# PixPirate back spreading via WhatsApp

By Nir Somech

Published: 2024-11-26 · Archived: 2026-04-05 18:25:36 UTC

Nir Somech

Malware Researcher – Trusteer IBM

*This blog post is the continuation of a previous blog regarding PixPirate malware. If you haven't read the initial post, please take a couple of minutes to get caught up before diving into this content.*

PixPirate malware consists of two components: a downloader application and a droppee application, and both are custom-made and operated by the same fraudster group. Although the traditional role of a downloader is to install the droppee on the victim device, with PixPirate, the downloader also *runs* the droppee. Without this operation by the PixPirate downloader, the droppee, i.e. the malware itself, would never run. In addition, the PixPirate downloader can send commands to the droppee for execution and has an active role in the droppee activities and operations.

In the most basic terms, the PixPirate downloader pretends to be a legitimate authentication application that helps users secure their bank accounts.

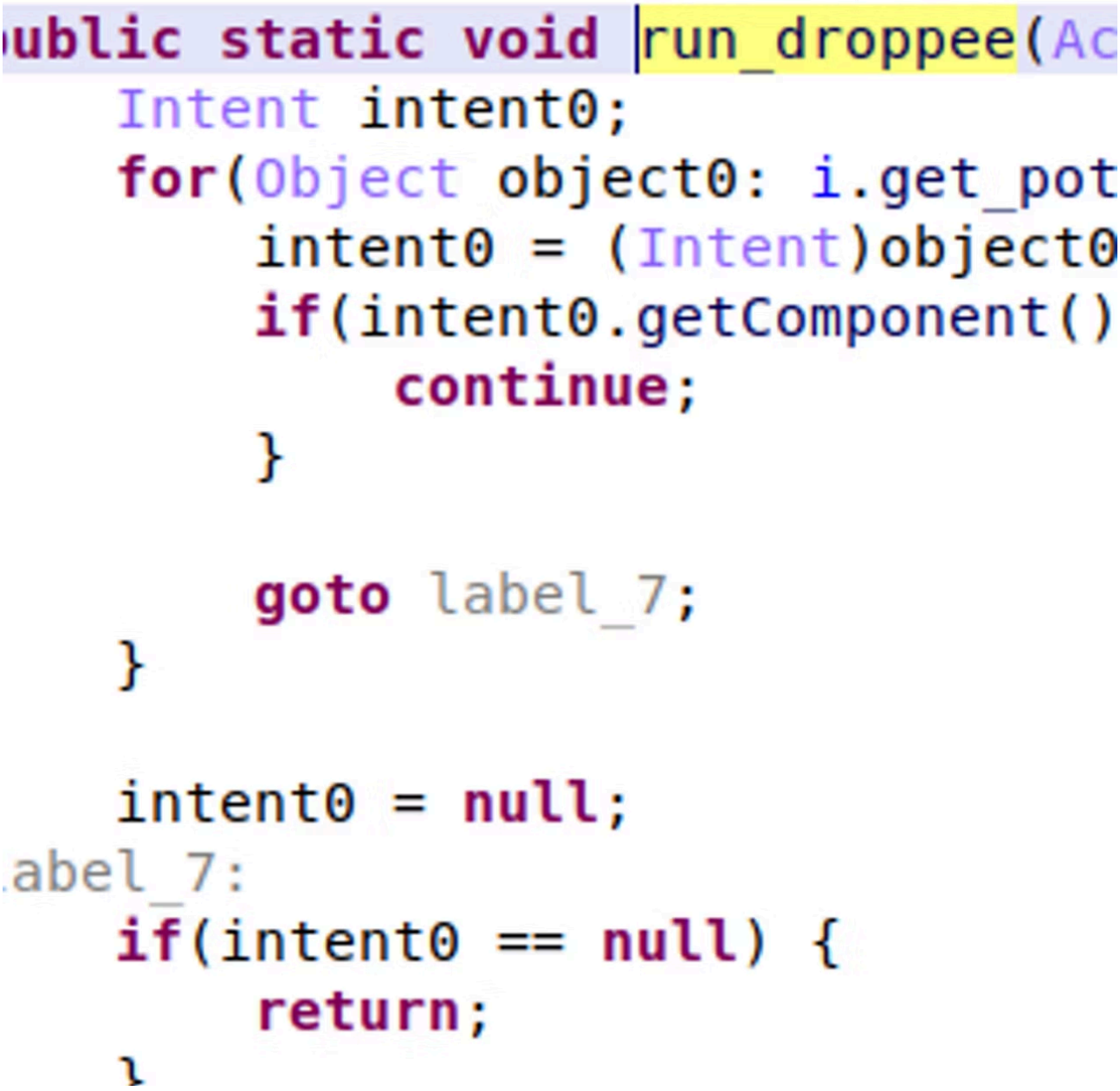
```
public static ArrayList get_potential_dr
    Intent intent1;
    ArrayList arrayList0 = new ArrayList
    for(Object object0: i.droppee_action
        Intent intent0 = new Intent(((St
        List activities_list = activity0
        if(activities_list.isEmpty()) {
            intent1 = null;
        }
        else {
            Intent intent2 = new Intent(
            ActivityInfo activityInfo0 =
            intent2.setComponent(new Com
            intent1 = intent2;
        }

        if(intent1 != null) {
            arrayList0.add(intent1);
        }
    }
```

