

Smart Watches for Kids

written by Mert SARICA | 1 September 2022

This story began on May 4, 2022, with an email from a reader named Erman ATEŞ. In his email, Mr. Erman, a conscious and sensitive father, stated that smart kids' watches are increasingly being preferred by many parents for valid reasons, but due to their lack of conformity to standards in terms of software, security, and privacy, and also due to a message he saw on Instagram, he began to worry on behalf of all parents and asked me to focus on this issue. As a security researcher who always listens to readers, as in my blog posts Instagram Scammers, Backdoor Hunting, Hacker Hunt with a Deception System, I decided to address this issue for the benefit of society and awareness of information security.



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 (inanıyorum bu konuda size yazan ilk kişi ben değilimdir).

Teşekkürler, saygılar.

Erman

Upon looking at the following photo, are kids' smartwatches really a tremendous technological boon for parents to keep their children under surveillance?



Or, upon looking at the following other photo, are parents unwittingly putting their own and their children's privacy and secrecy of their private lives at risk with a watch-like potential spy device that allows for audio surveillance?



To find answers to these questions, I decided to purchase a children's smartwatch that was affordable in terms of price for my security research. For this, I began to examine the Kid's Smartwatches categories on shopping sites such as Hepsiburada and Trendyol. After looking at the most popular watches with the most reviews and ratings, I decided on a brand and model with over 1000 ratings and purchased it.

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

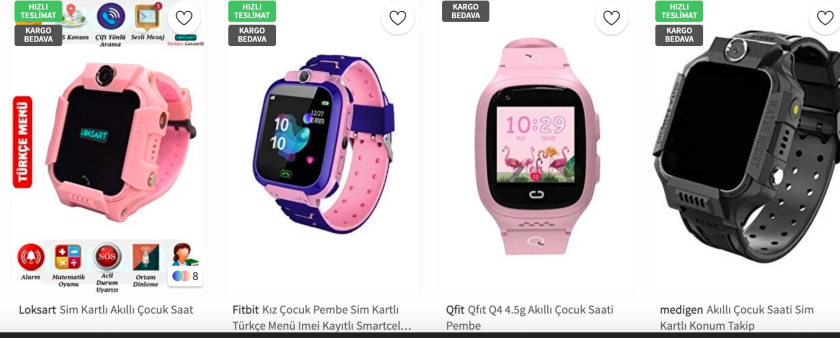
"Akıllı Çocuk Saati" araması için 673 sonuç listeleniyor

Önerilen

Hızlı Teslimat yapılan ürünleri göster.

