PixPirate: Brazilian financial malware

By Nir Somech

Published: 2024-03-13 · Archived: 2026-04-05 17:05:07 UTC

Nir Somech

Malware Researcher – Trusteer IBM

Malicious software always aims to stay hidden, making itself invisible so the victims can't detect it. The constantly mutating PixPirate malware has taken that strategy to a new extreme.

PixPirate is a sophisticated financial remote access trojan (RAT) malware that heavily utilizes anti-research techniques. This malware's infection vector is based on two malicious apps: a downloader and a droppee. Operating together, these two apps communicate with each other to execute the fraud. So far, IBM Trusteer researchers have observed this malware attacking banks in Brazil.

A hidden threat

Within IBM Trusteer, we saw several different techniques to hide malware from its victims. Most banking malware conceals its existence on the mobile device by hiding its launcher icon from the victim using the SetComponentEnabeldSetting application programming interface (API). However, since Android 10, that technique no longer works due to new restrictions imposed by Google.

To address this new challenge, PixPirate introduced a new technique to hide its icon that we have never seen financial malware use before. Thanks to this new technique, during PixPirate reconnaissance and attack phases, the victim remains oblivious to the malicious operations that this malware performs in the background.

PixPirate abuses the accessibility service to gain RAT capabilities, monitor the victim's activities and steal the victim's online banking credentials, credit card details and login information of all targeted accounts. If two-factor authentication (2FA) is needed to complete the fraudulent transaction, the malware can also access, edit and delete the victim's SMS messages, including any messages the bank sends.

PixPirate uses modern capabilities and poses a serious threat to its victims. Here is a short list of PixPirate's main malicious capabilities:

- Manipulating and controlling other applications
- Keylogging
- Collecting a list of apps installed on the device
- Installing and removing apps from the infected device
- Locking and unlocking device screen
- Accessing registered phone accounts
- Accessing contact list and ongoing calls

- Pinpointing device location
- Anti-virtual machine (VM) and anti-debug capabilities
- Persistence after reboot
- Spreading through WhatsApp
- Reading, editing and deleting SMS messages
- Anti-removal and disabling Google Play Protect

Thanks to its RAT capabilities, PixPirate can perform on-device fraud (ODF) and execute the fraud from the victim's device to avoid detection by the bank's security and fraud detection systems.

The latest tech news, backed by expert insights

PixPirate infection flow

Most financial malware comprises one main Android Package (APK) file. This is not the case for PixPirate, which is built of two components: a downloader APK and the droppee APK. The use of a downloader app as part of a financial attack is not new; however, unlike most financial malware today that uses a downloader as a service, both the droppee and the downloader for PixPirate were created by the same actor.

In addition, the PixPirate downloader role in the infection flow of the malware is different from other financial malware. Usually, the downloader is used to download and install the dropped, and from this point on, the droppee is the main actor conducting all fraudulent operations and the downloader is irrelevant. In the case of PixPirate, the downloader is responsible not only for downloading and installing the droppee but also for running and executing it. The downloader plays an active part in the malicious activities of the droppee as they communicate with each other and send commands to execute.

Usually, victims get infected with PixPirate by downloading the PixPirate downloader from a malicious link sent to them through WhatsApp or an SMS phishing (smishing) message. This message convinces the victim to download the downloader, which impersonates a legitimate authentication app associated with the bank. Once the victim launches the downloader, it asks the victim to install an updated version of itself, which is, in fact, the actual PixPirate malware (the droppee). After the victim approves this update, the downloader either installs the droppee embedded in its APK or downloads it directly from the PixPirate command and control (C2) server. If the droppee is embedded in the downloader's APK file, it is encrypted and encoded in the downloader "/assets/" folder, masquerading as a jpeg file to lower suspicion.

Next, the downloader sends a command to the PixPirate droppee to activate and execute it. On the first run, the droppee prompts the victim to allow its accessibility service to run. In the next stage, PixPirate abuses the accessibility service to grant itself all the necessary permissions it needs to run and successfully perform financial fraud.

