Analyzing Prominent Mobile Apps in Latin America

Beau Kujath
Arizona State University /
Breakpointing Bad
beau@breakpointingbad.com

Jeffrey Knockel
Citizen Lab
jeff@citizenlab.ca

Paul Aguilar
SocialTIC
seguridad@socialtic.org

Diego Morabito
SocialTIC
diego.morabito@socialtic.org

Masashi Crete-Nishihata
Citizen Lab
masashi@citizenlab.ca

Jedidiah R. Crandall
Arizona State University /
Breakpointing Bad
jedimaestro@asu.edu

ABSTRACT

We investigate the security and privacy state of a short list of widely used mobile apps that are relied on for crucial services by millions of users in Latin America (LATAM). Our assessment employs both static and dynamic analyses to evaluate each app (APK) for protection in three categories: proper encryption, safe handling of personally identifiable information (PII), and a properly secured and vetted software update process. These are important to at-risk users (such as journalists and activists) in any context, but the heightened risk to journalists in LATAM means that surveillance and targeted malware attacks are preeminent characteristics of information controls in this region. In LATAM, censorship often takes the form of surveillance coupled with physical threats to journalists, and government actors are not the only actors with the resources and power relationships to carry out this form of censorship. Therefore, the three categories of security and privacy issues we investigate for LATAM apps in this paper are of critical importance to the safety of journalists in the region.

KEYWORDS

reverse engineering, Latin America, security, privacy

1 INTRODUCTION

With the help of leaders at SocialTIC, a non-profit digital rights organization based in Mexico City, we identified eight 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 apps, government-developed apps, or marketplace apps. 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. The eight apps we analyzed break down into categories as follows:

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

Among the eight apps we analyzed, we found security and privacy issues relating to weak network security, leaked PII (personally identifiable information), and performing external updates outside of the app store. 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, we found the following issues:

- 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.

2 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 the 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 [2, 5], an independent transparency group in Mexico. This results in a media environment in the region that allows federal and state officials to

Table 1: Mobile apps analyzed during project.

App Name	Developer	Use	Popularity
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 seven 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 eight 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 eight different countries	second largest mobile provider in both Mexico and Paraguay
SAT Móvil	Government of Mexico	access tax services available in a personalized space	only official mobile app for Mexican citizens to access
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 one 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 dollars BTC incentive
Mercado Libre	Mercado Libre	e-commerce platform similar to Amazon	the largest e-commerce platform in Latin America with market share over 50%

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 [2]. Most news outlets in the region are dependent on the massive government advertisement 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 [7]. The Mexican digital rights group R3D (Red en los Defensa de los Derechos Digitales) released a report [21] that identified Pegasus malware infections [22] 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 [14] 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 [8] 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 [11]. 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 [6], 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 [6]. At least 119 media workers have been killed in the country since the turn of the century, according to the Committee to Protect Journalists [26]. 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 therefore vital that users are not exposed to vulnerable applications that make it simple to target their personal devices.

3 THREAT BREAKDOWN

Throughout our analysis, we used a Google Pixel 4a (Android 13) device to dynamically test the behavior of each app. We chose to focus solely on Android for the analysis (rather than iOS and others)

since Android dominates the market share in South America with 84% of the market share and holds a 69.9% market share worldwide [3]. There are three main security and privacy threat classes for which we assess each app:

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

3.1 Weak Network Security

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.

3.2 Leaked PII

The second threat for which we evaluated each app is the leaking of personally identifiable information. This is when info that 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 app developers. Apps may 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.

3.3 External Updates

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 either of these official app stores will be reviewed by a trusted team that is responsible for making sure there are no glaring security or privacy issues introduced in the update. 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 [1] 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 [4].

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 [18] 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 [12], 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 [16].

In the August 2023 Threat Horizons Report [9], the Google Cybersecurity Action Team 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 [13] 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.

4 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 2022, 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 [23]. 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 by Privacy International [10]. 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 six 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 [20].

Within Mexico, the telephony market is dominated by the American Movil owned brand Telcel. According to Statista [23], 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 [24]. They are followed by Tigo's owner, Millicom, with control of 19% then 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.

A summary of the companies and the regions in which they operate is as follows:

- MiTelcel — Mexico
- MiClaro — Argentina, Chile, Colombia, Dominican Republic, Ecuador, Peru, Puerto Rico
- Movistar — Argentina, Colombia, Ecuador, El Salvador, Honduras, Nicaragua, Panama, Paraguay
- MiTigo — Bolivia, Colombia, Costa Rica, El Salvador, Honduras, Nicaragua, Panama

5 APP BREAKDOWN

In this section we provide background on the telco, government, and marketplace apps that we analyze.