Uygula

ÖNCEKİ ÜRÜNLERİ GÖSTER



Fiyat Aralığı

250 - 500 TL

Cinsiyet

Erkek Çocuk

Cinsiyet

Kız Çocuk

Temizle

Marka

Filtrele

☐ Nabil

☐ Nalan

☐ Omni

☐ 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

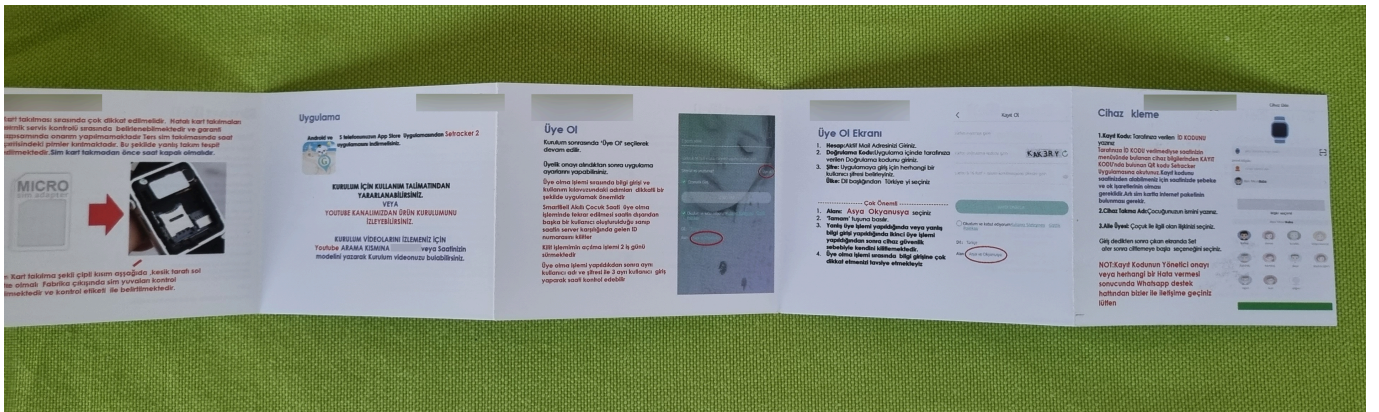
★★★★★ 801



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

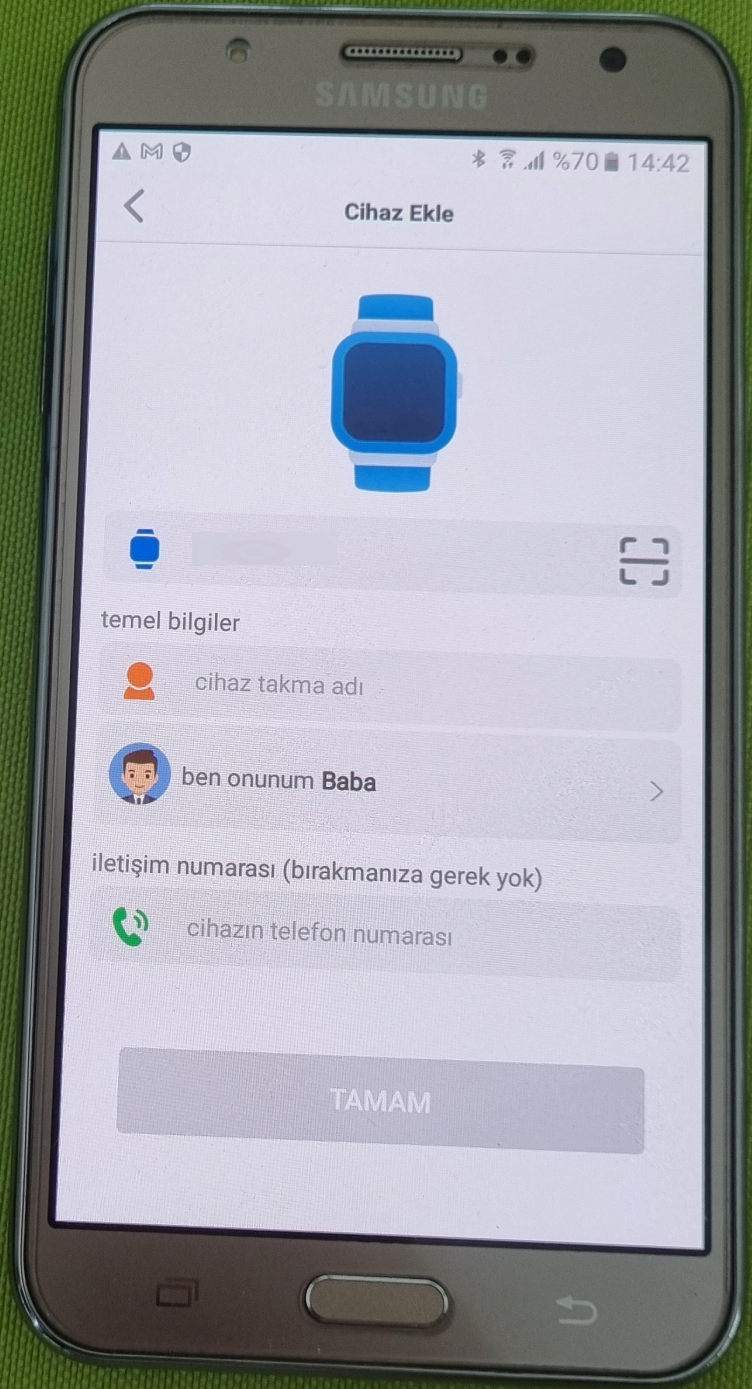


When I took the watch out of the box and looked at the installation guide, it stated that an Android or iOS mobile application developed by a Chinese company called 3G Electronics was required to remotely manage the watch.

