

Akıllı Çocuk Saatleri

written by Mert SARICA | 1 September 2022

If you are looking for an English version of this article, please visit [here](#).

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 standartlara uyan ve lisans sahibi değililer 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 mümkün olup olamayacağını sormak isterim (inaniyorum 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 ?



Yoksa ařağıdaki dięer bir fotoęrafa bakıldıęında ebeveynlerin, kendilerinin ve çocuklarının mahremiyetini, özel hayatlarının gizlilięini istemeden de olsa tehlikeye attıkları, ortam dinlemeye imkan tanıyan saat görünümlü potansiyel casus bir cihaz mı ?



Bu sorulara yanıt bulmak için ilk olarak güvenlik arařtırmamda kullanmak üzere fiyat aısından uygun olan bir ocuk saati satın almaya karar verdim. Bunun için Hepsiburada, Trendyol gibi alıřveriř sitelerindeki Akıllı ocuk Saatleri kategorilerini incelemeye bařladım. En ok satılan, yorum ve deęerlendirme yapılan saatlere baktıktan sonra 1000'e yakın deęerlendirmesi olan bir marka ve modelde karar kılıp, satın aldım.

trendyol

Ardığınız ürün, kategori veya markayı yazınız



Hesabım

Favorilerim

Sepetim

KADIN ERKEK ÇOCUK EV & MOBİLYA SÜPERMARKET KOZMETİK AYAKKABI & ÇANTA SAAT & AKSESUAR ELEKTRONİK SPOR&OUTDOOR

Anasayfa > Elektronik > Giyilebilir Teknoloji > Akıllı Çocuk Saati

İlgili Kategoriler

Akıllı Çocuk Saati

Marka

Marka ara

☐ Alcatel

☐ TCL

☐ Smartbell

☐ Bilicra

☐ HANGAREX

☐ Fitbit

☐ RealFoni

☐ Pami

Renk



Fiyat

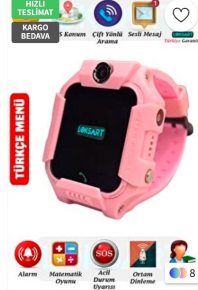
"Akıllı Çocuk Saati" araması için 673 sonuç listeleniyor

Önerilen

Hızlı Teslimat yapılan ürünleri göster.

Uygula

ÖNCEKİ ÜRÜNLERİ GÖSTER



Loksart Sim Kartlı Akıllı Çocuk Saat



Fitbit Kız Çocuk Pembe Sim Kartlı Türkçe Menü İmei Kayıtlı Smartcel...



Qfit Qfit Q4 4.5g Akıllı Çocuk Saati Pembe



medigen Akıllı Çocuk Saati Sim Kartlı Konum Takip

Fiyat Aralığı

250 - 500 TL

Cinsiyet

Erkek Çocuk

Cinsiyet

Kız Çocuk

Temizle

Marka

Filtrele

☐ Nabil

☐ Nalan

☐ Onni

☐ Otto

☐ Q12

☐ Xinhang

☐ Yohosport

☐ Yukka

☐ Intermex

Fiyat Aralığı

250 500

☐ 50 - 100 TL

☐ 100 - 250 TL

☒ 250 - 500 TL

☐ 500 - 750 TL

☐ 750 - 1000 TL

☐ 1000 - 1500 TL

☐ 1500 - 2000 TL

☐ 2000 - 2500 TL

☐ 2500 TL üzerinde

Marka

Sharplace

Easytoy

Flameer

Xbazzar

StarWomen

Sunfay

Wayle



LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kameralı, Gizli Dinleme...

389,90 TL

★★★★★ 1575



LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kameralı, Gizli Dinleme...

389,90 TL

★★★★★ 1575



LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kameralı, Gizli Dinleme...

389,90 TL

★★★★★ 1575



LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kameralı, Gizli Dinleme...