5.1 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 seven different mobile apps available on the Google Play Store that target each of the different countries in which it operates. This includes "MiClaro Brazil", "MiClaro Argentina", "MiClaro Peru", and more. The MiMovistar apps are similar to Claro in that it has eight 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 eight 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 a plan, managing members on a 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.

5.2 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 one 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. The official emergency app from the Mexico City Police has over one million downloads and a Play Store rating of 4.1 out of 5.

5.3 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 [25]. 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 [17] 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 one 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.

6 METHODOLOGY

Below we describe the test environment we used to analyze each of the apps. We also detail the tools and steps involved for assessing each app against the three different threat classes presented above.

In order to have the permission to install custom root certificates on the client device to decrypt outgoing application traffic, we required a mobile device with root access. As stated before, we chose to use a Google Pixel 4a to root. On it we installed a custom certificate generated by mitmproxy. Using mitmproxy we can MITM an app's traffic on the rooted mobile device and see the details of what is sent and to whom. We used an Ubuntu 22.04 desktop to run mitmproxy.

6.1 Weak Network Security

By statically analyzing the Android manifest file, we discerned whether apps would permit cleartext traffic using high level Android APIs by looking for the "cleartextTrafficPermitted" flag. However, the existence of this flag does not mean that the app actually generates such traffic. Similarly, even in the absence of this flag, an app may still generate cleartext traffic using lower level APIs.

As such, we also applied dynamic analysis using mitmproxy and a rooted device (or Wireshark for cleartext) to be able to determine which apps transmit or fetch any information in the clear and what those communications contain. Furthermore, dynamically, we can view the details of the encryption protocols being used and the certificates the apps are trusting so as to identify issues such as the use of outdated encryption protocols or trust issues with certificates.

6.2 Leaked PII

To start, we use static analysis to see which background services and receivers are used in the Android manifest file. Then, dynamic analysis is conducted with mitmproxy and a rooted device to be able to decrypt the outgoing HTTPS traffic being sent and received by the app. This allows us to capture and view (in real-time) the details of the encrypted traffic being sent to each background receiver and if any includes PII of the user. This step requires the analyst to manually step through each request that is seen in mitmproxy. Each packet is checked for potential PII that is shared and not disclosed in the privacy policy. If we do find a potential private info leak, then we will re-verify the leak is consistent by continually killing and opening the app to ensure it is reproducible.

6.3 External Updates

The external update threat may be difficult to capture in practice because apps may rarely receive updates. The most effective way we found to determine if an app can receive external updates is by first examining the permissions and receivers that are used. Historically, if an Android app used the "REQUEST_INSTALL_-PACKAGES" permission it would be able to install APKs outside of the app store. This could be potentially dangerous to the user who could unknowingly have a separate app installed on their device by the known app. However, we did not see this permission included in any of the current versions of the apps we reviewed, although we did see older versions include this. We did find, through dynamic analysis, one app — Chivo Wallet — that will check with external servers each time it is opened to see if it needs a dynamic update.

Aside from executable code, we also evaluated apps for externally downloading other types of data that significantly affect the behavior of the app. As a key example, we found apps that downloaded lists of phone numbers used to programmatically forward all phone calls to those numbers over a third party voice-over-IP service. In our threat model, we are not concerned only with attacks from third parties but also consider that the app vendors themselves or the operators of services used by the apps may be complicit in targeted attacks, and therefore we consider ways in which apps' behavior could be modified at runtime for targeted users in a way that escapes Google Play Store review.

6.4 Further Details

A repo further documenting our analysis methods is available publicly on Github[1]. It includes steps to configure a similar test environment for anyone with an APK they want to reverse engineer and dynamically analyze. It also includes more information on the specific static and dynamic analysis tools used. Along with the steps used to root the Android device and configure the custom root certificates needed.

7 FINDINGS

In this section we detail our findings from analyzing each of the telco, government, and marketplace apps.