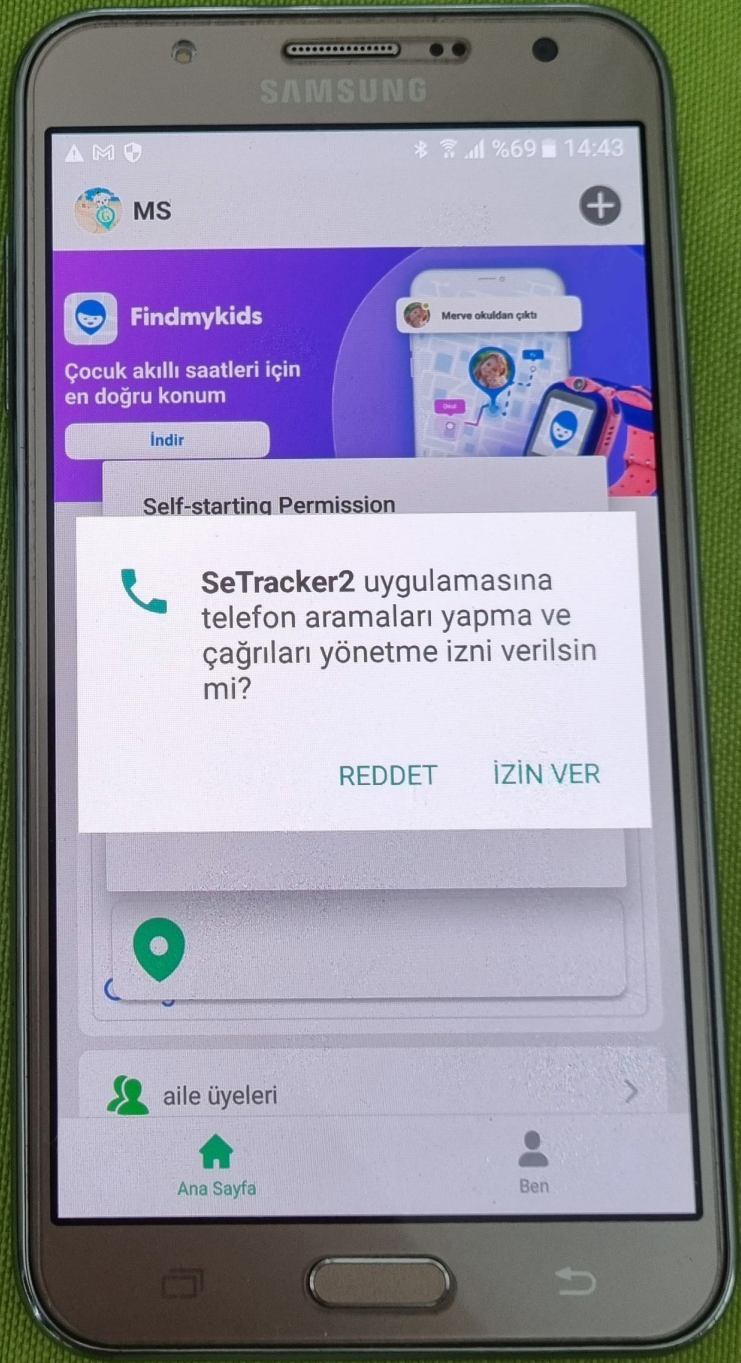


Upon examining the information collected by the SeTracker2 app, I saw that it collected personal, sensitive, and potentially private information ranging from location, audio, and video recordings, to the contact list, name, phone number, and email address.