569,90 TL %14

489,90 TL

★★★★★ 1575



Smartbell Q539/2020 Sim Kartlı Akıllı Çocuk Saati - Pembe

390,00 TL %1

385,00 TL

Sepete ekle



Smartbell Q539/2020 Sim Kartlı Akıllı Çocuk Saati - Mavi

390,00 TL %1

385,00 TL

★★★★★ 914



Kallow Z10 Akıllı Çocuk Takip Saati - Yeşil

390,00 TL

★★★★★ 801



Kallow Z10 Akıllı Çocuk Takip Saati - Mor

390,00 TL

★★★★★ 801



ÜRÜNÜ 2 SAAT BOYUNCA POWER BANK VEYA BİLGİSAYAR İLE ŞARJ EDİNİZ.
AKSİ TAKDİRDE ÜRÜN GARANTİ KAPSAMI DIŞINDA KALACAKTIR.

Sayın kargo personeli, büyük bir özveri ile üretilip,
Paketlenen bu ürünün çok özel bir bekleyeni var.
Lütfen bu paketi özenle ulaştırın. Her şey için teşekkürler.

Değerli müşterimiz eğer hizmetimizden memnun kaldıysanız.
Memnuniyetinizi yorumlar kısmında değerlendirerek bizlere
destek vermiş olursunuz ve sizlerin sayesinde ürünlerimizi
bütün çocuklarınıza ulaştırmış oluruz.

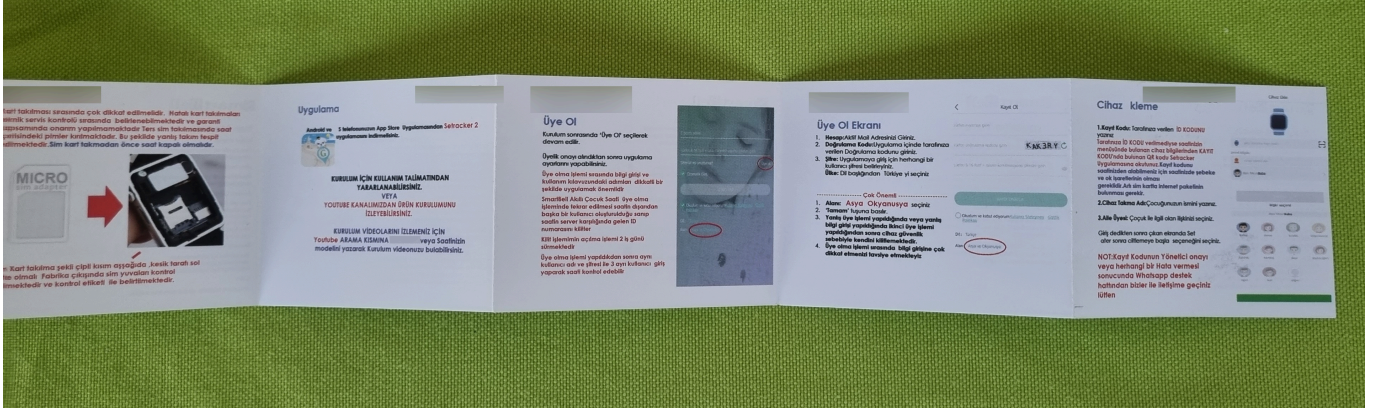
Elektronik kategorisinde 'ki ürünler'de ambalaj, kutu
açıldıktan sonra **iate koşulu** bozulmaktadır.

LÜTFEN ÜRÜNÜ AÇARKEN VIDEO ÇEKİP AÇINIZ.

Üründe sorun olduğunu düşünüyorsanız
Whatsapp hattından servis desteği almalısınız.

