

Analyzing Prominent Apps in Latin America

Overview

With the help of leaders at SocialTIC, a non-profit digital rights organization based in Mexico City, we identified 8 popular mobile apps that are relied on by hundreds of millions of users in the region everyday. Each of the apps chosen fall into one of three categories: telco app, government-developed app, or a marketplace app. We chose these particular apps since users in the region are often incentivized through promotions, access to government services, and usability to download these apps and keep them installed on their personal device. For example, three of the four telco apps that we analyzed offer data package incentives to customers who download and login to their mobile app from their device. Since millions of users need to have these apps installed on their personal device, we wanted to investigate the security and privacy states of the apps to ensure the users are not susceptible to the same threats.

The apps we chose to analyze are relied on for vital services including cellular service, emergency response, healthcare, money transfers, and more. We used reverse engineering techniques, including both static and dynamic analysis, to inspect if there were any major security issues or privacy concerns. A further breakdown of what each app's main functionality is detailed below in the App Breakdown section, as well as the main threats we are looking for in the Threat Breakdown section.

- Telco apps: MiTelcel, MiClaro, MiMovistar, MiTigo
- Gov-developed apps: IMSS Digital, SAT Movil, MiPolicia
- Marketplace apps: Mercado Libre, Chivo Wallet

<i>App Name</i>	<i>Developer</i>	<i>Use</i>	<i>Popularity</i>
MiTelcel	America Movil (telco)	manage your Telcel cellular plan (Mexico)	holds 62% market share of mobile subscribers in Mexico as of 2022
MiClaro	America Movil (telco)	manage your Claro cellular plan from 7 different countries	largest provider in Latin America, holds 61% market share of wireless subscribers in Brazil
MiTigo	Millicom International (telco)	manage your Tigo cellular plan from 8 different countries	largest mobile provider in Paraguay and Honduras with over 60% market share in each
MiMovistar	Telefonica (telco)	manage your Movistar cellular plan from 8 different countries	second largest mobile provider in both Mexico and Paraguay
SAT Móvil	Government of Mexico	access services available in a personalized space for	only official mobile app for Mexican citizens to access

		taxpayers through their RFC and Password	their tax documents
IMSS Digital	Government of Mexico	schedule medical appointments and view health records	only official app of the Mexican Social Security Institute
MiPolicía	Government of Mexico	get in emergency contact with the closest police "quadrant" near Mexico City	over 1 million downloads in the Google Play Store
Chivo Wallet	Government of El Salvador	official Bitcoin wallet app of the El Salvadoran government to exchange BTC and USD	researchers found around 33% of the population installed the app primarily for the 30\$ BTC incentive
Mercado Libre	Mercado Libre	e-commerce platform similar to eBay or Amazon	the largest e-commerce platform in Latin America with market share over 50%

Key Findings

We found issues belonging to each of the three threat classes discussed in the Threat Breakdown section amongst the 8 apps we analyzed. We sent two vulnerability disclosures to app developers for consistently using cleartext HTTP elements in main components of their apps. We found instances of telco and marketplace apps leaking user’s personal information to third-party servers in violation of their privacy policies. We also found an app that is able to use dynamic code loading (DCL) to retrieve updates to the source code of the app, outside of the typical app store update mechanisms. Specifically:

- The MiTelcel app consistently fetches three images and JSON files for the splash configuration over cleartext HTTP.
- The SAT Movil app uses cleartext HTTP for the “Chat” page that is responsible for communicating highly sensitive personal info including citizen ID numbers and passwords.
- The MiTelcel app sends POST requests to five different third party servers with personal info of the user including their email and phone number.
- The ChivoWallet app checks with Microsoft CodePush servers each time it is opened to see if there is a new update available to fetch.
- Three of the four telcos send SMS messages that include external links that are vulnerable to SSL strip attacks.

Motivation

The security of mobile apps throughout the region is important because Mexico has a long history of using state resources to influence the media and flow of information throughout the area. Political leaders across all parties use hundreds of millions of dollars in state money to

advertise and in some cases even bribe specific media outlets or journalists across the region according to [Fundar](#), an independent transparency group in Mexico. This results in a media environment in the region that allows federal and state officials to control the news and dictate what outlets should and should not cover. According to a [New York Times article](#) where a variety of journalists, reporters, and executives were surveyed, two-thirds of Mexican journalists admit to censoring themselves to avoid these issues. Most news outlets in the region are dependent on the massive government advertising spending to support operations. According to the same report, some government press secretaries will openly demand positive press coverage from specific local news organizations before signing a new advertising contract. The result is a news and media landscape across the region where federal and state officials dictate the news, telling the outlets what they can and cannot report on.