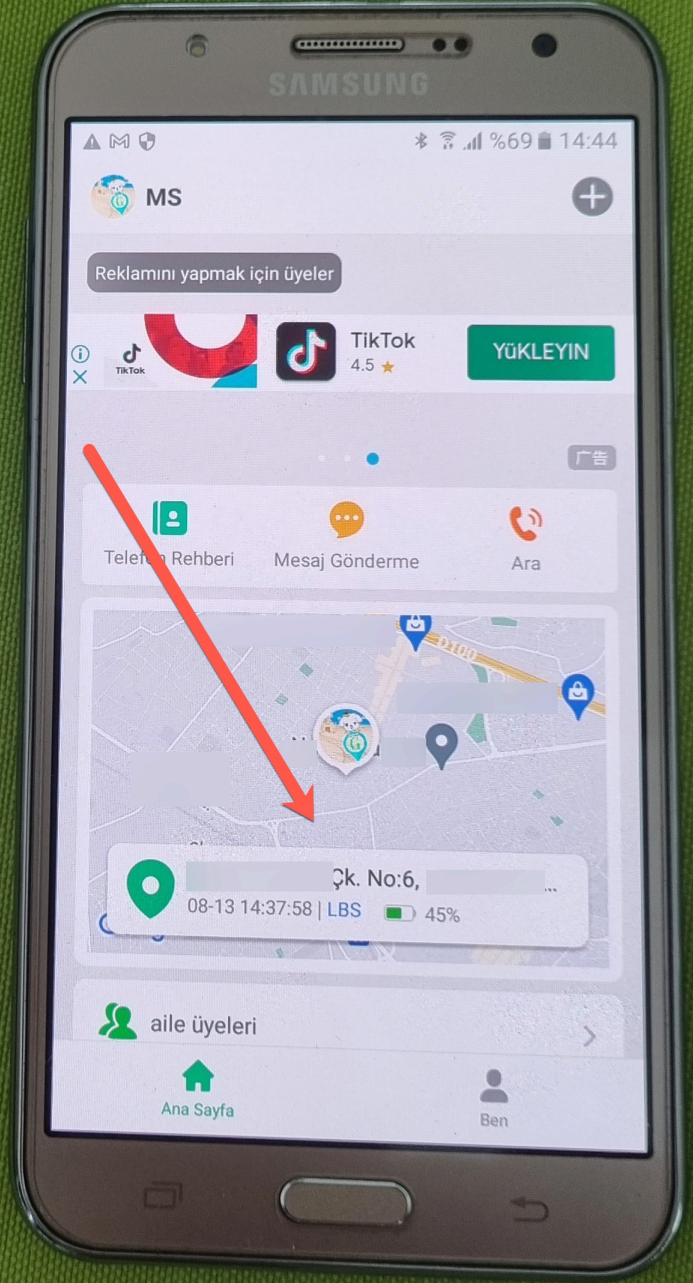
After inserting a SIM card into the watch and turning it on, I opened the SeTracker2 app and registered. Then, after pairing the app with the watch, I began to examine the app and the menu steps.