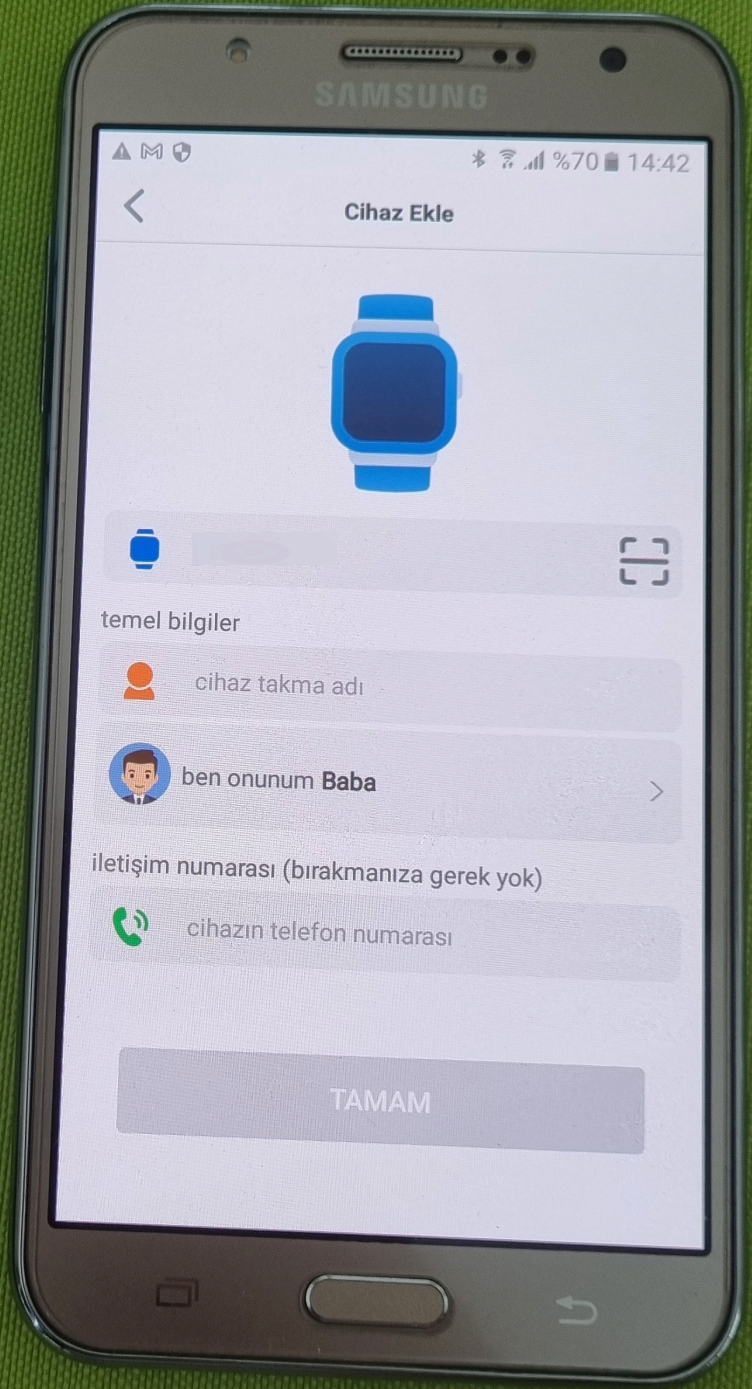
Servisten alacağınız rapor ile ürün **değişimini** yapabilirsiniz.

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.