Both at the federal and state level, there have been multiple documented cases of targeted cyber attacks and surveillance against journalists and activists in the past decade. The Mexican digital rights group R3D (Red en los Defensa de los Derechos Digitales) released a [report](#) that identified [Pegasus malware infections](#) on journalist and human rights defenders's devices that took place between 2019-2022. An opposition political party candidate, Agustín Basave Alaní, was also one of those infected with the malware in 2021. This occurred after Mexico's current President told the public that the government would no longer use the spyware and there would be no further abuses. Recently, there have been reports of mass surveillance being conducted on citizens throughout the region. In 2020, The Citizen Lab published a [report](#) about the Mexican Navy and the city of Durango's use of the cyberespionage company Circles in order to conduct mass surveillance of the local population that connected to their deployed endpoints. There have also been [reports](#) in *Forbes Mexico* on the purchase of a NeoLinx license that included over 130,000 phone's geolocations.

Recently, drug cartels in the region have begun to use advanced cyber attacks and operations to further their business interests. According to a report from the Guardian, corrupt officials in Mexico have helped cartels and other organized criminal groups get access to state-of-the-art spyware (Pegasus and many others) that can be used to hack and eavesdrop on mobile devices. As many as [25 different private companies](#), including the NSO Group in Israel and Hacking Team in Italy, have sold surveillance software to Mexican federal and state police forces. Some of the regional and state police forces that have officially purchased spyware are accused of colluding with the criminal groups they are supposed to be confronting with the tools and selling it to them to use against their adversaries.

The combination of targeted cyber attacks from both criminal and state forces has caused a wave of violence that has now made Mexico the most dangerous country for journalists in the world, outside of war [zones](#). At least 119 media workers have been killed in the country since the turn of the century, according to the Committee to Protect Journalists. Reporters in the area fear that as the prevalence of these target cyber attacks grows, it will only lead to more journalists and activists being targeted. It is vital that users are not exposed to vulnerable applications that make it simple to target their personal devices as state officials, police forces, and criminal groups become more sophisticated cyber threats in the region.

Threat Breakdown

There are three main security / privacy threat classes we assess each app in our list for:

1. Weak network security - using cleartext traffic or weak encryption schemes or implementations
2. Leaked PII (personally identifiable information) - sending user's personal information off device without explicitly stating so in the privacy policy or user agreement
3. External update - ability to update the app's functionality outside the trusted app store update mechanisms

The first threat, weak network security, would allow a local or in-path adversary to eavesdrop or modify network traffic and potentially change the behavior of the app. This would include an app using cleartext (unencrypted) traffic, such as HTTP, to communicate with application servers and third-party services. This threat would also imply that any upstream, in-path router that is forwarding the user's traffic, often controlled by the ISP the user is connected to, is able to take advantage of the weakness in the app's network security as well.

The second threat we evaluated each app for is the leaking of personally identifiable information. This is when info can be used to confirm a person's identity such as an individual's phone number, email, etc. is sent off-device to a server that is not owned by the app developers. Most apps include multiple third-party services in the background for utilities such as payments, analytics, mobile engagement, serving ads, app health monitoring, and more. These third-parties should not be receiving personal info on individual users unless it is explicitly made known through the privacy policy, app store description, or user agreement. We consider an app to leak PII if any case of personal info is captured in our dynamic analysis being sent to a third-party server and the app is not clear that the data is being shared.

The third threat is the ability to conduct external updates to the APK outside of the Google Play Store or iOS App Store. Each update that is pushed to these official app stores will be reviewed by a trusted team that is responsible for making sure there are no security or privacy issues in the new app version. If an app is able to update its own behavior and code without going through this app store verification, then we consider this a serious threat to the user. For example, the app could update to a version that tracks and posts the location of the user, without the device owner ever knowing. Furthermore, an app with this capability could target specific users with updates without them being aware of the changes that other users did not receive.

In 2018, the ACLU released an advisory [report](#) that warns software developers that "government agents may try to force you to create or install malicious software in products to help them with surveillance." The report warns that as companies and apps embrace encryption, government demands may continue to increase to find new ways to implement

surveillance. The report discusses how law enforcement may try to compel developers to install malicious code in the update through a court order. Additionally, in some jurisdictions if they are worried the developers will protest, then they may include a gag order that stops the developers from telling anyone what they have been compelled to [add](#).

There have been multiple prominent cases of apps using malicious updates to alter their behavior and take advantage of users. In 2021, a barcode scanning [app](#) with over 10 millions installs was transformed into a “malvertising” app that pushed advertising to victim devices. In March 2023, the app Pinduoduo, one of China’s most popular e-commerce platforms with over 900 million monthly active users, was suspended for security concerns from the Google Play Store for including malware in the source code. According to [researchers](#) at Ars Technica, the app was exploiting a zero-day vulnerability in Android which allowed the app to perform privilege escalation in order to gain market share by stealing [user data from its competitors](#).

In the August 2023 Threat Horizons [Report](#), the Google Cybersecurity Action Team (GCAT) discussed threat actors using a technique they called “versioning” to evade Google Play Store’s malware detection. In this method, the developer releases an initial version of the app that passes Google’s pre-publication checks, but then later through dynamic code loading (DCL) the app is updated from an attacker-controlled server to include malicious functionality. In May of 2023, [ESET](#) research found a screen recorder app, “iRecorder - Screen Recorder”, that remained undetected on the Play Store for over a year after it received a malicious DCL update that allowed the app to spy on its users.