PixPirate downloader function responsible for getting droppee launching activity

The PixPirate downloader doesn't exist in the Google Play Store, but it spreads through Smishing campaigns or a WhatsApp spam message from an infected user. In these cases, the victim is tricked into downloading and installing the downloader application. As it runs, the downloader prompts the target victim that there is an updated version of the application and asks for permission to install other untrusted apps, as a way to install the related PixPirate droppee.

## The new PixPirate campaign




PixPirate downloader function that runs and executes PixPirate dropped

In recent months, the Trusteer research lab monitored and detected a new campaign of PixPirate running in Brazil, and directly attacking Brazilian banks. At the time of this blog, PixPirate still primarily targets the Pix payment services that are integrated with most Brazilian banking apps.

In the current PixPirate campaign, Trusteer noticed the largest number of infections in Brazil (almost 70% of all infections), but with an additional reach that expanded to other markets in the world, including India and most recently Italy and Mexico. Outside of Brazil, India is the next-most infected country by PixPirate, with nearly 20% of the total infections in the world. Although no Indian banks appear in the PixPirate target list, the Trusteer research lab assumes the malware developers are laying the foundation for future campaigns in India. One assumption for the infection spread in India is the widespread use of India's Unified Payments Interface (UPI)

instant payment service. The UPI is utilized by hundreds of millions of consumers in India, where it has become the country's standard payment platform, and is regulated by the Reserve Bank of India (RBI).

## PixPirate droppee installation made easy

The newly identified PixPirate campaign also includes a new version of the downloader, which includes a link to a YouTube video that explains and demonstrates to the target victim how to unknowingly install the droppee Android package kit (APK) and grant all the necessary permissions and capabilities in order to fully execute on the victim's device. The YouTube video simulates a legit tutorial video explaining to the user how to install a legitimate financial service app, and to date has more than 78,000 views providing some scope of the infection's reach, assuming every YouTube viewer has followed through and unknowingly installed the PixPirate malware.

In the video, a user launches the downloader app for the first time, which simulates being a legitimate financial services application. The PixPirate downloader then asks the user to install an updated version of itself. Once the installation is complete, the victim has actually installed a new malicious application, rather than simply upgrading the downloader. This new app – the droppee app – is in fact the PixPirate malware. The PixPirate malware then remains incognito to the user by having no icon on the home screen of the infected device.

As discussed in the previous PixPirate blog, remaining incognito to the user has many advantages, including giving the PixPirate malware a better chance to sustain a long infection period with the ability to conduct financial fraud. However, this also introduces a problem – without an icon, the victim cannot "start" or activate the malware manually, so who will do it? That's where the PixPirate downloader comes back into play, as the resource that is responsible for running the malware. The previous Trusteer blog post described the innovative way the PixPirate downloader ran the droppee, but in this current campaign, Trusteer has detected a new way the downloader executes the malware, as described in the next section.



