

BrasDex: A new Brazilian ATS Android Banker with ties to Desktop malware

Published: 2024-10-01 · Archived: 2026-04-05 12:45:50 UTC

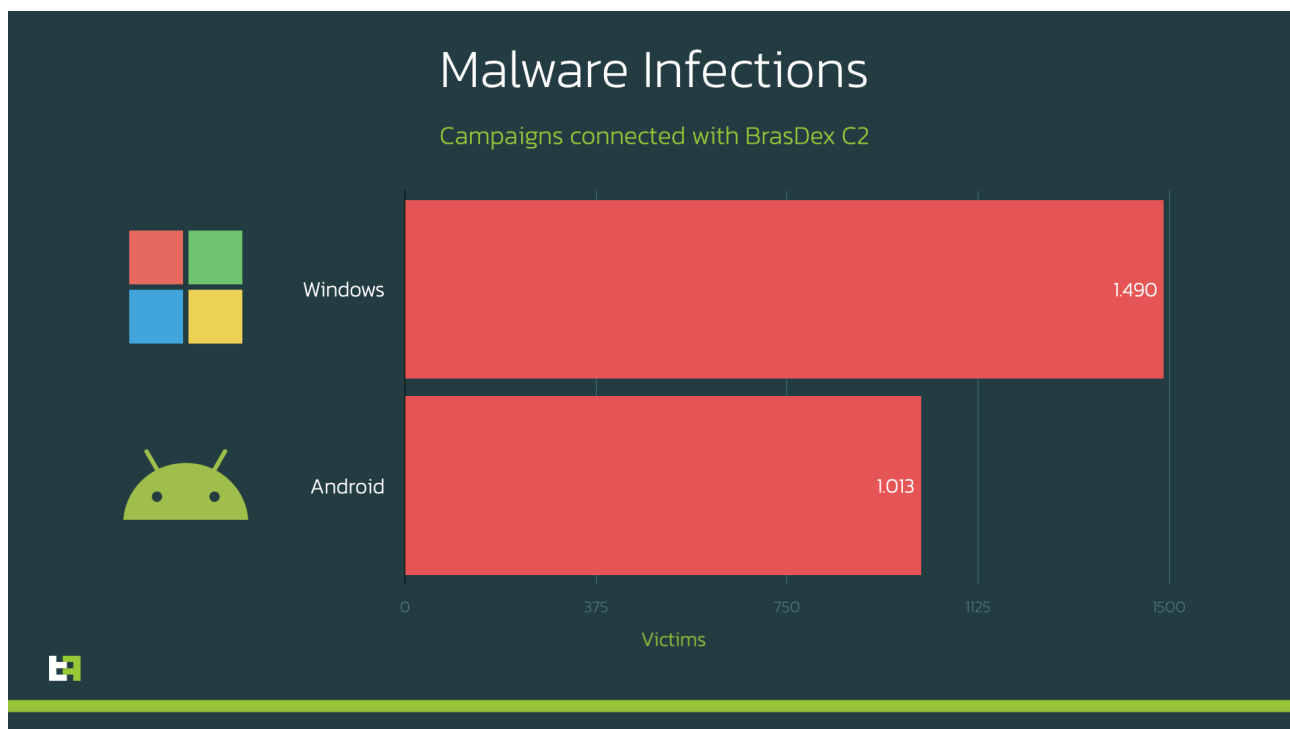
A varied and wild landscape

The mobile malware landscape of the LATAM region, more specifically Brazil, has recently risen to prominence in the news due to families like Brata and Amextroll, extending their reach all the way to Europe. [ThreatFabric has already reported in length about these families](#). However, not all malware developed in South America targets the European market.

In fact, ThreatFabric analysts discovered an ongoing multi-platform malware campaign, targeting both mobile and desktop Brazilian users, with thousands of infections and with an **estimated loss of hundreds of thousands of Brazilian Reals (R\$), which corresponds to tens of thousands of USD**.