After the malware gets all the necessary permissions it needs to run, it collects some information and data regarding the infected device to decide if this is a legitimate device and a good candidate for fraud (anti-VM/anti-

emulator, which bank apps are installed on the device and so on) and then sends all this data to the PixPirate C2.

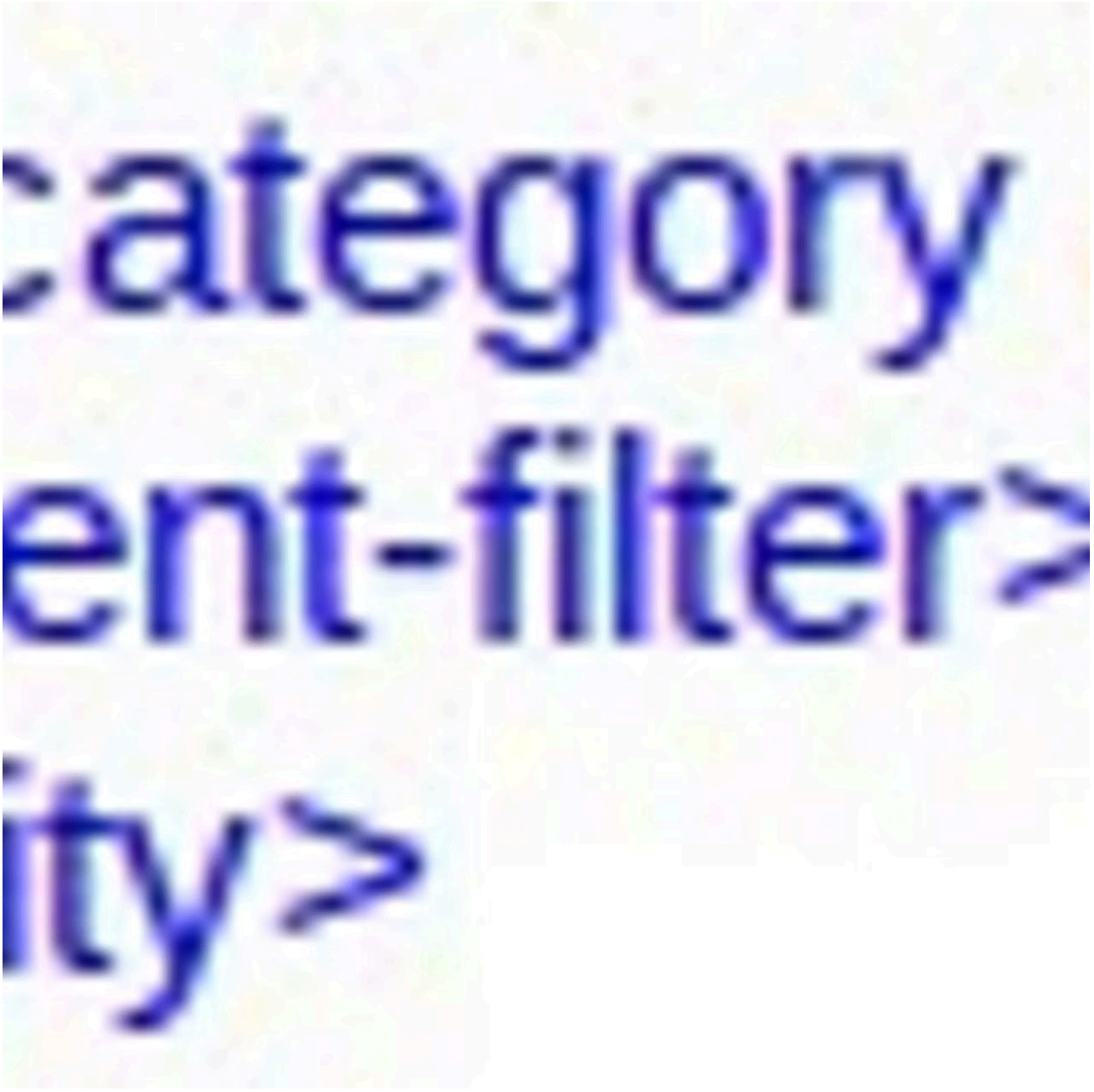
New hiding technique in the wild

Malware has always tried to hide and conceal itself from its intended victim. The most obvious and effective way is to hide the launcher icon of the malicious APK because most users do not look at the app settings screen to check which apps are installed, so they won't notice the malicious app and will not try to remove it.

Traditionally, financial malware hides the launcher icon using the "SetComponentEnabledSetting" API. This technique does not require any permission to be granted by the victim. However, from Android 10, this technique became ineffective for malware and could not be used anymore. We will explain how the technique works using the FakeChat malware that also uses this technique.

The malware declares in the manifest the MainActivity that will be executed once the victim launches it by pressing its icon on the home screen of the mobile device.

In the following image, we can see in the FakeChat manifest the malware's app tag and the path of the app icon in the icon value. Also, the manifest contains the MainActivity with the name "com.eg.android.AlipayGphone.MainActivity" with the action "android.intent.action.Main" and the category "android.intent.category.LANUCHER." This activity will be run and executed once the user presses the app's icon and launches the app.



In the first run of the malware, it makes the launcher icon disappear by calling the Android API "SetComponentEnabledSetting" with the following parameters:

- ComponentName: the component that represents the MainActivity related to the icon for launching the app.
- NewState: the new state of the component. In this case, the malware specifies the state "COMPONENT_ENABLED_STATE_DISABLED" to disable and hide the APK icon.
- Flags (optional): Value is either 0 or a combination of DONT_KILL_APP and SYNCHRONOUS.

In the following image, we can see how it is done programmatically:

```
Bot.Context.getPackageManager().SetComponentEnabledSetting(New ComponenetName (Bot.Context, MainActivity.class), 2, 1);
```

From Android 10, all app icons are visible in the launcher unless it is a system app or it does not ask for any permission at all (look at the documentation and the guide). Those limitations made this technique irrelevant for malware from Android 10 and later. Therefore, malware could no longer hide its launcher icon and its existence.