Telco Background

In 2013, América Móvil, who owns both Telcel and Telmex, held 75% of the Mexican telecommunications market, which led the government to lead major antitrust reforms and the establishment of a telecommunications regulator (IFT). As of 2020, the Mexico City based América Móvil still holds over 70% of the telco market share in the country with its two biggest entities, Telmex and Telcel. The Mexican government was the sole owner of Telmex from 1972 until 1991 when they sold all remaining shares. Based on recent transparency data, it appears the state and the company are still closely allied. According to the telecommunications regulator (IFT) from 2016-2017 Telmex and Telcel, both owned by the same parent company América Móvil, surrendered data 100% of the time that authorities requested as documented in [Privacy International](#). Soon after this information was released, the IFT removed the transparency obligations that were detailed in the Guidelines for Collaboration on Security and Justice Matters which obligated telcos to report on user data requests made by authorities every 6 months. Additionally, 30% of such requests were made by unidentified authorities or authorities that did not have a legal right to the user data requests.

Within Mexico, the telephony market is dominated by the American Movil owned brand Telcel. According to [Statista](#), as of 2022 Telcel accounted for approximately 76% of the market share, followed significantly behind by AT&T and Movistar, each controlling around 10% of the market in the country. However, throughout the rest of Latin America, the telephony market share within

each country varies significantly. American Movil's brand that operates outside of Mexico, Claro, also controls the largest chunk of the Latin American market with about 43% share as of 2022 revenue [statistics](#). They are followed by Tigo's owner, Millicom, with control of 19% and Movistar's parent company, Telefonica, with just 5% of the market. We chose to analyze and compare the top four most popular cellular management apps who's primary customer base is within Latin America. This includes both brands American Movil operates under, Telcel and Claro, along with the Movistar and Tigo applications.

MiTelcel: <https://play.google.com/store/apps/details?id=com.speedymovil.wire>

MiClaro (Colombia): <https://play.google.com/store/apps/details?id=com.clarocolombia.miclaro>

MovistarMx (Mexico): <https://play.google.com/store/apps/details?id=com.movistarmx.mx.app>

MiTigo (El Salvador):

<https://play.google.com/store/apps/details?id=com.juvmobileinc.tigoshop.sv>

App Breakdown

Telco Apps - MiTelcel, MiClaro, MiMovistar, MiTigo

The first set of apps analyzed in this project were the client apps for the main telco operators throughout the Latin American region: Telcel, Claro, Movistar, and Tigo. America Movil's in-country network provider, Telcel, is only available within Mexico so there is only one version of the "MiTelcel" app. On the other hand, Telcel's sister provider, Claro, has 7 different mobile apps available on the Google Play Store that target each of the different countries it operates in. This includes "MiClaro Brazil", "MiClaro Argentina", "MiClaro Peru", and more. The MiMovistar apps are similar to Claro in that it has 8 different apps depending on the country the user is accessing the network from. Each of the versions is named "MiMovistar" with the country name following besides the "MovistarMx" and "Movistar Venezuela" versions. MiTigo has 8 different versions of the app targeting different countries, but as we will discuss in more detail in the findings section, they are almost identical to one another outside the country code used in the package name for each.

The main functionality of each of the telco apps is for users to be able to manage their personal cellular plans from their mobile device. This includes topping up the plan, managing members on the plan, and paying bills. Most of the applications also offer extra data packages that can be added in the app such as a 3GB per month plan or unlimited data plan. Each app has a registration and login where users must enter their personal phone number from the given telco and their password in order to sign up and login to manage their account. The apps and or cellular provider will often send SMS messages to the device with promotions and 2FA codes when logging in.

Government apps - IMSS Digital, SAT Movil, MiPolicia

The second set of apps we selected to analyze are widely used apps developed by the federal government in Mexico. They each have application endpoints and package names that end with “gob.mx” which is the official platform of the Government of Mexico (Gobierno de Mexico).

IMSS is the Mexican Institute of Social Security which is a government organization that assists public health, pensions and social security in Mexico operating under the Secretariat of Health. It forms an integral part of the Mexican healthcare system. According to the official “imss.gob.mx” site, the IMSS Digital app is a “strategy to evolve the IMSS and adapt it to the new reality of digital services, through a new model of attention, with the implementation of modern channels.” It allows users to schedule medical services including family medicine appointments, discharge or change clinic, disability registration, get proof of non-entitlement, get Covid permits, and more all by registering with the user’s CURP (Unique Population Registry Code) and email address. The app has over 10 million downloads on the Google Play Store and a user rating of 4.5 out of 5.

The SAT Movil app is the latest app from the Tax Administration Service in Mexico ([Servicio de Administración Tributaria](#)). According to the Google Play Store description, it offers personalized digital services for taxpayers along with “the consultation of documents with greater demand in the attention office: Taxpayer ID card, Evidence of Fiscal Situation, and Certificates of signature and active digital seals.” Each user must login with their RFC (Mexican Tax Identification Number) and password to access their personal management portal. The tax management app has over 1 million downloads through the Play Store.