## New PixPirate droppee new execution method

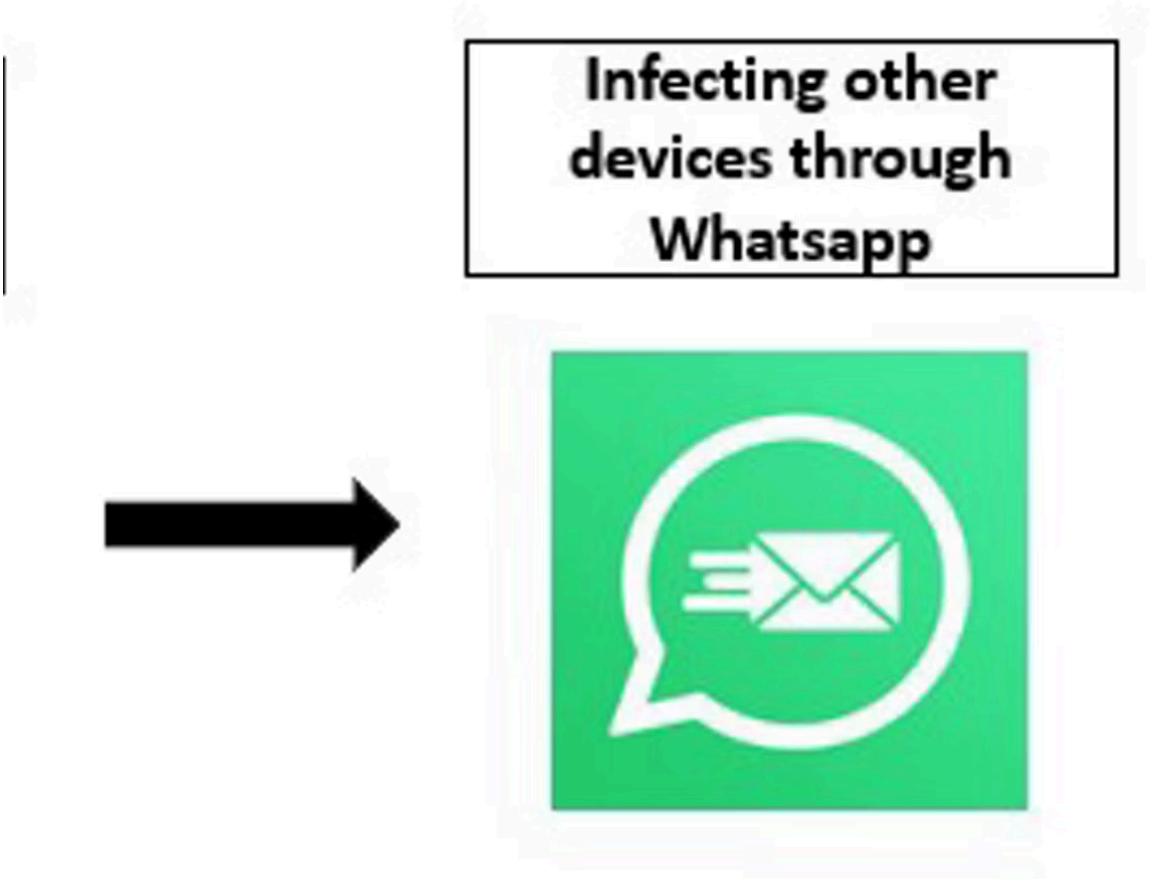
The previous Trusteer blog post assessed the method used by the PixPirate droppee to hide its icon and, as a result, the special technique used by the downloader in order to run the droppee. In the new PixPirate campaign, the downloader uses a new method for launching the droppee.

In the new method, the downloader maintains the execution role of the invisible droppee. The droppee holds in the manifest activity with an intent filter with one of the following unique action names:

- "com.ticket.stage.Service"
- "com.ticket.action.Service"
- "com.sell.allday.Service"

When the PixPirate downloader wants to run the correlated droppee, the first thing it needs to do is to get the droppee activity holding this specific unique action and the droppee's package name. To do that, the downloader uses the API "*queryIntentActivities(android.content.Intent, int)*" with an argument of the intent with the desired action name. This function retrieves a list of all activities that hold an intent filter for the given intent. It returns a list of "ResolveInfo" objects containing one entry for each matching activity.

We can see in the image below the function that is responsible for returning a list of all intents for all the activities of packages that contain one of the action names mentioned above. The PixPirate downloader starts with a for loop over a list of activity action names belonging to the PixPirate droppee using a call to the "*queryIntentActivities*" API. This API returns a list of "ResolveInfo" objects containing all activities with one of the droppee action names. For each "ResolveInfo" object returned it creates an intent with the corresponding activity name and package name and stores it in an array. This array is returned by the function.



PixPirate new infection methodology

In the following function, we can see in the for loop a call to the function “get_potential_droppee_packagenames” that is responsible for returning a list of all intents for all activities of packages that contain one of the droppee action names. Then, it validates that the package name related to the returned intent is really the droppee package. If so, it adds other relevant and necessary data to the intent and uses the “startActivity(android.content.Intent)” API to start the relevant droppee activity and perform the action of running the droppee.