PixPirate's new innovative hiding technique

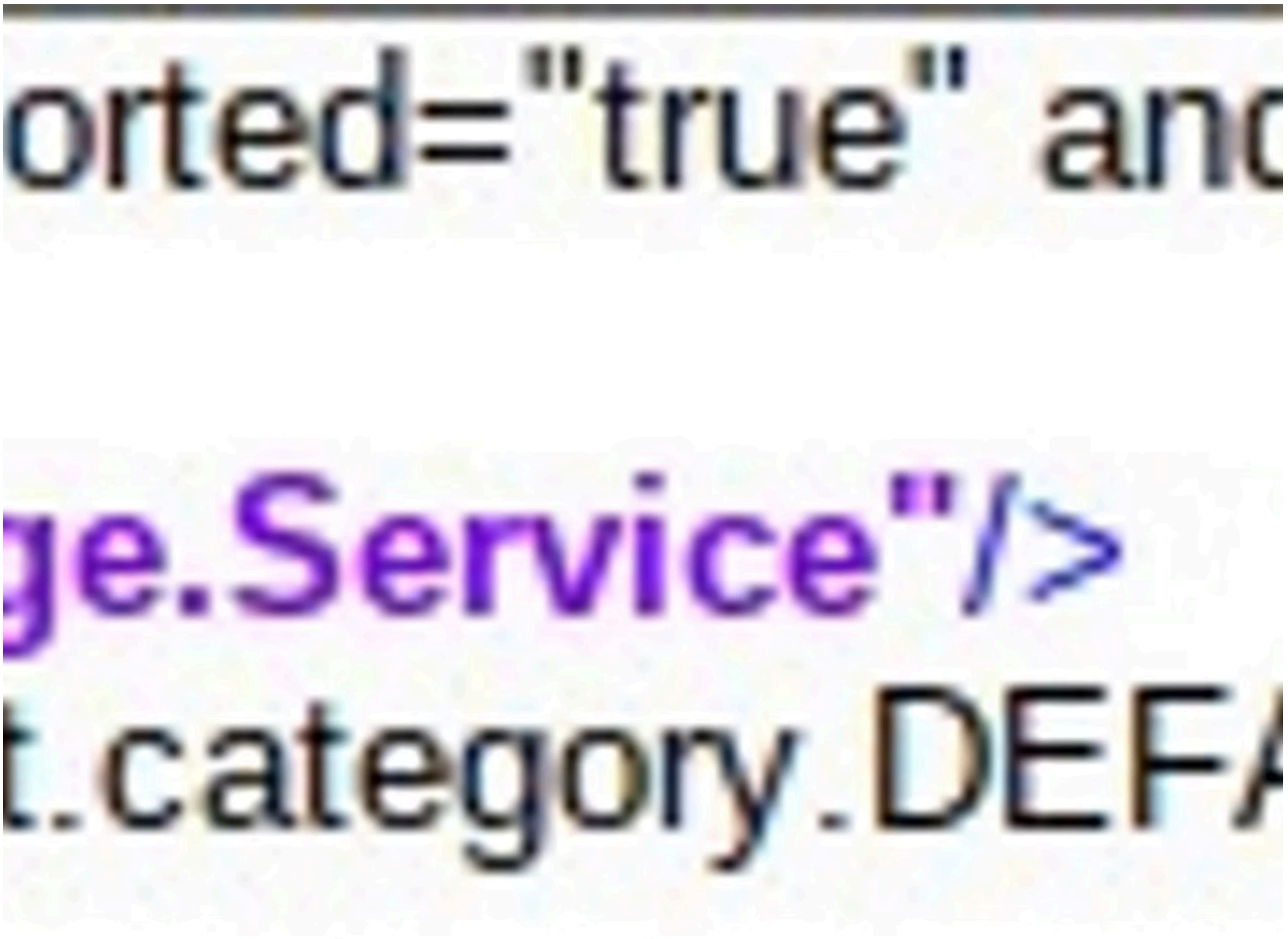
When examining PixPirate, IBM Trusteer detected a new technique to achieve the same goal that works in all Android versions to date. To accomplish the goal of hiding malware from the victim, the PixPirate droppee does not have a main activity; that is, it does not have an activity with the action "android.intent.action.MAIN" and category "android.intent.category.LANUCHER." This change in behavior means that the app's icon does not exist on the home screen of the victim's device at all. However, this also presents a new problem. If the droppee's icon does not exist on the victim's home screen, how will the victim launch the app in the first place?

The new technique requires the malware to have two applications: in this case, the downloader and the droppee that operate together. The downloader is the app that runs. The downloader then runs the droppee, which would not be executed otherwise since its icon does not exist.

How the droppee runs

So, how does the droppee run? PixPirate built a mechanism that triggers the droppee to run when different events occur on the device.

In the following image, we can see the service used to launch the droppee replacing the activity ("MainActivity") used in other apps and APKs. The service is exported and can be run by other processes running on the device. This service has a custom-made action triggered by binding to this specific service. The downloader uses this to create and bind to this service and run the droppee every time it is required.



The method works as follows:

- The droppee has a service called “com.companian.date.sepherd” exported and holds an intent-filter with the custom action “com.ticket.stage.Service.”
- When the downloader wants to run the droppee, it creates and binds to this droppee service using the API “BindService” with the flag “BIND_AUTO_CREATE” that creates and runs the droppee service.
- After the creation and binding of the droppee service, the droppee APK is launched and starts to operate.