MiPolicía is a civil security app that is used primarily within Mexico City to contact police services for emergencies. The main purpose of MiPolicía is to be able to notify police from the nearest of the 126 police “quadrants” in the city while also sharing location from the device when doing so that the responders will have access to. The home page of the app has an interactive map of the local area with locations of major police stations and landmarks. A user can trigger the large, red “Emergencia” button at the bottom of the screen to begin sharing location with the nearest police quadrant to respond to. The official emergency app from the Mexico City Police has over 1 million downloads and a Play Store rating of 4.1 out of 5.

IMSS Digital: <https://play.google.com/store/apps/details?id=st.android.imsspublico>

SAT Movil: <https://play.google.com/store/apps/details?id=mx.gob.sat>

MiPolicia: <https://play.google.com/store/apps/details?id=com.moobky.MiPolicia>

Marketplace Apps - Chivo Wallet, MercadoLibre

The Chivo Wallet app is the official Bitcoin and US dollar wallet of the Government of El Salvador. It enables citizens to send and or receive Bitcoin and US dollar payments through the mobile app. It also allows users to easily convert between BTC and USD and withdraw and deposit funds in the application. We chose this app to analyze because many citizens in the country are compelled to use it since it is the official wallet app from the government that was

being heavily pushed by government officials during its rollout in September 2021. This made the country the first in the world to make [Bitcoin legal tender](#). According to the report by RestOfWorld in 2022, around half of Salvadorans surveyed have installed Chivo Wallet. The app even offered a Bitcoin “bonus” to incentivize new users to sign up to claim their free funds. There have been serious security issues with the app including [reports](#) that many Salvadorans have had their identities used by hackers to create new accounts in the app under their name and DUI ID number. The app has over 1 million downloads from the Google Play Store and a rating of 3.1 out of 5.

Mercado Libre is the leading e-commerce platform in Latin America with a mobile app that has over 100 million downloads on the Google Play Store. The app has similar functionality to eBay or Shopee, but it is geared towards customers throughout Latin America. It is a pure-play online marketplace, meaning they do not sell any products themselves. The platform operates in 18 countries and receives over 668 million visits per month. As soon as the app or main page to the website is opened, a user can choose from a list of each country within Central and South America to continue in. Each user has the ability to register an account in any of these countries in order to purchase or sell products. Since MercadoLibre is the largest ecommerce and payments ecosystem in Latin America, millions of users rely on the app being safe to use from a security and privacy perspective every day.

Chivo Wallet: <https://play.google.com/store/apps/details?id=com.chivo.wallet>

Mercado Libre: <https://play.google.com/store/apps/details?id=com.mercadolibre>

Findings

Telco Apps - MiTelcel, MiClaro, MiMovistar, MiTigo

The Claro, Movistar, and Tigo apps each have multiple different versions depending on the country the app is targeting. For example, there are eight different Movistar apps available in the Google Play Store that include MiMovistar Argentina, MiMovistar Ecuador, MovistarMX, and more. We found that the eight different Tigo apps’ source code are almost identical to one another outside of the country code used for the domain in the manifest file. For Claro and Movistar, on the other hand, we found the permissions used, third-party services included, and background receivers vary significantly depending on which country the app is made for. As an example, the MiMovistar Argentina app requests access to all phone call related permissions while the MiMovistar Uruguay app does not. Next, we list each of the main findings from the telco apps and then discuss them in more detail below.

Security / Privacy Issues Found

MiTelcel cleartext	Cleartext (HTTP) traffic consistently used for main page of the app to load multiple images and JSON files
--------------------	--

MiTelcel PII leak	The app will post to five different third-parties with PII of the user including their name, email, and phone number in the HTTP “referer” field
MiTelcel, MiTigo, MiClaro, MiMovistar	Telcos will send SMS messages to device with external links that are vulnerable to SSL strip attacks
MiClaro Colombia	Will POST fine location info from the device before users accept permission prompt

Table 1: Summary of issues found in the telco apps that we analyzed.

In the telco apps we found examples of two of our three main threat classes we examined each app for. The MiTelcel app, with over 10 million downloads, is vulnerable to both the weak network security and PII leak threats. The app will send consistent cleartext HTTP requests to download images shown right on the main page of the app that could allow an in-path attacker to inject their own image to possibly trick the user into following malicious directions such as going to a malicious change password link. An example of this image injection in the real app (March 2023 release) is shown in figure 1 below.