## WhatsApp: Key player in PixPirate malware spreading technique

As part of the installation flow of PixPirate downloader on a device, the downloader checks to see if the WhatsApp instant messaging app is installed. The downloader contains in its “assets” folder the “WhatsApp” APK, so if the WhatsApp application is not installed on the victim’s device, the malware pushes the victim to install it.

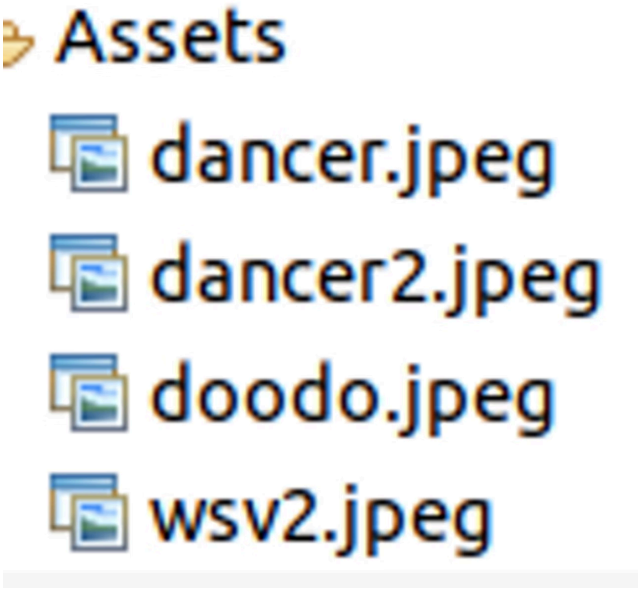



Figure 5: Downloader assets.

We can see in the image above the “assets” folder of the downloader APK, where “wsv2.jpeg” stands for WhatsApp APK. The other files are different versions of the droppee APKs.

Due to the size of the WhatsApp APK, we see the downloader is almost 100MB. Comparatively, the WhatsApp APK is abnormally large compared to other common finance malware downloaders that have relatively small code sections and little functionality, as they generally aim to only download and install the droppee (and not run them).

The PixPirate Droppee uses the WhatsApp app to send malicious phishing messages through a victim’s WhatsApp account with the intent to spread itself and infect other devices. The malware has the ability to read the contact list

of the victim, in addition to being able to add contacts, and then can send WhatsApp messages to a victim's contacts or even WhatsApp groups to further the spread and infect more users.

The new capabilities and functionality related to the WhatsApp app can include:

- Sending messages
- Deleting messages
- Creating groups and sending messages
- Reading and deleting the user contact list
- Adding and changing the user contact list
- Blocking and unblocking other WhatsApp user accounts

While the WhatsApp messages are sending, the PixPirate malware uses an overlay technique to hide the device screen, so the victim won't notice the malware is using the WhatsApp app.