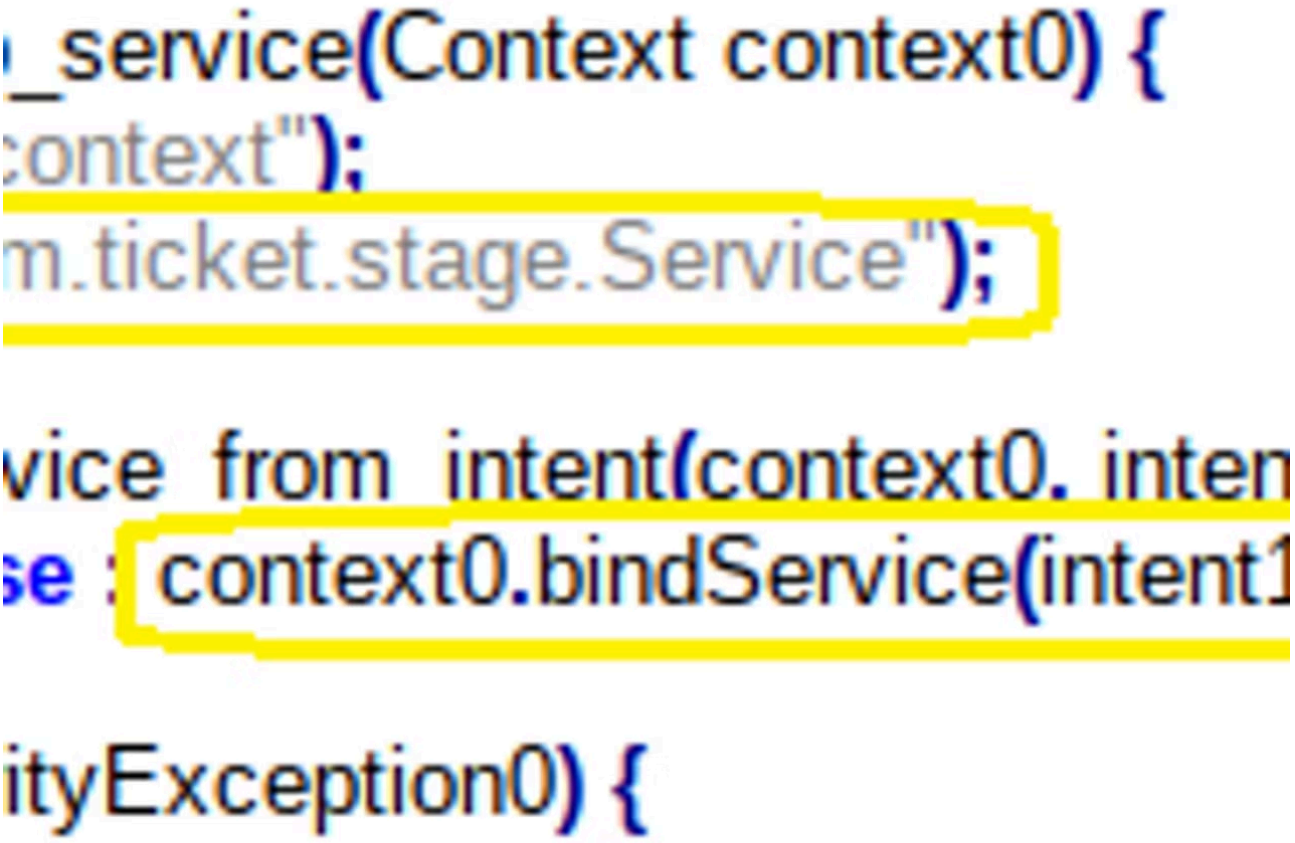
The BindService API has the following parameters:

- The service intent “com.ticket.stage.Service”
- The flag “BIND_AUTO_CREATE” (0x01) that creates and binds to the service (if the service does not exist)

- ServiceConnection object that connects to the droppee service and consists of an interface to monitor the state of the application service

In this way, the downloader succeeds in triggering the droppee to run. The ServiceConnection object is used as an interface to maintain communications between the downloader and the droppee and allows them to send messages between themselves and communicate through this interface.