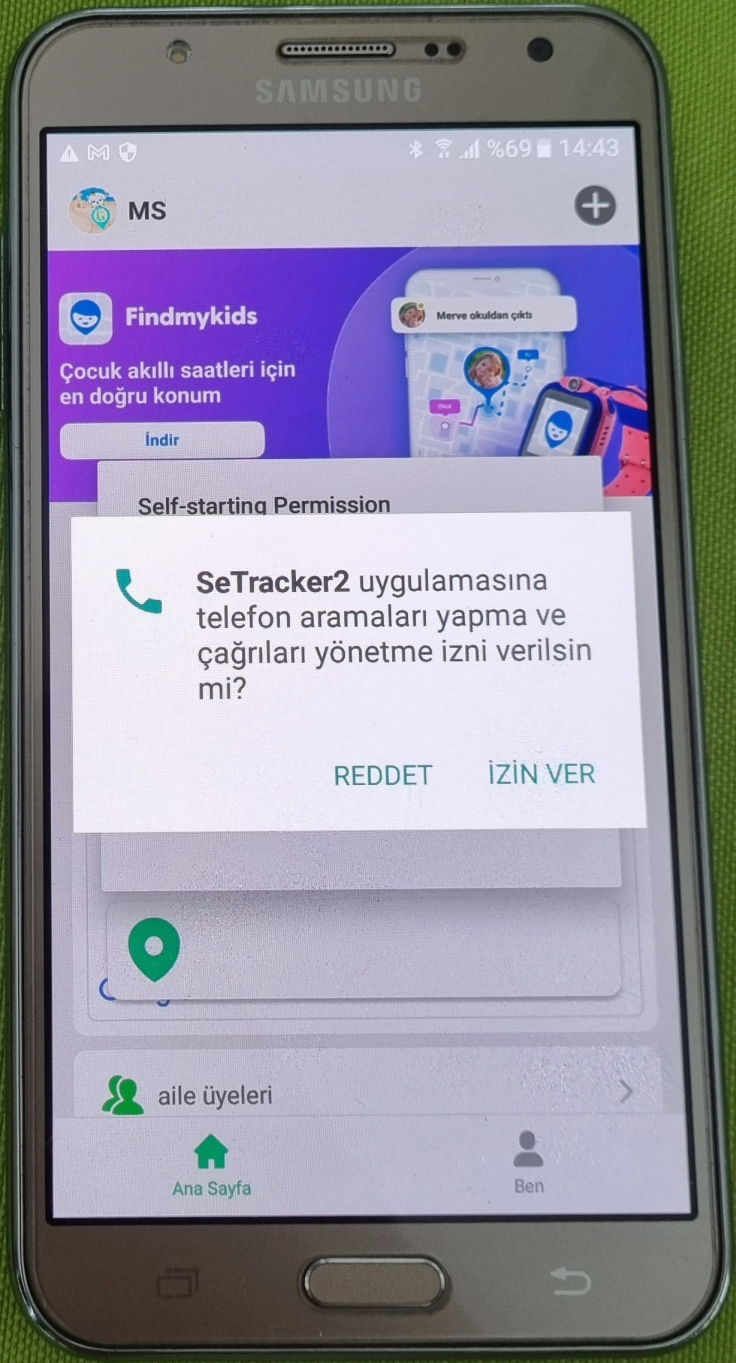


SeTracker2 isimli uygulamanın topladığı bilgilere baktığımızda lokasyon, ses ve görüntü kaydından, rehber, isim, cep telefonu ve e-posta adresine kadar kişiye özel, hassas, mahrem sayılabilecek bilgiler olduğunu gördüm.