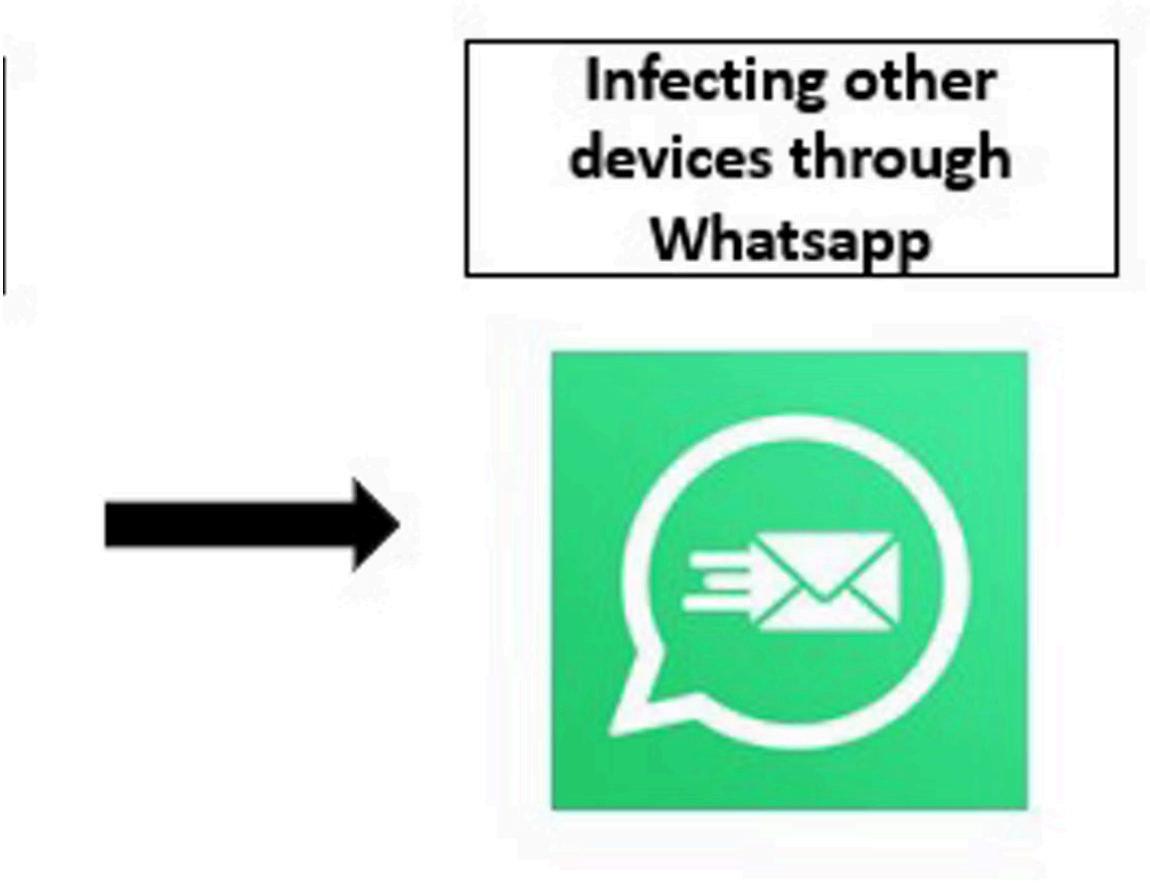


Figure 6: PixPirate new infection methodology.

It should be noted that sending WhatsApp phishing messages is an extremely effective tool for attackers to spread and infect other victims, for a couple of reasons:

1. WhatsApp messages look more legitimate and reliable than SMS messages. Smishing is an already well-known technique by fraudsters and attackers to spread spam and malicious content, and users are aware of those types of malicious threats. However, that precaution and awareness is not as pronounced with WhatsApp messages.
2. As opposed to smishing attacks, where the sender tends to be unknown to the victim which can raise their suspicions, messages received via WhatsApp are often sent from a known contact, which gives the recipient a false sense of security that the message is legitimate.

Using WhatsApp helps foster PixPirate infections and spread the malware to more victims and devices, even if they are not potential intended targets.

## Sending a WhatsApp message

In the image below, the PixPirate function that is responsible for sending WhatsApp messages from the victim account is clearly visible. Note that the function gets three parameters:

- Contact list – a list of contacts to send the malicious WhatsApp message
- messagesArr – array of messages to send
- sleepTime – time to wait between each message sending

The malware then uses the phone number from the victim's contact list and uniquely creates an intent where the data field contains the key for sending a WhatsApp message to the targeted phone number with the text it would like to send. In the package message, PixPirate sets the package name of the WhatsApp application ("com.whatsapp") and then it triggers the sending message action by starting the activity using the intent it just created.

```
mineRun = true
RunErr = 0
for (let phone_number of contact_list) {
  let index = Math.floor(Math.random() * messagesArr.lengt
  let msg_text = message_list[index]
  Data =
    'https://api.whatsapp.com/send/?phone=+' +
    phone_number +
    '&text=' +
    msg_text +
    '&type=phone_number&app_absent=0'
  msgHand = msg_text.substring(0, 4)
  try {
    let Intent = new android.content.Intent(Intent.ACTION_
    Intent.setPackage('com.whatsapp')
    Intent.setData(android.net.Uri.parse(Data))
    Intent.addFlags(android.content.Intent.FLAG_ACTIVITY_N
    context.startActivity(Intent)
  } catch (_0x52abe2) {
    XLog.r('wsMine', "Not whtasapp App or Can't startup th
    RunErr = 3
    JobUtils.syncUpdateJob(
      missionIDm,
      'whtasapp',
      phone_number,
      '□□□WhatsApp□□□□□',
      2
    )
    return
  }
```

Figure 7: Malware creating a WhatsApp message.

In the next image, after the message to be sent via PixPirate has been created, the malware locates the “send” button and it abuses the device’s Accessibility service to click on it, just like a human user would, to send the WhatsApp message to the intended recipients.