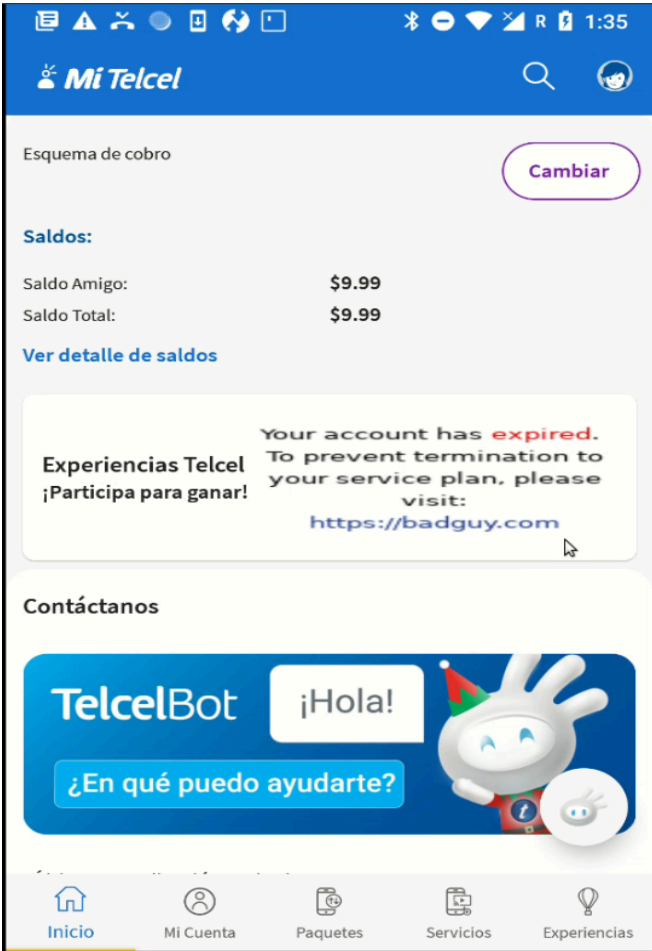
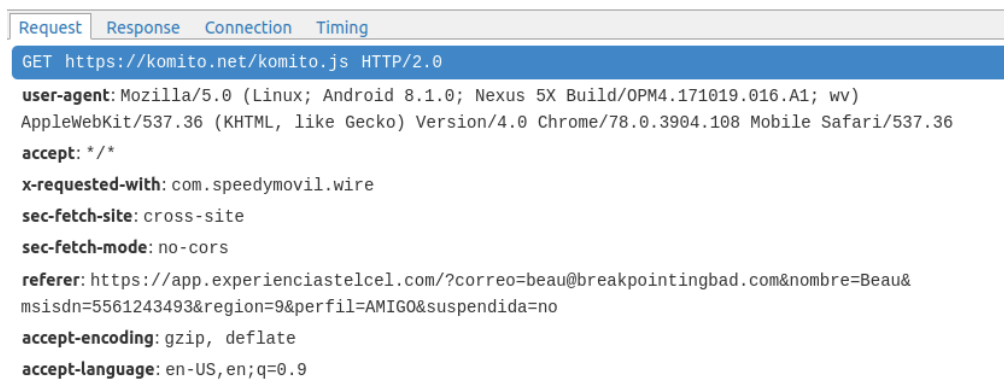


Figure 1: Fake attacker image being injected and shown on the MiTelcel homescreen.

Furthermore, all four of the telcos we tested sent SMS messages directly to the mobile device that included external links that were not secured with HTTPS. Generally, if the user clicks these links, the server will respond with a 301 redirect message to the secured TLS (formerly SSL) web address. However, if there is an in-path attacker present using an [SSL strip attack](#) they could downgrade the connection to cleartext HTTP and eavesdrop on the contents of each packet. These connections may include highly sensitive info including the user's number, password, and payment information if they are topping up the plan or logging into their cellular account.

We also captured MiTelcel sending POST requests to five different third-party services where PII, the user's phone number and email, was leaked in the "referer" HTTP field. An example of this issue is shown in Figure 2 below. These requests were sent out each time a user in the app clicked the "Experiencias" tab in the bottom corner of the main toolbar. In our dynamic analysis of the "MiClaro Colombia" app, we captured the application sending fine location information of the latitude and longitude of the device before the privacy prompt was accepted by the user. We also consider this to be a leak of PII since the user has not agreed to supplying the information being sent out.



```
Request  Response  Connection  Timing
GET https://komito.net/komito.js HTTP/2.0
user-agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X Build/OPM4.171019.016.A1; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/78.0.3904.108 Mobile Safari/537.36
accept: */*
x-requested-with: com.speedymovil.wire
sec-fetch-site: cross-site
sec-fetch-mode: no-cors
referer: https://app.experienciastelcel.com/?correo=beau@breakpointingbad.com&nombre=Beau&msisdn=5561243493&region=9&perfil=AMIGO&suspendida=no
accept-encoding: gzip, deflate
accept-language: en-US,en;q=0.9
```

Figure 2: mitmproxy capture of one of the five GET requests being sent to a third party server from the MiTelcel app that includes my PII in the "referer" field URL. This request is triggered by clicking the "Experiencias" tab at the bottom right of the app.

We found a couple low-hanging security issues that could be addressed by the telco apps including the cleartext traffic used in MiTelcel and the predictable web links sent to each device that an in-path attacker could SSL strip. An official security disclosure with demos of the issue was sent to the MiTelcel developers in March of 2023. Additionally, there were privacy concerns found in some of the telco apps including the sharing of PII with multiple third parties (MiTelcel and MovistarMx) and fine location being leaked before permission was granted (MiClaro Colombia). The Tigo apps were the least invasive in terms of the permissions requested from each user, third parties it communicates with, and the fact that the source is practically identical for each country it operates in.