7.1 Telco Apps — MiTelcel, MiClaro, MiMovistar, MiTigo

The Claro, Movistar, and Tigo apps are available in 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,

---

[1]https://github.com/beaukuj15/relab

**Table 2: Security / privacy issues found in telco apps.**

MiTelcel	Loads multiple images and JSON files on the main page in the clear (plain HTTP)
MiTelcel	POSTs 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	Receives telco SMS messages with external links vulnerable to SSL strip attacks
MiClaro Colombia	POSTs location info to multiple third party servers without user disclosure

MovistarMX, and more. We found that in the eight different Tigo apps, the source code is nearly identical to one another besides 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.

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.

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 HTTPS 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 tested each of the servers included in the links of the SMS messages for HSTS (HTTP Strict Transport Security), but none of the servers included the feature to protect from SSL strip attacks.

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 location information, including latitude and longitude coordinates of the device,
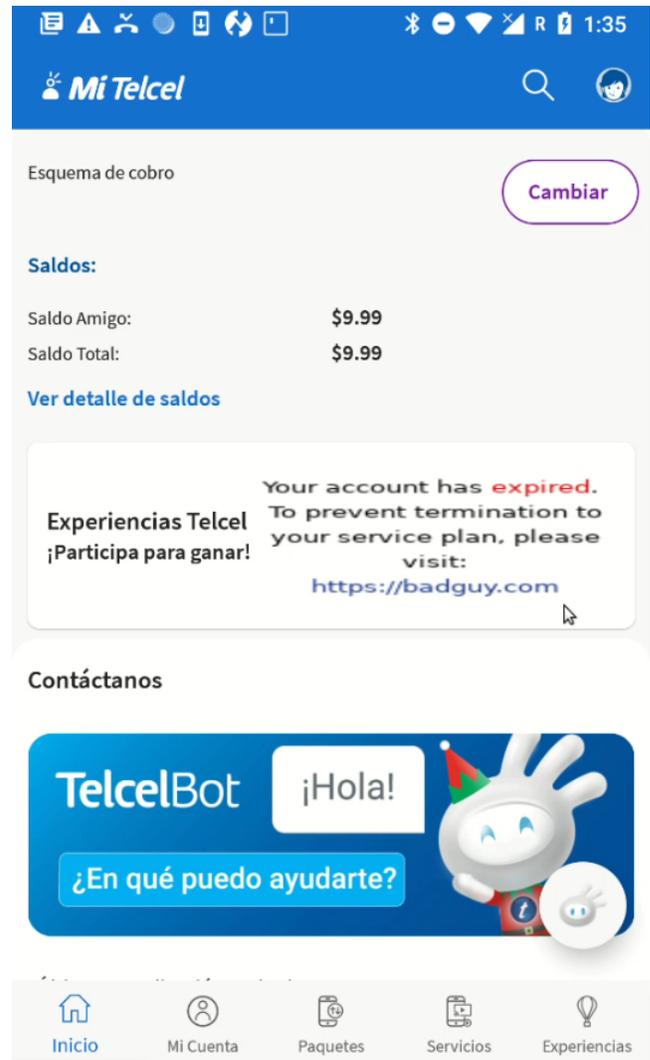
Figure 1: Fake attacker image being injected and shown on the MiTelcel home screen.

to third parties without user disclosure. We also consider this to be a leak of PII since the app directly states in the Google Play Store that it does not share personal info with any third parties.

While we found that the telco apps in general perform updates in a secure manner that can be vetted by Google in the Google Play Store, the MiTelcel and MovistarMX apps include a money-saving functionality called DialMyApp that grants a third party the ability to reroute phone calls using the "PROCESS_OUTGOING_CALLS" permission. The phone numbers to be rerouted are downloaded by the app from DialMyApp servers and thus can be updated in a way that cannot be vetted by Google or even by the telco itself. Some United States based telco apps including MyVerizon and TMobile also are able to process outgoing calls, but they are redirected and handled by an in-house call receiver.