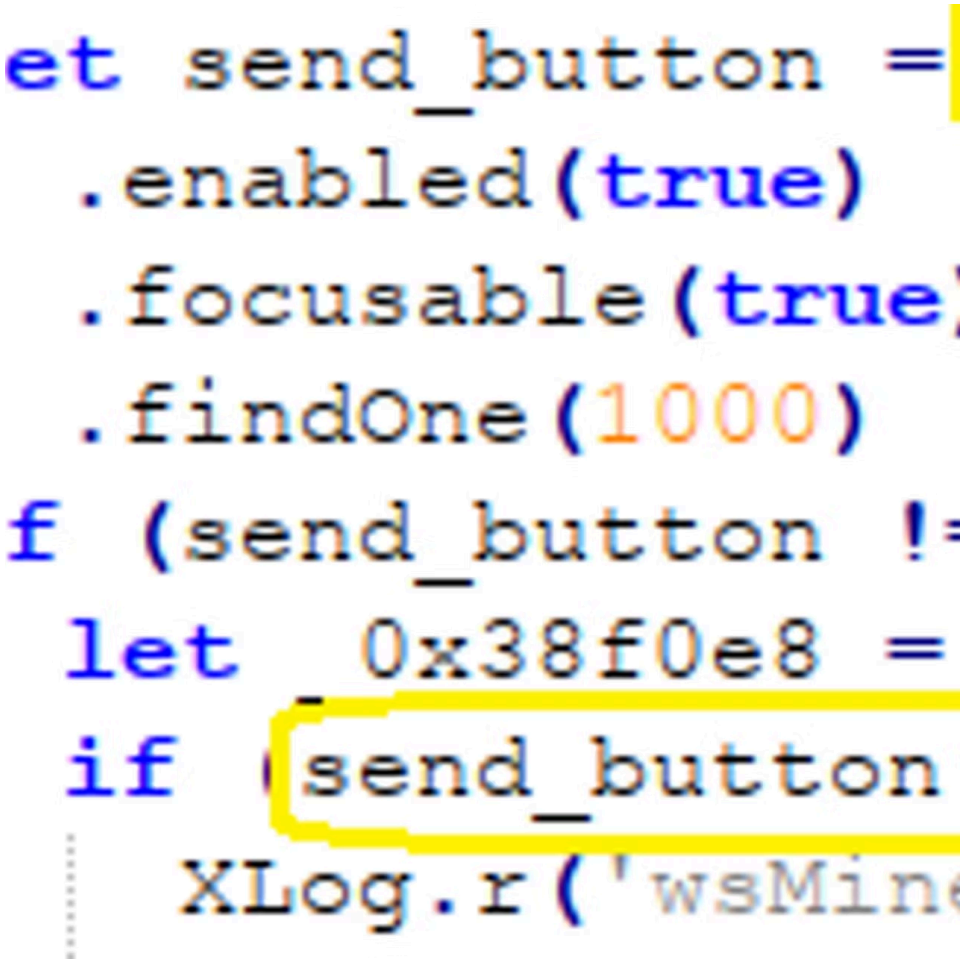



Figure 8: Malware sending WhatsApp message function.

## Summary

PixPirate is a dangerous remote access tool (RAT) malware campaign first seen in late 2021, but which has recently returned via a new campaign infecting users primarily in Brazil and India, with campaigns beginning to appear in Italy and Mexico. PixPirate's threats and malicious activities are based on the malware's unique accessibility capabilities, including being a RAT and having remote-control capabilities to ensure automatic fraud execution, theft of user data, spreading through WhatsApp messages, hiding and anti-removal, intercepting SMS, recording user activities and more. The malware also holds some anti-virtual machine (anti-vm) and obfuscation capabilities.

This latest iteration of the PixPirate malware also uses a new hiding technique to conceal its existence on the device, including hiding its icon on the home screen.

Early on in the malware's lifecycle, PixPirate was identified only in Brazil, targeting Pix payment services and Brazilian banks. Today, however, the new PixPirate version and campaign identified by Trusteer Lab has spread to other regions in the world, with a specific focus on India. Although Trusteer hasn't observed any Indian targets to date, our assumption is this is only the beginning of this heavily maintained malware, to the point that we may see PixPirate outgrow its name in the future.

## IOCs

Downloader SHA256: 1196c9f7102224eb1334cef1b0b1eab070adb3826b714c5ebc932b0e19bffc55

Droppee SHA256: d723248b05b8719d5df686663c47d5789c323d04cd74b7d4629a1a1895e8f69a

---