Government apps - IMSS Digital, SAT Movil, MiPolicia

Amongst the three government apps we analyzed, there were far less security and privacy issues that stood out compared to the telco apps. One reason for this is that the telco apps each have multiple third party services included for various functionalities such as geofencing, mobile marketing, analytics, user engagement, and more. The government apps are not trying to maximize engagement and revenue the same way, and do not include practically any third-party receivers or services in the apps besides very standard services like the ability to communicate with Firebase databases.

Security / Privacy Issues Found:

SAT Movil cleartext	Cleartext (HTTP) traffic consistently used for the “Chat” page of the app that handles extremely sensitive data including ID numbers, passwords, and other personal info
IMSS Digital (requires “system”/root access so not vulnerability)	Holds clear text file in app folder on device with every piece of personal info collected by the app including medical diagnosis, ID numbers, health appointments, and more

Table 2: Summary of issues found in the government-developed apps that we analyzed.

In the government apps we found only one of our three main threat classes we looked for. The SAT Movil app consistently uses weak network security and fetches components in the app over cleartext HTTP. The “Chat” page specifically within the app is always fetched over HTTP which is a serious issue for users of the app because there is very sensitive information being exchanged on the page. The “Chat” dropdown in the app allows users to select between multiple options including “Declaración Anual Personas Físicas” (annual declaration natural persons), “Cedula de Identificación Fiscal” (Taxpayer identification card), and “Solicitud de datos del RFC de trabajadores” (Request for data from the RFC of workers), “Tramites Fiscales” (Fiscal procedures), and a few more. Once an option is selected, the user will often be redirected to another page requesting a variety of sensitive personal information that may include their CURP number, RFC, email, name, address, and often password. A security disclosure with demos of the issue was sent to the SAT Movil developers in July of 2023.

An in-path attacker could use the well-known SSL strip techniques to downgrade the entirety of the connection to the “chat.gob.mx” to cleartext HTTP. This would allow the attacker to eavesdrop on all the info being sent over this connection which will most likely include personal details that could be used to steal the victim’s identity or hijack their personal tax account. A demo of how simple this vulnerability is to take advantage of is shown in Figure 3 and 4 below. A full video of the attack in action is shown in the link beneath the image. An official disclosure was sent to the developers of SAT Movil with information on the vulnerability and how to address it.

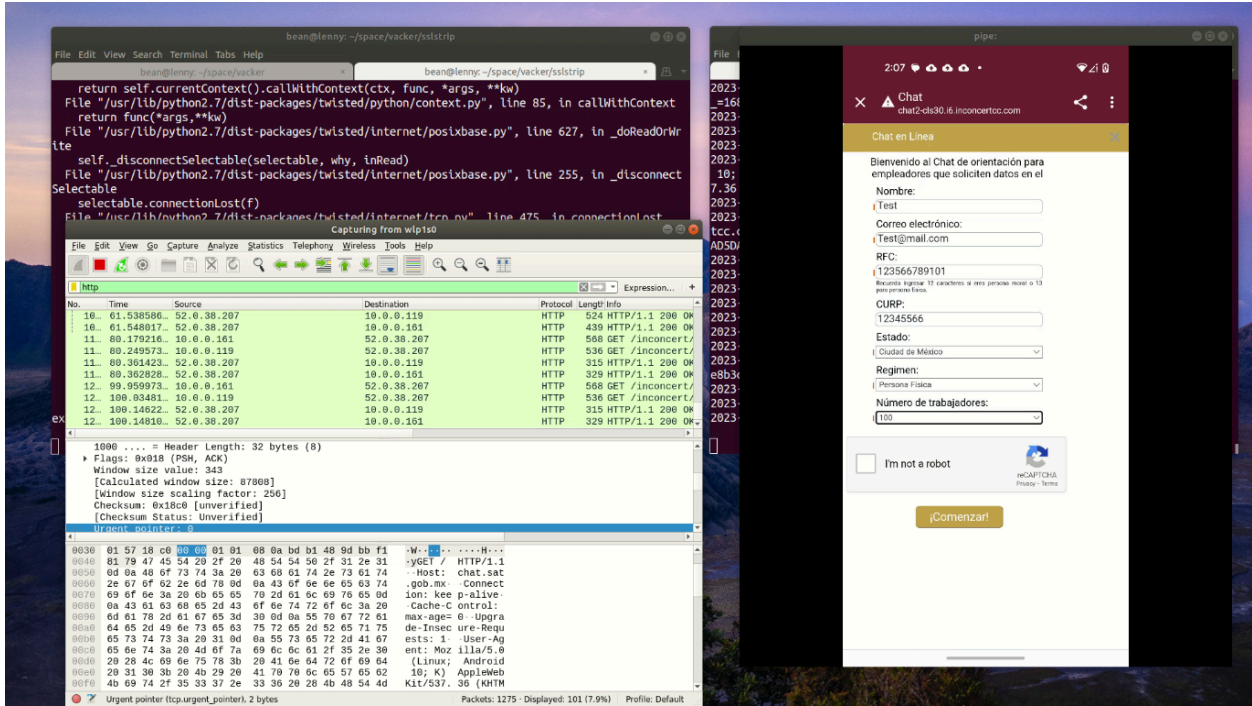


Figure 3: Screenshot of one of the chat pages being opened and personal info being input into the page during an sslstrip attack.