We found a few common security issues that could be addressed by the telco apps including the cleartext traffic used in MiTelcel

```
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 five GET requests sent to third party servers from the MiTelcel app that includes PII in the "referer" field URL. The above request is triggered by clicking the "Experiencias" tab at the bottom right of the app.

Table 3: Security / privacy issues found in government apps.

SAT Movil	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	Holds clear text file in app folder on rooted devices with every piece of personal info collected by the app including medical diagnosis, ID numbers, health appointments, and more

and the predictable web links sent to each device that an in-path attacker could SSL strip. We disclosed these vulnerabilities to MiTelcel developers in March of 2023. Additionally, we found privacy issues with some of the telco apps including the undisclosed sharing of PII with multiple third parties (MiTelcel and MovistarMx) and location information being leaked to various third party servers (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 code is practically identical for each country in which they operate.

7.2 Government apps — IMSS Digital, SAT Movil, MiPolicia

Among 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.

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 Fisicas" (annual declaration natural persons), "Cedula de Identificacion 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 any connection to "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 Figures 3 and 4 in Appendix A. We provide a link to the full demonstration video of the attack[2]. An official disclosure was sent to the developers of SAT Movil with information on the vulnerability and how to address it.

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

---

[2]https://drive.google.com/file/d/1WwqxQQ0mKKJYkOTSSGOXchVJobioMUhL/view?usp=sharing

Table 4: Security / privacy issues found in marketplace apps.

Chivo Wallet (external update)	Includes Microsoft CodePush service that could externally update the app
Chivo Wallet (activity leak)	POSTs to a NewRelic analytics server with in-app event details that include what each user types, including ID numbers, phone numbers, and passwords.
Mercado Libre	Sends POST requests to three different third parties (TikTok, Facebook, and Google) with information on each product that is clicked in the app

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.

7.3 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 background services: Braze for customer engagement, AppAdjust for analytics, and Bitmovin for playing videos in app. Chivo Wallet 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.

Each time the Chivo Wallet app is opened it will make a request to "codepush.appcenter.ms/b0.1/public/codepush/updatecheck?..." 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 [15] repository for CodePush, it is "a cloud service that enables Cordova and React Native developers to deploy mobile app updates directly to their users' devices. CodePush works by acting as a central repository that developers can publish updates to (JavaScript, HTML, CSS and images), and that apps can query for updates from." This functionality allows the Chivo Wallet developers (the 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 servers operated by NewRelic, which is 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 among 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 personally identifiable information unless ML models were able to consistently predict which person is most likely to access a set of products.

