video ile kalakalmıştım.

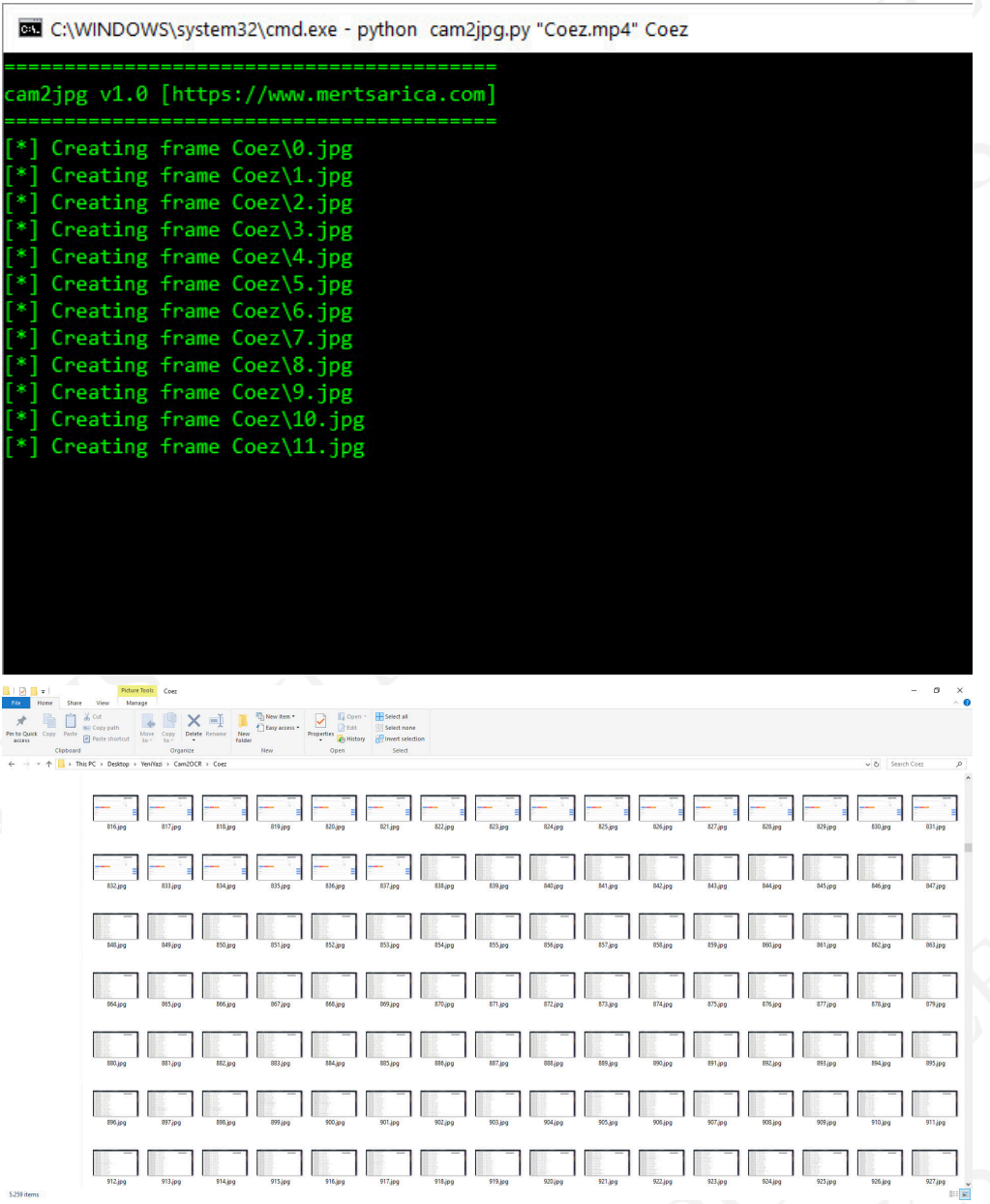


Vatandaşların dolandırıcılar tarafından mağdur edilmemesi adına bu videodaki kart bilgilerini başta Sektörel SOME/BDDK olmak üzere bankalarla da paylaşmak için videodan nasıl elde edebileceğimi düşünmeye başladım. 2009 yılında X Finans Kuruluşu – Animated Captcha (GIF) başlık blog yazım için benzer bir çalışma yaptığımı anımsayarak bu defa video dosyasını karelere (frame) ayırmaya ardından da Sponsorlu Dolandırıcılık başlıklı blog yazımda olduğu gibi görüntü dosyalarını OCR ile analiz edip kart bilgilerini ortaya çıkarmaya karar verdim.