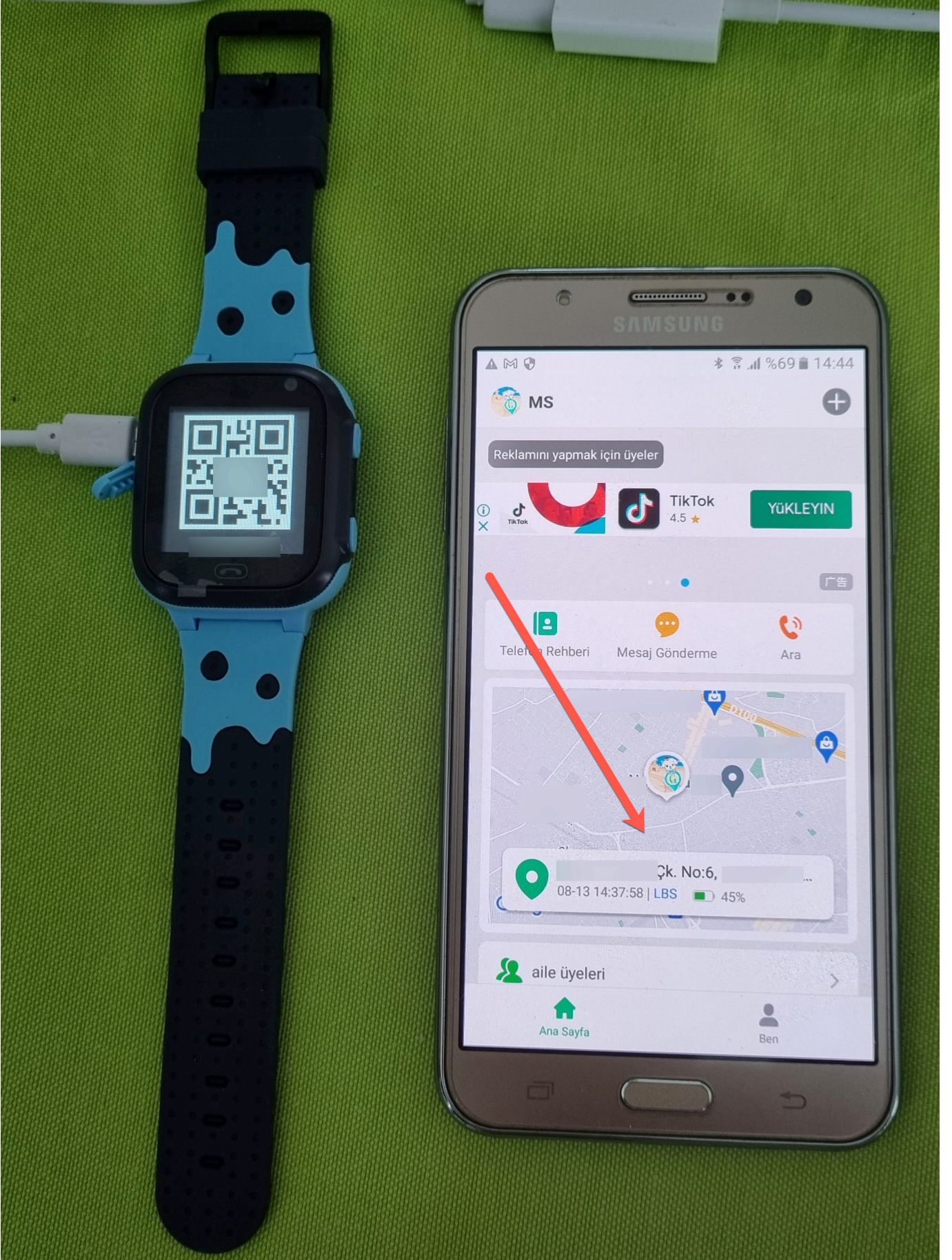
Saate SIM kartı takıp, çalıştırdıktan sonra SeTracker2 uygulamasını açıp, kayıt oldum. Daha sonra uygulamaya ile saati eşleştirdikten sonra uygulamayı ve menü adımlarını incelemeye başladım.