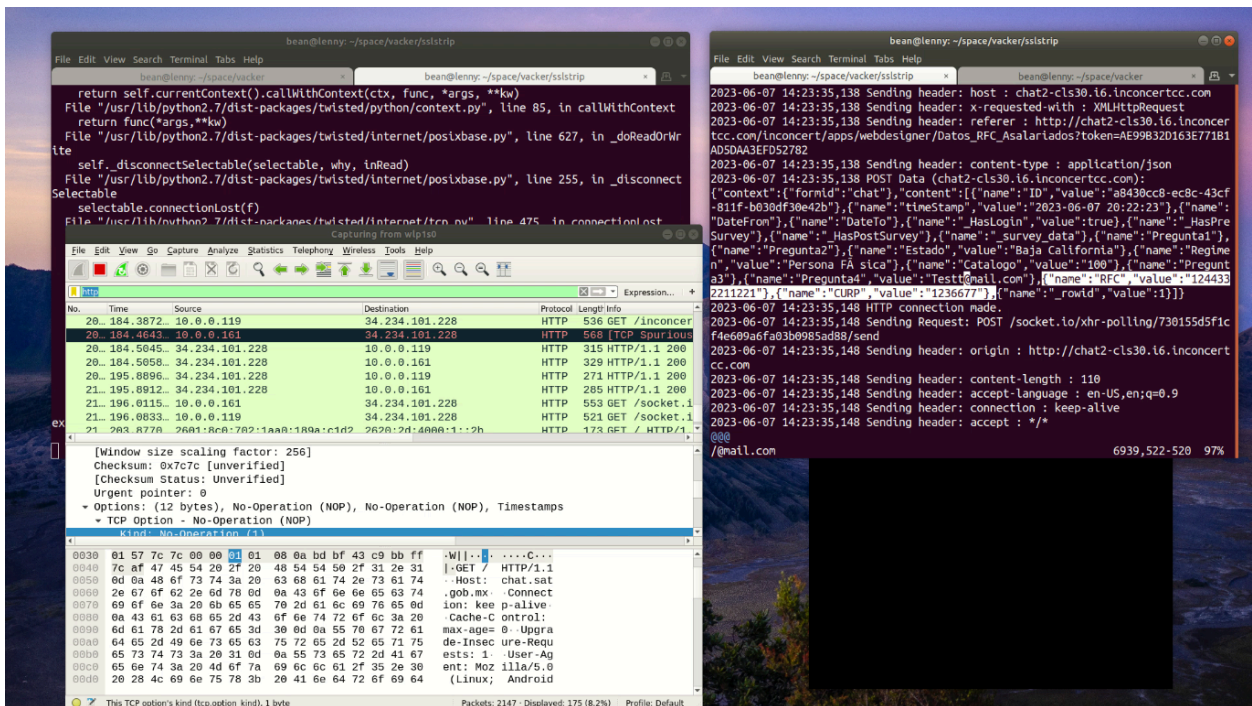


Figure 4: Screenshot of the result of sslstrip being used on SAT Movil's network communications; on the left, sensitive information is shown in the clear in Wireshark, on the right, sensitive information is outputted in the attacker's console.

Demo video for SAT Movil SSL strip on “Chat” page:

<https://drive.google.com/file/d/1WwqxQQ0mKKJYkOTSSGOXchVJobioMUhL/view?usp=sharing>

The IMSS Digital app keeps an unencrypted file on the mobile device with every piece of personal info the app can collect including the user’s ID numbers, medical history and diagnosis, birth history, and more. This file is stored inside the app folder on the device that requires system permissions to access so we do not consider this a security issue. As long as the user does not have a rooted device, an attacker could not access the file unless they were to gain system permissions themselves. The app does not include any third-party background services besides some Firebase services that allow the apps to receive push notifications on medical appointments that were scheduled through the app.

The MiPolicia app does not include any permissions that could be considered potentially “dangerous” besides access to fine and background location, along with the ability to call. These three permissions are all used in the main functionality of the app where a user can trigger an “Emergencia” in the app which will make an outgoing call to the nearest Quadrant police station. At this time the app will begin sharing the background location and fine location of the device with application servers that can be accessed by the Quadrant police station that was called. There were no significant security or privacy issues found in the emergency police app.

Marketplace Apps - Chivo Wallet, MercadoLibre

We did not find any network security issues in the two marketplace apps that we analyzed. The apps follow best security practices and do not permit any cleartext traffic being used in the apps using high level Android APIs. Mercado Libre uses three third-party services in the background including Braze for customer engagement, AppAdjust for analytics, and Bitmovin for playing videos in app. Chivo Wallet, on the other hand, only includes background services that allow it to communicate with Huawei Mobile Services (HMS) and Firebase messaging services to communicate with the app built with React Native.