İlk iş olarak Y2mate YouTube Downloader web sitesinden faydalanarak Youtube üzerinden ilgili video dosyasını indirdim.

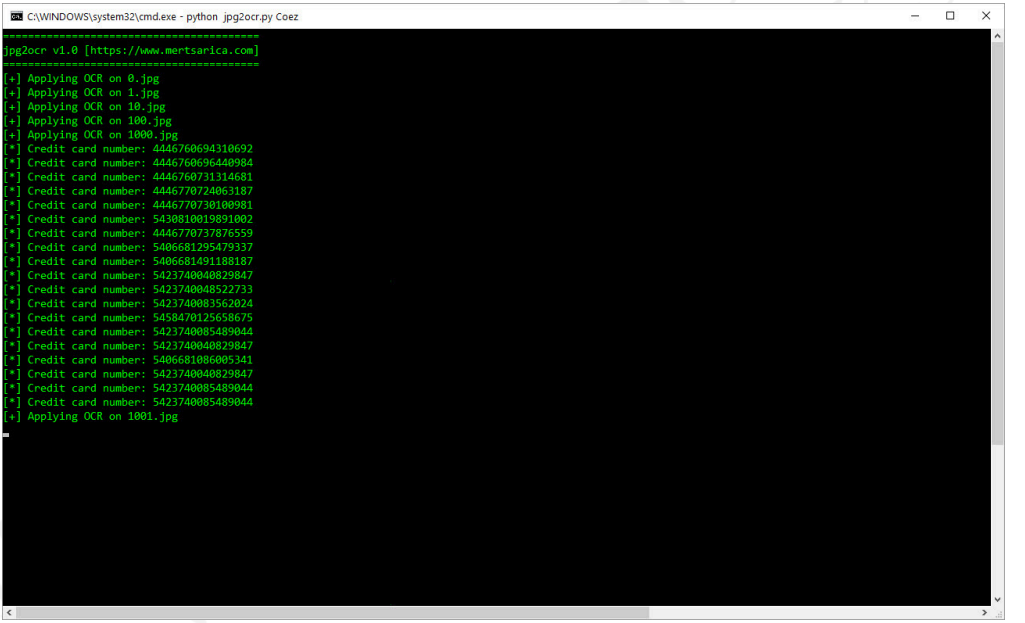


Python ile belirtilen video dosyasını karelere ayırıp, JPEG dosya biçiminde saklayan Cam2Jpg isimli bir araç geliştirip indirdiğim video dosyası üzerinde çalıştırdığımda ortaya 5000'den fazla görüntü dosyası çıktı.



Bu defa Python ile Python-tesseract projesinden faydalanarak görüntü

dosyalarını analiz edip, kredi kartı numaralarını tespit eden **Jpg2Ocr** (kötüye kullanılmaması adına aracı yayınlamama kararı aldım) isimli başka bir araç daha geliştirdim. Bu aracı görüntü dosyaları üzerinde çalıştırdığımda kısa süre içinde **1000**'den fazla kredi kartı numarası ortaya çıkmış oldu.



Elde ettiğim tüm kredi kartı bilgilerini aynı gün içinde yetkili mercilerle paylaşarak daha fazla vatandaşımızın mağdur olmasını engellemenin verdiği sorumluluk bilinci ve mutluluk ile bir güvenlik araştırmamı daha tamamlamış oldum.

Kurum olarak bir veya birden fazla siber tehdit istihbaratı servisinden faydalansanız da istihbaratın gelmemesi veya gecikmeli gelmesi durumlarına karşı kendi imkanlarınızla da sosyal ağları yakından takip etmenizde her zaman fayda olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.