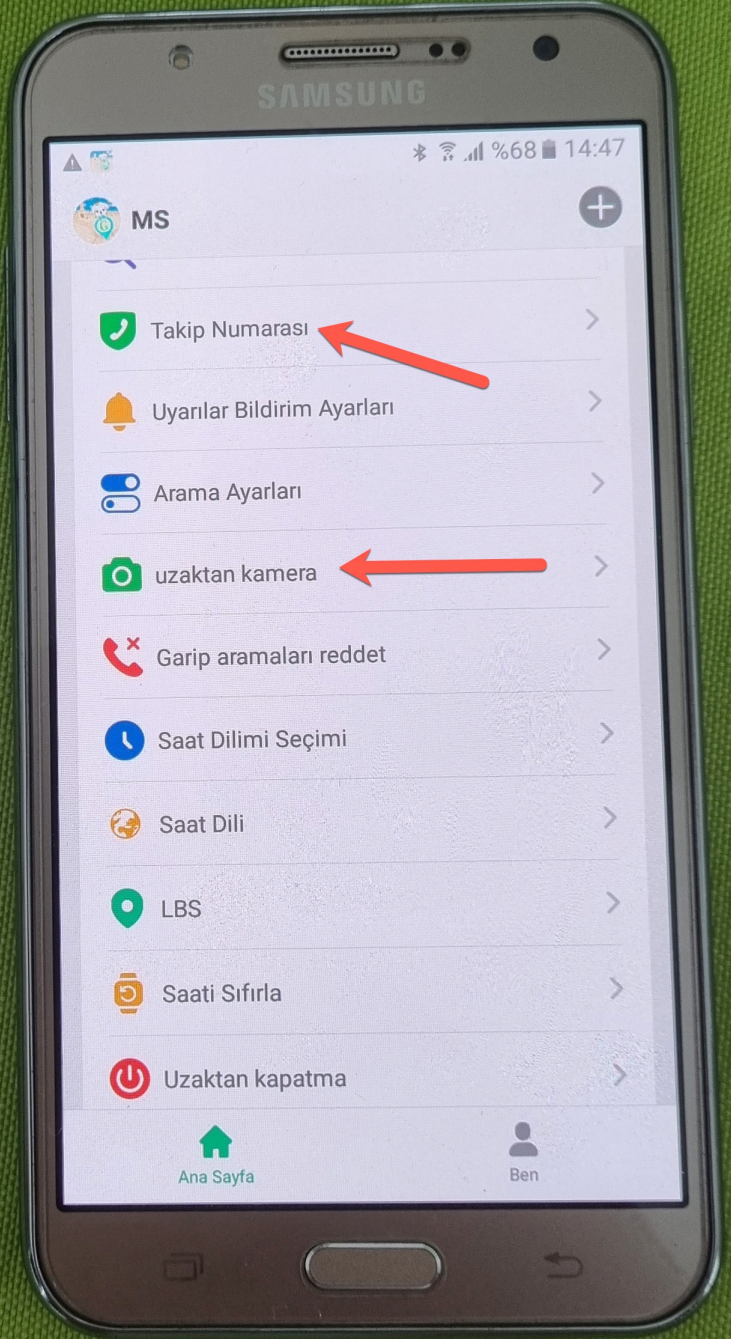


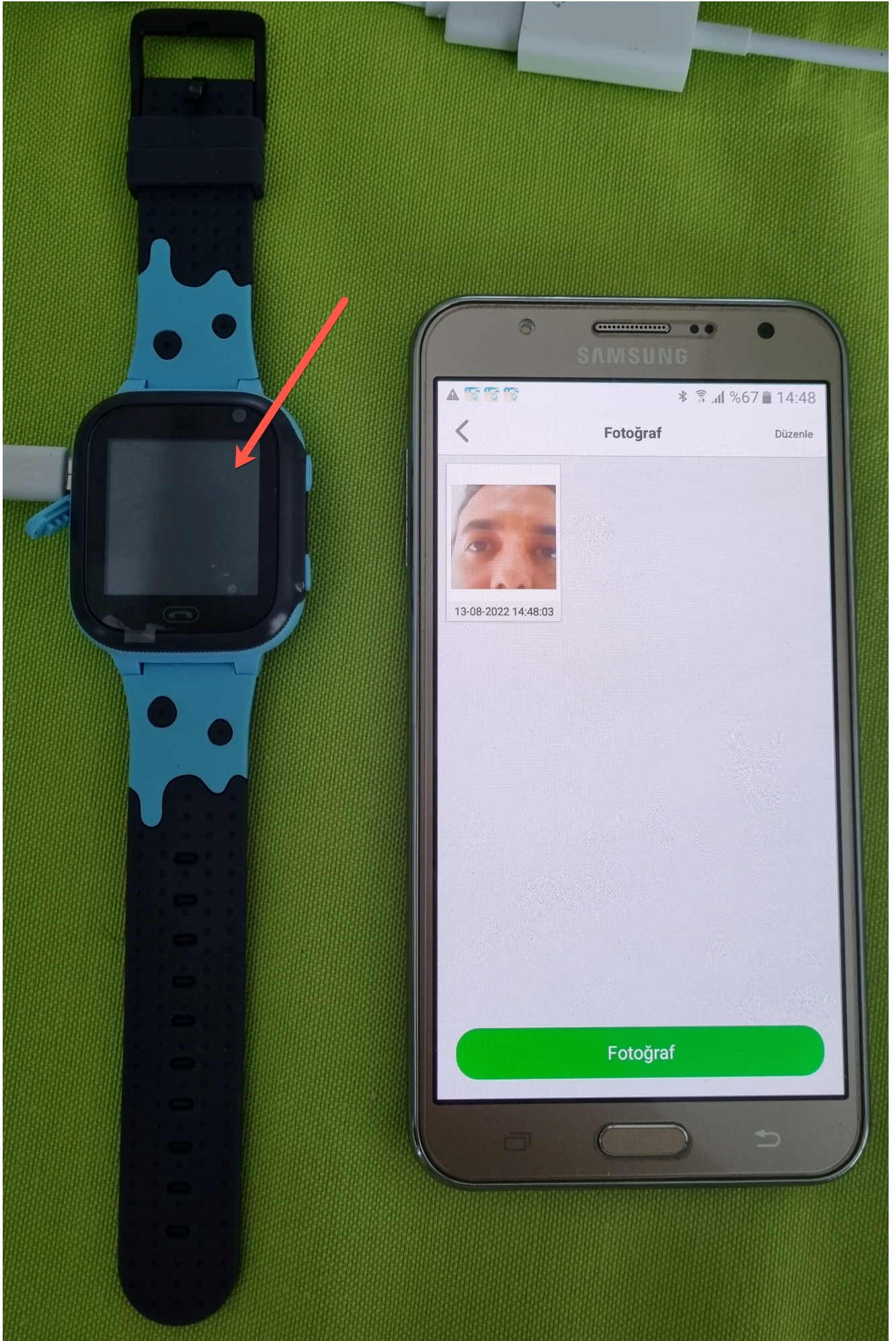




Uygulamada öncelikle dikkatimi çeken nokta, saatin harita üzerinden anlık olarak izlenebilmesi daha sonra ise Takip Numarası ve uzaktan kamera menü adımları oldu. Uzaktan kamera menüsü üzerinden saatteki kamera ile istediğiniz zaman fotoğraf çekilebiliyorsunuz. Bu esnada saat herhangi bir görsel veya 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 adımıyla olduğu gibi telefon, ortam dinlemesi yapıldığına dair herhangi bir uyarı vermiyor.







“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 olmadığına da altını çizelim!

“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 adli 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 adli 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 araştırmalarım aşına 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 anlattıklarımın sonuna 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 görünümü 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.

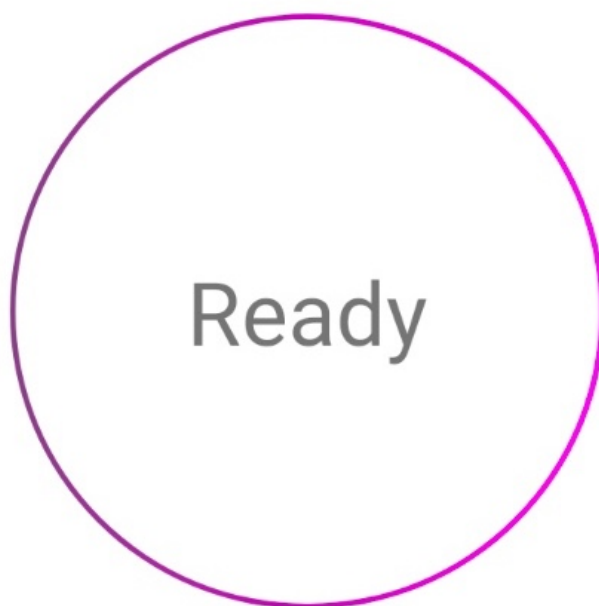
Not: Teknik okurlarım için de SeTracker2 uygulamasında SSL Pinning yönteminin kullanıldığını, HTTPS trafiğini analiz etmek için PCAPdroid isimli bir

Android uygulaması sayesinde basit bir şekilde trafięi kayıt altına aldığımı ve daha sonrasında da Wireshark aracı ile analiz edebildiğimi de paylaşayım.



STATUS

CONNECTIONS



PCAP file

Create a PCAP file in device storage



Target app



SeTracker2 (com.tgelec.setracker)





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