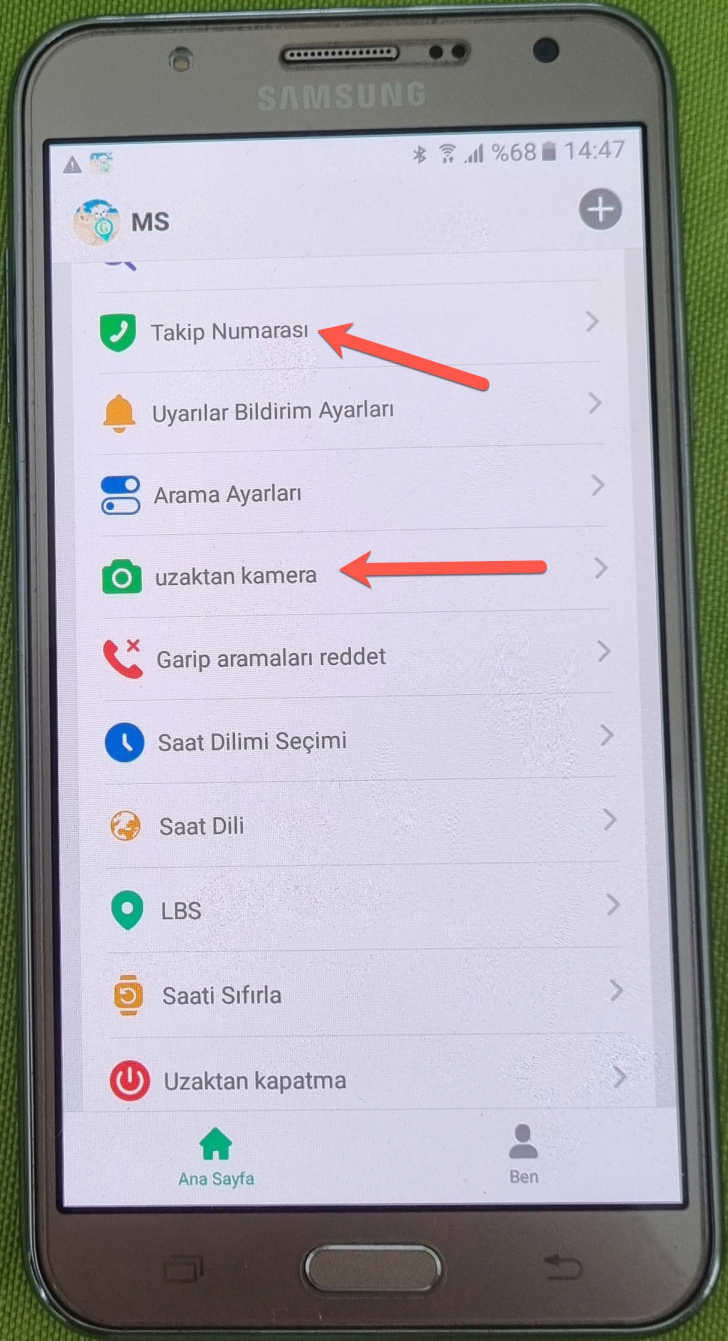


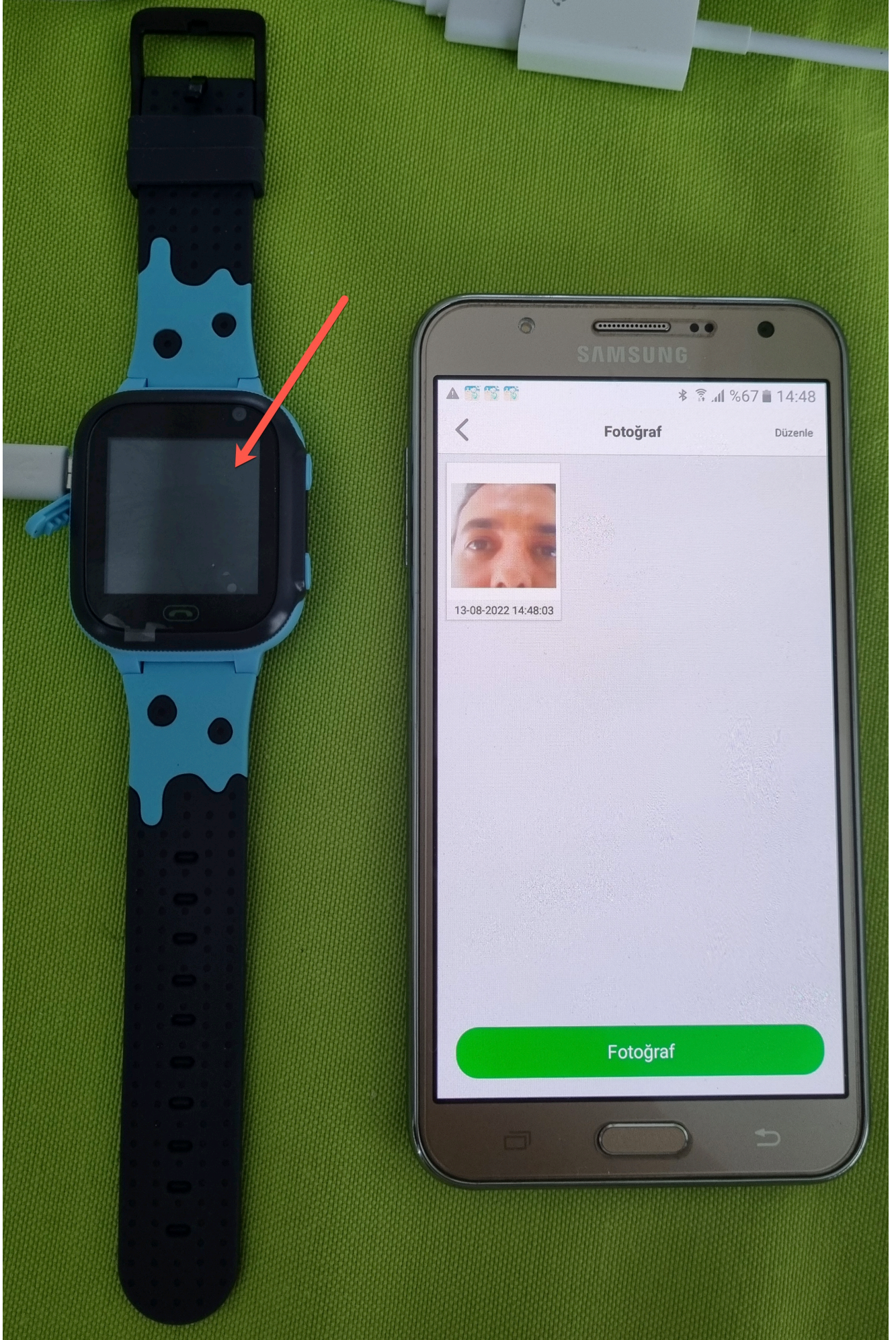




The first thing that caught my attention in the app was the ability to track the watch on a map in real-time, followed by the Tracking Number and Remote Camera menu steps. The Remote Camera menu allows you to take photos with the watch's camera at any time. The watch does not produce any visual or auditory alerts at this time. The Tracking Number menu allows you to make the watch call the entered phone number, and audio surveillance can also be performed using the watch's microphone. Again, as in the Remote Camera step, the phone does not provide any alert that surveillance is being performed.







“Oh, how wonderful, we can track and listen to our child in real-time,” you might think. But let’s suppose that the email address you used to log in to the SeTracker2 app, and the password you could not strengthen by using special characters, was stolen or guessed by malicious people for a moment. A malicious person could violate your privacy and secrecy of your private life by accessing the app through the watch on your child’s arm and tracking their location in real-time, taking their photo, sending messages, deleting the sent message without leaving a trace, and making the watch call the phone number specified to perform ambient listening. In addition, let me emphasize that there is no chance of accessing the log of all these operations performed by a malicious person through the SeTracker2 app!

“I am very careful and cautious and don’t easily fall into the hands of scammers,” you might say. But if you use the same password for multiple websites during login, one of those websites may have already been hacked, and your username/email and password may have been obtained. If you do not use Multi-factor Authentication (MFA) (the SeTracker2 app does not support MFA!), remember that malicious people can easily log into websites and mobile applications (such as the SeTracker2 app) where your account is with the information obtained!