In the following image, we see the code from the downloader APK that creates and binds to the exported service of the droppee APK, which we saw in the previous image, to trigger the droppee to run and send it commands to execute.



This code must run at the first running and execution of the droppee, just after the downloader installs the droppee. Later, to maintain persistence, the droppee is also triggered to run by the different receivers that it

registered. The receivers are set to be activated based on different events that occur in the system and not necessarily by the downloader that initially triggered the droppee to run.

This technique allows the PixPirate droppee to run and hide its existence even if the victim removes the PixPirate downloader from their device. PixPirate malware is the first financial malware observed by IBM Trusteer researchers that uses this technique to hide itself and its launcher icon so that victims won't notice that malware is installed and running on the device.

Fraud modus operandi

PixPirate campaigns mostly target customers of banks in Brazil. It mainly attacks the Brazilian payment service called Pix, the standard instant payment platform in Brazil. Most of the banks in Brazil implement the Pix API to support Pix transactions from within the banking app itself.

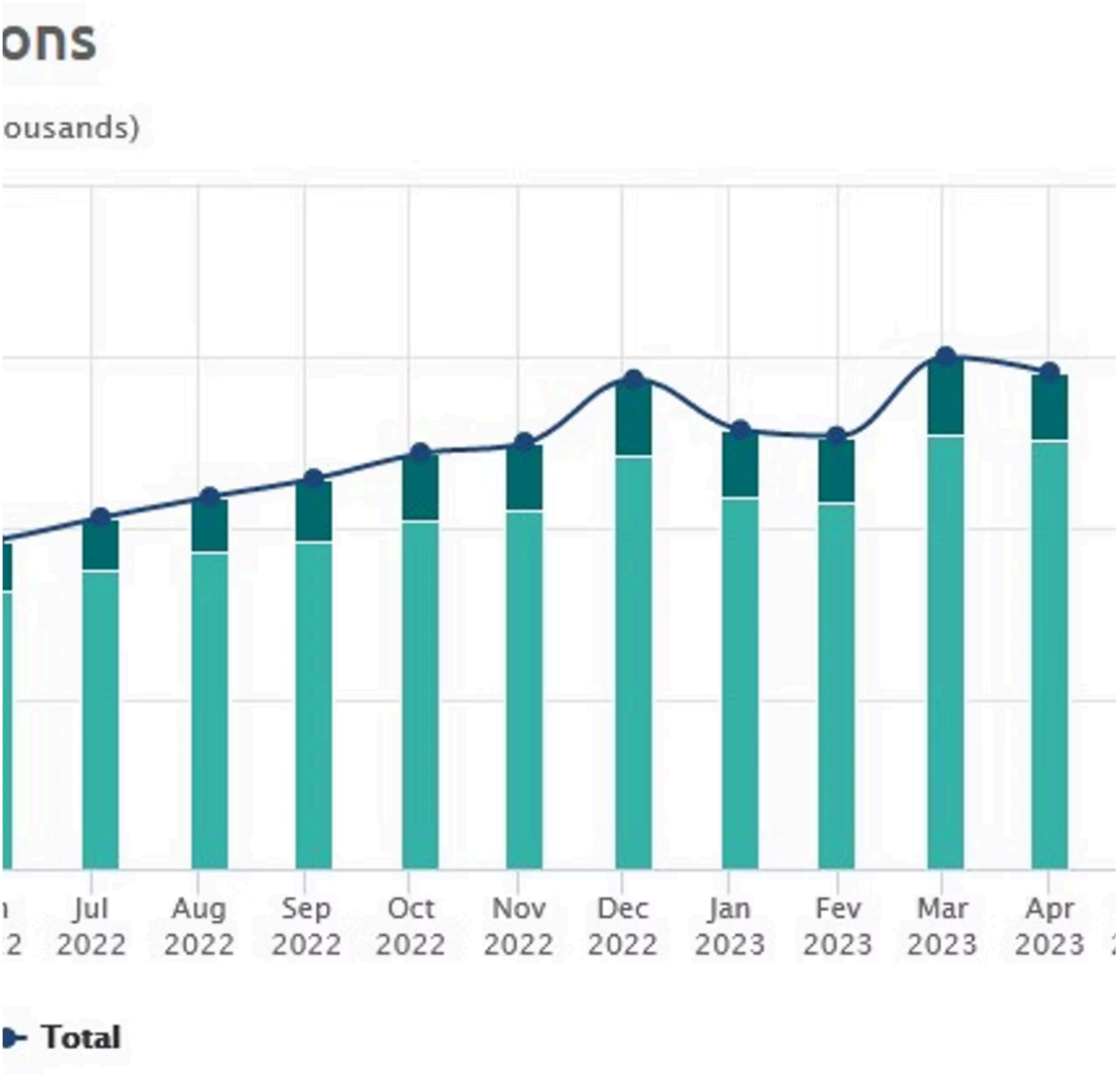
When the malware decides to carry out the fraud, it pops up a new screen on top of the current screen of the device that hides the malware's malicious activities from the victim. The malware launches the bank app (if it's not running yet) and goes to the Pix page by pressing the app buttons programmatically. Once on the Pix transfer/payment page, the malware executes the Pix money transfer.