Capture as root

Allows PCAPdroid to run with other VPN apps



The screenshot displays the Wireshark network protocol analyzer interface. The top status bar indicates the capture file is 'PCAPdroid_15_Aug_08_10_30.pcap' and the filter is 'ip.dst == 54.169.10.136 and http'. The packet list on the left shows a series of HTTP and TLS-related packets. The packet details pane on the right shows the 'Transport Layer Security' dialog box, which is used to configure TLS decryption. The dialog box has tabs for 'RSA key list', 'TLS debug file', and 'Pre-Shared Key'. The 'TLS' tab is selected, showing a list of TLS records and a 'Reassemble TLS records spanning multiple TCP segments' checkbox. The 'Reassemble TLS Application Data spanning multiple TLS records' checkbox is also checked. The 'Message Authentication Code (MAC), ignore "mac failed"' checkbox is unchecked. The 'Pre-Shared Key' field is empty. The '(Pre)-Master-Secret log filename' field is set to 'locust Saati/pcap_dump_tls/sslkeylogfile_1508.txt'. The 'Help' button is visible at the bottom left of the dialog box. The main packet list shows a series of HTTP and TLS-related packets, including a 'POST /app/public/S10APP/v2_new_userLogin2 HTTP/1.1' packet and a 'GET /app/public/S10APP/v2_getNoticeInfo?language=enUS×tamp=1660800000 HTTP/1.1' packet. The packet details pane shows the 'Form Data' of the selected packet, including fields like 'language', 'appid', 'password', 'loginname', 'flag', 'version', 'isIPHONE', and 'timestamp'.