Multi-factor authentication (MFA; encompassing two-factor authentication, or 2FA, along with similar terms) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects user data—which may include personal identification or financial assets—from being accessed by an unauthorized third party that may have been able to discover, for example, a single password.

Another important issue is that you may inadvertently commit a crime through your child using watches with audio surveillance feature.

I hope that those familiar with my security research, especially my blog post titled Run Mert Run expect to see in this article how the vulnerabilities I identified through reverse engineering, static and dynamic code analysis of the SeTracker2 application can be exploited, or how a hardware vulnerability I discovered can turn the watch into a spy device. After all this, I believe that I can clearly convey that these watches, through the SeTracker2

application, invite malicious individuals to use them for nefarious purposes and pose a significant danger to parents and children. :) Still, anybody who wants to learn more about the application's technical aspects can take a look [here](#) and [here](#) for studies that were conducted in previous years.

I hope that, like the example set by the decision taken by Germany in 2017, our authorities will also take a similar decision and ban the sale of these potential spy devices that look like watches on shopping websites, thus bringing an essential step towards protecting parents and children from such dangers.

In light of this information, I strongly recommend that those who use smart children's watches that can record their surroundings use them with awareness of the risks. Please share this article with other parents, friends, and loved ones to create awareness.

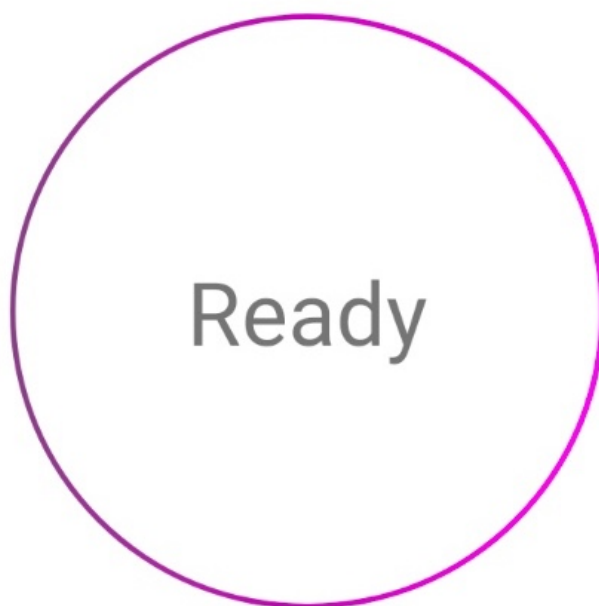
Hope to see you in the following articles.