In the following image, we can see the different functions the malware calls to enter the relevant details and execute the money transfer (Pix details, amount, password and so on).

What is Pix?

Pix is an instant payment platform that enables the quick execution of payments and transfers between bank accounts. Customers receive a Pix string or QR code that contains the amount to pay for services or goods to complete a transaction. Then, customers pay the Pix payment using their bank apps or through internet banking. They can pay or transfer money using Pix through their banking app.

The Pix payment service launched in November 2020 was heavily adopted by users and businesses in Brazil and broke records in the number of users, financial transactions, and volumes. In the following graph, we can see the number of Pix transactions (in thousands). In March 2023, it reached 3 billion transactions in a single month.



Financial transaction volume reached 1,250,000,000,000 Brazilian reals in March 2023, which is about $250 billion. By May 2023, the number of Pix users reached 140 million.

Pix fraud MO

PixPirate Pix fraud occurs by initiating a new Pix transaction from the victim to the fraudster's Pix account or by changing the Pix details of the receiver of a legitimate Pix transaction initiated by the victim to the fraudster's Pix details.

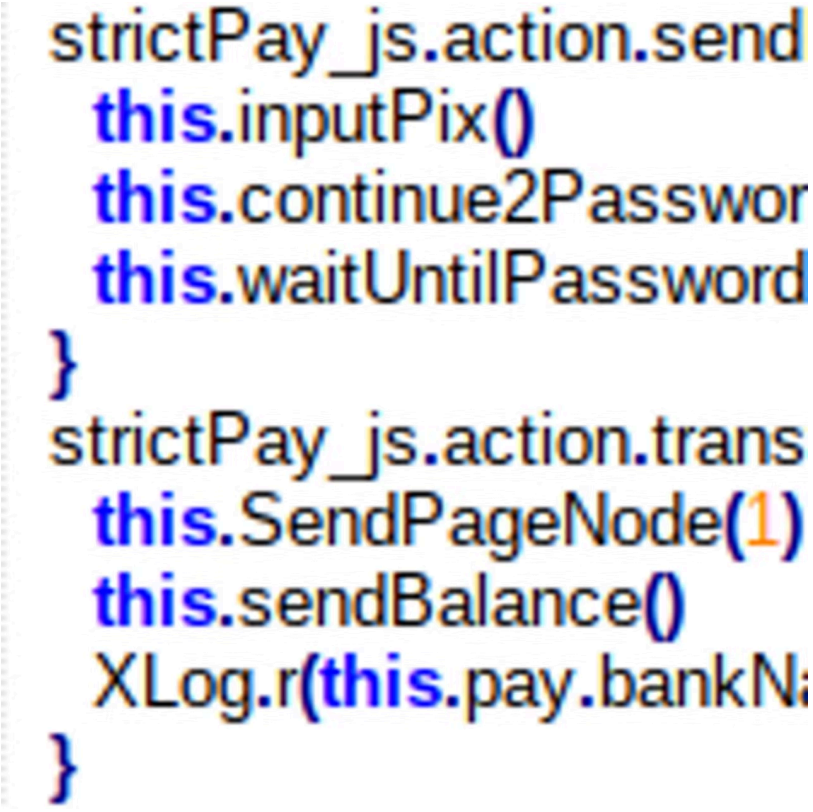
Technically, Pix fraud is performed thanks to PixPirate RAT capabilities gained by abusing the Android accessibility service. The malware monitors the victim's activities on the device and waits for the user to launch a targeted banking application. On each accessibility event, it checks the type of event that occurred. If the event