8 CONCLUSION

In the short list of widely used mobile apps in LATAM that were analyzed, we found issues belonging to each of our three protection categories: proper encryption, safe handling of personally identifiable information (PII), and a properly secured and vetted software update process. With the elevated risk to journalists and civil rights defenders currently in the region, these issues imply that surveillance and targeted malware attacks are still prevalent in the latest versions of major apps with large threat surfaces due to their millions of users. For example, a low-budget attacker that knows about the tax app that leaks cleartext ID information could sit on an airport WiFi and collect identities of users that access the "Chat" page. This same threat example could apply to a small town in the region that has network choke points upstream to route internet traffic.

In a 2024 Politico [19] interview with internet freedom journalist, Byron Tau, the expert said, "The police could buy up your geolocation movements and look at them without a warrant. And so he was essentially saying that the success lies in the secrecy, that if people were to know that this was what the police department was doing, they would ditch their phones or they would not download certain apps." Conducting dynamic analysis on these prominent apps is vital to ensure that this "secrecy" can be caught and reported so that users are not put at more risk than they are aware of.

REFERENCES

[1] ACLU. 2018. How Malicious Software Updates Endanger Everyone. https://www.aclu.org/issues/privacy-technology/consumer-privacy/how-malicious-software-updates-endanger-everyone [Accessed 14-04-2024].

[2] Azam Ahmed. 2017. Using Billions in Government Cash, Mexico Controls News Media (Published 2017) — nytimes.com. https://www.nytimes.com/2017/12/25/world/americas/mexico-press-government-advertising.html [Accessed 14-04-2024].

[3] Andrew Buck. 2024. Android vs iOS Market Share: Most Popular Mobile OS in 2024. https://www.mobiloud.com/blog/android-vs-ios-market-share

[4] Graham Cluley. 2018. Beware Malicious Software Updates for Legitimate Apps. https://www.bitdefender.com/blog/businessinsights/malicious-software-updates-legitimate-apps/ [Accessed 14-04-2024].

[5] Fundar. 2024. Fundar English. https://fundar.org.mx/english/

[6] The Guardian. 2020. The Cartel Project. https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption [Accessed 14-04-2024].

[7] The Guardian. 2021. Mexico accused of spying on journalists and activists using cellphone malware. https://www.theguardian.com/world/2017/jun/19/mexico-cellphone-software-spying-journalists-activists

[8] Enrique Hernández. 2021. La FGR usa poco el superequipo de espionaje que le costó más de 49 mdp1. https://www.forbes.com.mx/la-fgr-usa-poco-su-super-equipo-de-espionaje-legal-que-le-costo-mas-de-49-mdp/ [Accessed 14-04-2024].

[9] Threat Horizons. 2023. Malicious Apps Use Sneaky Versioning Technique to Bypass Google Play Store Scanners. https://thehackernews.com/2023/08/malicious-apps-use-sneaky-versioning.html [Accessed 14-04-2024].