Security / Privacy Issues Found:

Chivo Wallet external update	Includes Microsoft CodePush service that could allow for external updates to the app
Chivo Wallet activity leak	will POST to a NewRelic analytics server with in-app event details that will include the exact info each user types such as their ID number, phone number, and password.
Mercado Libre activity leak	sends POST requests to three different third-parties (TikTok, Facebook and Google) with information on each product that is clicked in the app

Table 3: Summary of security/privacy issues found in the marketplace apps that we analyzed.

Each time the Chivo Wallet app is opened it will make a request to “codepush.appcenter.ms/b0.1/public/codepush/update_check?...” which is responsible for telling the app whether there is a new deployed version of the app that it should update to through Microsoft’s CodePush service. According to the official [GitHub](#) for CodePush, it is “a cloud service that enables Cordova and React Native developers to deploy mobile app updates directly to their users' devices. It works by acting as a central repository that developers can publish updates to (JS, HTML, CSS and images), and that apps can query for updates from.” This functionality allows the Chivo Wallet developers (government of El Salvador) to push arbitrary updates to the apps without having to first go through the Google Play Store or Apple Store update process.

The Chivo Wallet app makes consistent POST requests to NewRelic servers, a popular US based web tracking and analytics company. It allows mobile apps to track user interactions and the performance of the app. The Chivo app will post logs of every event that happens in the app to an endpoint at “log-api.newrelic.com.” This includes in-app events from a user clicking a new page to them typing in their ID number. This event-based information is all sent to the NewRelic servers with the body of the POST containing data on the event which may include the user’s personal information such as their DUI number that was typed into the text box on the registration page. Although these NewRelic logs should be managed by developers from Chivo Wallet, it is not made clear in the privacy policy that this is taking place in the background.

The MercadoLibre app will make three different POST requests to third-party servers each time a user clicks a product in the app. There will be information on the name of the item and the URL it is located at sent to TikTok analytics, Google analytics, and Facebook servers every time an item is visited. This behavior is not uncommon amongst similar apps. The Amazon Shopping app, for example, indicated in the “Data Safety” section on Google Play Store that the app will share “App activity” with various third parties. However, the MercadoLibre app’s Data Safety section does not make this behavior clear and it is not mentioned in the detailed privacy policy for the app. Therefore, we consider the app to leak personal behavior information that is most likely used to show more relevant products and ads on those third-party platforms. The information being sent is likely not personal identifiable information unless ML models were able to consistently predict which person is most likely to access a set of products.

Reverse Engineering Environment

One of the main objectives of this project was to create a starting point repository for anyone with an APK they wanted to reverse engineer and analyze. The instructions to set up and deploy a reverse engineering environment that includes all of the primary tools used for both static and dynamic analysis in this project is attached at the [Github link](#). The repo includes instructions on how to set up a dynamic analysis environment with “mitmproxy” being used to capture and decrypt HTTPS traffic from a live mobile device. There are details on how to set up Frida, a dynamic code instrumentation toolkit, to be able to hook live function calls and inject

custom Javascript into mobile apps. In the main README there are instructions on how to use Frida and mitmproxy together to bypass an app that uses SSL pinning and view the decrypted traffic from the app.

The repo also includes instructions for setting up the main static analysis tools that were used during this project as well. There are bash scripts that will install Jadx and apktool to allow the analyst to decompile any APK given to it. There are also small bash parsing scripts that will parse through the AndroidManifest of the decompiled APK to retrieve a human readable text file with the important permissions, services, receivers, and network manifest file details used. The repo also includes scripts to help set up Genymotion to create a virtual mobile device that can be used for testing the suspicious APK if they do not have a physical rooted device to test with. Lastly, there are detailed instructions on how to “root” an Android device running Android 13 with Magisk. The instructions also detail the process of installing a root certificate from “mitmproxy” on the physical, rooted Android device so traffic leaving the device can be decrypted.

Conclusion

Even on modern mobile devices running the latest operating systems, installed apps still have the potential to expose the device to low-hanging security issues that have been around for decades. Major applications that are used by tens of millions of users are still using cleartext HTTP traffic in components, as seen in at least one of the telco and government apps we analyzed. Although Android and iOS have tried to make it more difficult to use any cleartext network traffic in applications, there are still techniques for developers to get around this by explicitly declaring the domains that cleartext can be used for. In addition, every telco we tested but one, sends SMS links to the user’s device that are vulnerable to SSL strip techniques where an attacker can downgrade the connection to cleartext and eavesdrop on the information exchanged.

Furthermore, these apps often exchange personally identifiable information (PII) of the users that should only be sent to application servers or third-party servers that the user is made explicitly aware of receiving their data through the app’s privacy policy or user agreements. However, through developer error or lack of transparency, we observed two of the four telco apps leaking PII to third-party entities. The companies and developers that maintain these apps need to ensure they are not exposing their own customers and citizens to cyber threats for simply downloading their app that they are incentivized to use. The developers of these major apps need to address serious vulnerability disclosures like the two that were sent to MiTelcel and SAT Movil in a timely manner. As of September 2023, we have received no response to both vulnerability disclosures submitted.