type is “TYPE_WINDOW_STATE_CHANGED,” it retrieves the name of the package of the app from the window. If the app is in the target list, the malware can start its malicious activities.

When the victim launches their bank app, the malware grabs and collects the user credentials and account info while the user enters their credentials to log in. The malware sends the stolen info and credentials to the attacker’s C2 server. The victim is not aware that the malware is stealing credentials as everything seems legitimate, as the malware hides itself and operates in the background.

When the malware decides to carry out the fraud, it pops up a new screen on top of the current screen of the device that hides the malware’s malicious activities from the victim. The malware launches the bank app (if it’s not running yet) and goes to the Pix page by pressing the app buttons programmatically. Once on the Pix transfer/payment page, the malware executes the Pix money transfer.

In the following image, we can see the different functions the malware calls to enter the relevant details and execute the money transfer (Pix details, amount, password and so on).



The main function responsible for the fraud is “strictPay_js.action.transfer,” which automatically executes the fraud. First, it calls SendPageNode(1) with the argument “1”. This function navigates to the Pix page in the banking application. The next function is sendBalance(), which consists of three subfunctions:

- **inputPix():** Enters the Pix details for executing the Pix money transfer
- **continue2Password():** The malware enters the stolen victim’s credentials
- **waitUntilPassword():** Waits until the Pix money transfer is completed and validates that it was successfully executed

The same technique is used by PixPirate for the second Pix attack MO of intercepting the victim operations and changing the Pix details while the victim transfers the money without the victim knowing. PixPirate can manipulate both the target account and the Pix transaction amount.

If 2FA is needed as part of the banking flow, the malware can also intercept SMS messages that the user receives from the bank.

Automatic fraud capabilities

PixPirate fraud occurs automatically, as this malware contains code for all the different activities that are required to complete Pix fraud — log in, enter Pix details, enter credentials, confirm and more. PixPirate is not only an automated attack tool, but it also has the capability of becoming a manually operated remote control attack tool. This capability is probably implemented to manually execute fraud if the automatic fraud execution flows fail because the user interface of the banking app changes or if a new lucrative target presents itself.

The manual fraud is initiated by popping up an overlay screen on the victim's device and disabling the user control on the infected device to hide the fraudster's activities in the background. Next, the malware connects to the C2 and receives commands from the fraudster to be executed. This remote-control capability gives the fraudster control of the victim's device, including accessing private information and manipulating applications on the victim's device.

Stay up to date on PixPirate's capabilities

With nuanced methods of staying hidden and the capacity for serious harm, PixPirate presents a troubling new threat on the malware playing field. We will discuss more on PixPirate's functionality, capabilities and commands it can receive from the C2 server in part two of our PixPirate blog.

PixPirate IOCs:
Downloader: 019a5c8c724e490df29020c1854c5b015413c9f39af640f7b34190fd4c989e81
Droppee: 9360f2ee1db89f9bac13f8de427a7b89c24919361dcd004c40c95859c8ce6a79