[10] Privacy International. 2019. State of Privacy Mexico. https://privacyinternational.org/state-privacy/1006/state-privacy-mexico [Accessed 14-04-2024].

[11] Paul Rexton Kan. 2013. Cyberwar in the Underworld: Anonymous versus Los Zetas in Mexico. https://www.yalejournal.org/publications/cyberwar-in-the-underworld-anonymous-versus-los-zetas-in-mexico

[12] Brian Krebs. 2023. Google Suspends Chinese E-Commerce App Pinduoduo Over Malware. https://krebsonsecurity.com/2023/03/google-suspends-chinese-e-commerce-app-pinduoduo-over-malware/ [Accessed 14-04-2024].

[13] Ravie Lakshmanan. 2023. Data Stealing Malware Discovered in Popular Android Screen Recorder App. https://thehackernews.com/2023/05/data-stealing-malware-discovered-in.html [Accessed 14-04-2024].

[14] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert. 2020. *Running in Circles*. Technical Report. The Citizen Lab. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/ [Accessed 14-04-2024].

[15] Microsoft. 2015. Microsoft CodePush. https://github.com/microsoft/code-push [Accessed 14-04-2024].

[16] Lily Hay Newman. 2023. Security News This Week: Popular Chinese Shopping App Pinduoduo Is Laced With Malware. https://www.wired.com/story/pinduoduo-malware-security-roundup/ [Accessed 14-04-2024].

[17] Tom Nyarunda. 2021. Hackers Exploit Chivo Wallet Security Issues. https://blockzeit.com/hackers-targeting-free-bitcoin-hijack-chivo-bitcoin-wallet-setup-process/ [Accessed 14-04-2024].

[18] Charlie Osborne. 2021. With one update, this malicious Android app hijacked millions of devices. https://www.zdnet.com/article/with-one-update-this-malicious-android-app-hijacked-10-million-devices/ [Accessed 14-04-2024].

[19] Steven Overly. 2024. The Government Really Is Spying On You — And It's Legal. https://www.politico.com/news/magazine/2024/02/28/government-buying-your-data-00143742

[20] R3D. 2018. ¿Quién no defiende tus datos? https://r3d.mx/publicaciones/

[21] R3D. 2022. Ejército Espía: Fuera de Control. https://ejercitoespia.r3d.mx/ [Accessed 14-04-2024].

[22] John Scott-Railton. 2022. *New Pegasus Spyware Abuses Identified in Mexico*. Technical Report. The Citizen Lab. https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/ [Accessed 14-04-2024].

[23] Statista. 2022. Distribution of mobile telephony market in Mexico in 3rd quarter 2022, by company. https://www.statista.com/statistics/709668/mobile-telephony-market-company-mexico/ [Accessed 14-04-2024].

[24] Statista. 2023. Revenue generated by selected telecommunication providers in Latin America and the Caribbean in 2022. https://www.statista.com/statistics/998151/telecommunication-providers-revenue-latin-america/ [Accessed 14-04-2024].

[25] Luke Taylor. 2022. Most Salvadorans have already ditched their national bitcoin wallets. https://restofworld.org/2022/el-salvador-chivo-bitcoin-wallet/ [Accessed 14-04-2024].

[26] Committee to Protect Journalists. 2024. Committee to Protect Journalists - Mexico. https://cpj.org/americas/mexico/

A   SUPPLEMENTARY FIGURES

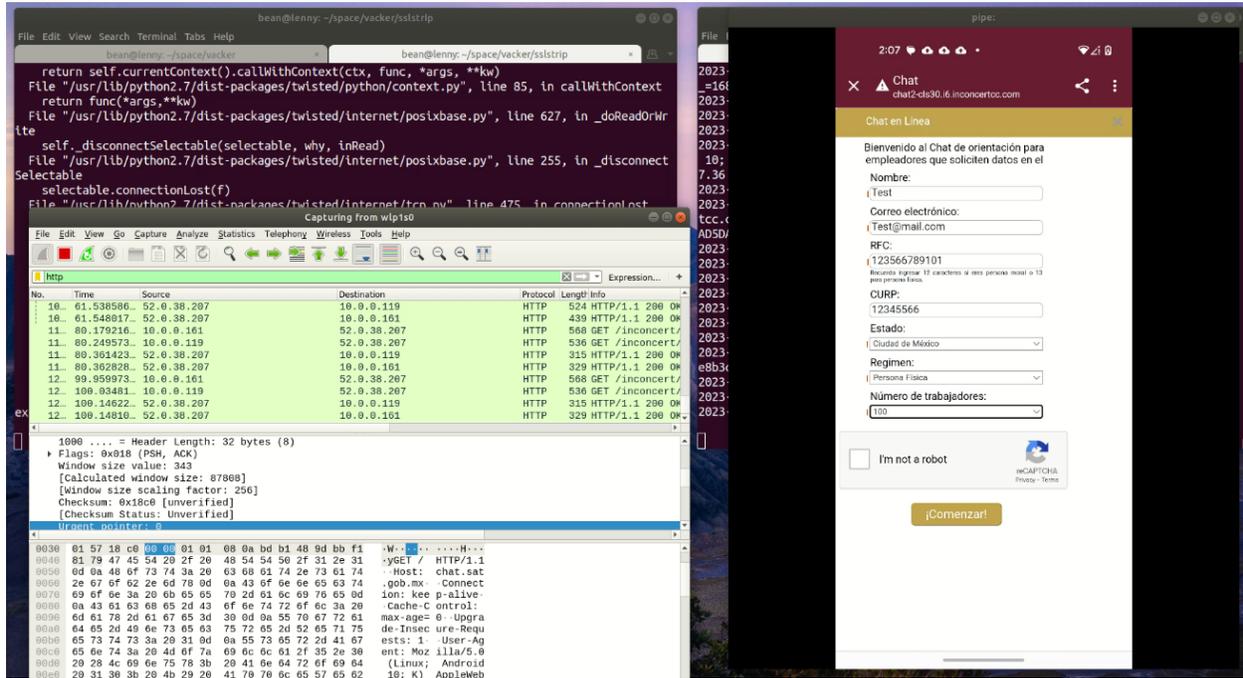In this section we present additional figures illustrating our successful sslstrip attack on SAT Movil.

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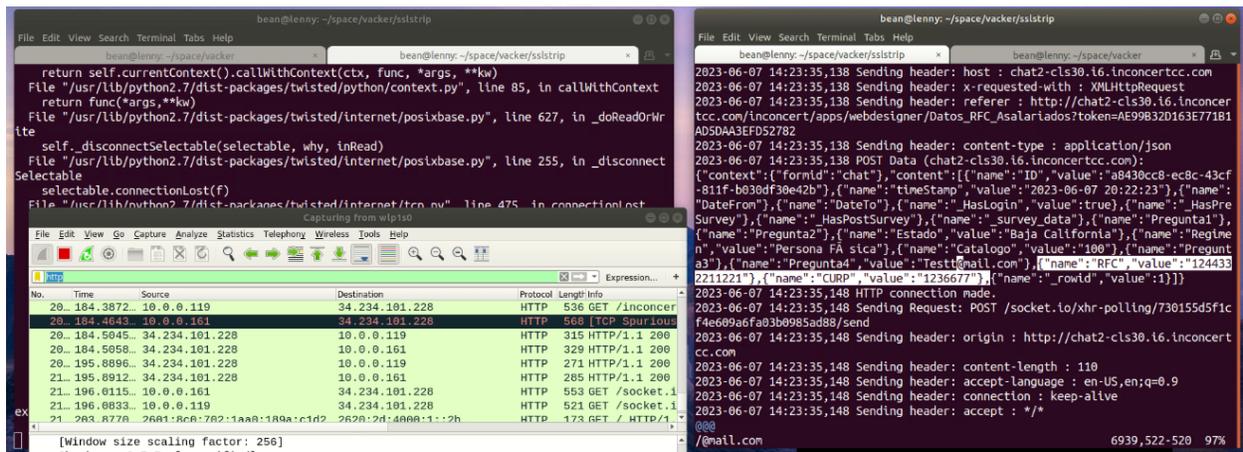

Figure 4: Screenshot of the result of sslstrip being used on SAT Movil's network communications; on the left, sensitive information is shown in the clear in Wireshark, on the right, sensitive information is outputted in the attacker's console.