Note: For my technical readers, I would like to share that the SSL Pinning method is used in the SeTracker2 application, and through the use of a simple Android application called PCAPdroid, it is possible to record and analyze HTTPS traffic. This can be done quickly by recording the traffic and then analyzing it using the Wireshark tool.



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



PCAPdroid_15_Aug_08_10_30.pcap

ip.dst == 54.169.10.136 and http

No.	Time	Source	Destination	Protocol	Length	Info
31	2022-08-15 05:10:42.640911	10.215.173.1	54.169.10.136	HTTP	529	GET /app/public/S10APP/v2_getNoticeInfo?language=enUS×tamp=1660540243000
78	2022-08-15 05:10:44.155382	10.215.173.1	54.169.10.136	HTTP	750	POST /app/public/S10APP/v2_new_userLogin2 HTTP/1.1 (application/x-www-form-urlencoded)
171	2022-08-15 05:10:45.354494	10.215.173.1	54.169.10.136	HTTP	645	GET /app/u9103038.580153.M80QE08UFP68I5749SDRSJ2I8JVFVH1L1666
181	2022-08-15 05:10:45.426324	10.215.173.1	54.169.10.136	HTTP	645	GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1666
189	2022-08-15 05:10:45.433760	10.215.173.1	54.169.10.136	HTTP	634	GET /app/u9103038.580153.M80QE08UFP68I5749SDRSJ2I8JVFVH1L1666
267	2022-08-15 05:10:46.002569	10.215.173.1	54.169.10.136	HTTP	575	GET /app/public/S10APP/v2_findAdInfo_new?language=enUS&flag=1
269	2022-08-15 05:10:46.015562	10.215.173.1	54.169.10.136	HTTP	660	POST /push/msg/bindUser HTTP/1.1 (application/x-www-form-urlencoded)
419	2022-08-15 05:10:47.813877	10.215.173.1	54.169.10.136	HTTP	587	GET /app/public/S10APP/v2_new_findUserDeviceInfo?language=enUS
420	2022-08-15 05:10:47.813892	10.215.173.1	54.169.10.136	HTTP	587	GET /app/public/S10APP/v2_new_findUserDeviceInfo?language=enUS
423	2022-08-15 05:10:47.814177	10.215.173.1	54.169.10.136	HTTP	633	GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1666
424	2022-08-15 05:10:47.814181	10.215.173.1	54.169.10.136	HTTP	677	GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1666
427	2022-08-15 05:10:47.815374	10.215.173.1	54.169.10.136	HTTP	638	GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1666
456	2022-08-15 05:10:48.750561	10.215.173.1	54.169.10.136	HTTP	689	GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1666
473	2022-08-15 05:10:48.987693	10.215.173.1	54.169.10.136	HTTP	608	POST /S10APP/findFaceAuthInfo HTTP/1.1 (application/x-www-form-urlencoded)
536	2022-08-15 05:10:51.566225	10.215.173.1	54.169.10.136	HTTP	719	GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1666

File Data: 299 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "language" = "enUS"
- Form item: "appid" = "aaagg10006"
- Form item: "password" = "5f7b2e730cbbc2ca4928cfc0a19f249320e65fefbd6830299e924b0942745b7"
- Form item: "loginname" = "mert.sarica@gmail.com"
- Form item: "flag" = "70"
- Form item: "version" = "2.8.6"
- Form item: "isIPHONE" = "1"
- Form item: "timestamp" = "1660540243000"

Frame (750 bytes) | Decrypted TLS (688 bytes)

0066pass word=5f7b2e730cbbc2ca49428cfc0a19f249320e65fefbd6830299e

Text item (text), 74 bytes

Packets: 809 · Displayed: 15 (1.9%)

Profile: Default

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

locuk Saati/pcap_dump_tls/sskeylogfile_1508.txt Browse...

Cancel OK