This campaign involves a highly flexible novel Android malware dubbed **BrasDex** by ThreatFabric, featuring a complex keylogging system designed to abuse Accessibility Services to extract credentials specifically from a set of Brazilian targeted apps, as well as a highly capable Automated Transfer System (ATS) engine.

When analyzing BrasDex, our team found the evidence of some desktop malware controlled through the same backend. Our analysts were able to identify the malware samples related to the same campaign targeting Brazilian users as well: it involves [Casbaneiro](#), a well-known malware family known to be active in Latin America.

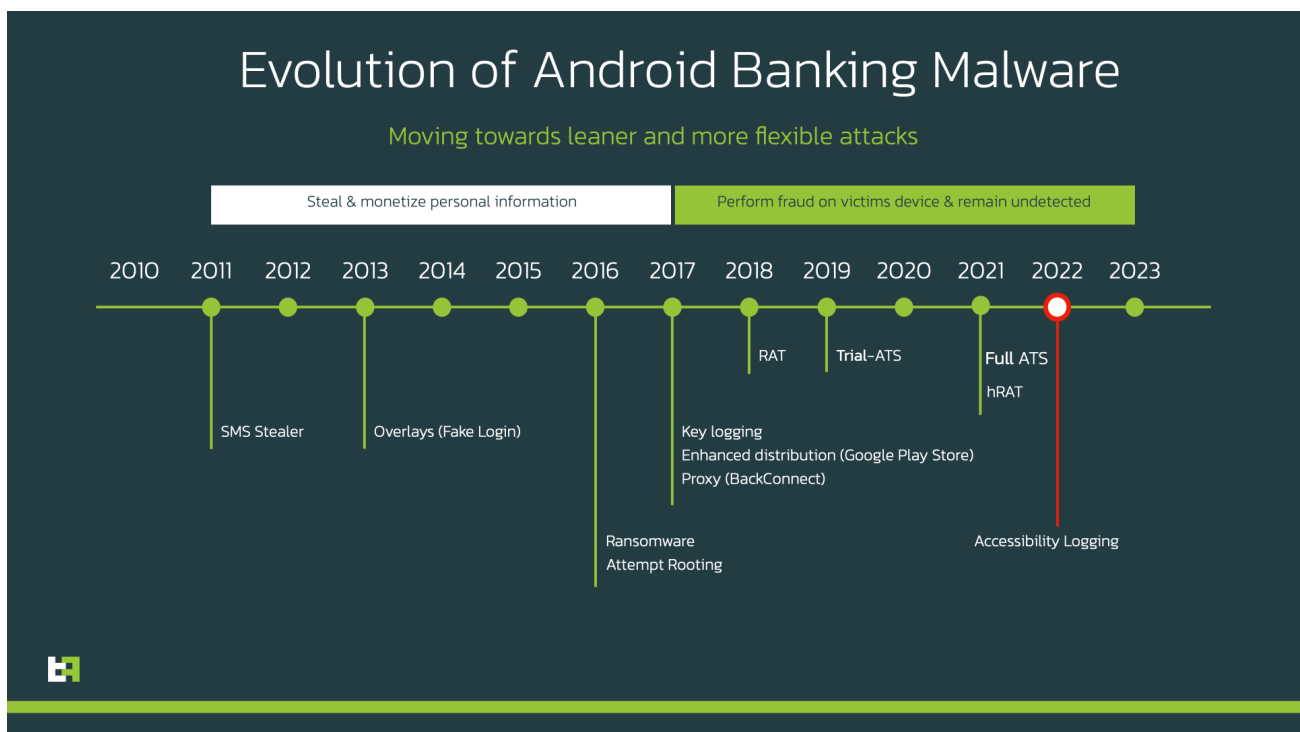


BrasDex: a trend switch away from overlay attacks

The malware has been active for more than a year, initially posing as Android settings applications and targeting Brazilian banking applications. In its latest campaign, it started posing as one specific Banking application (Banco Santander BR), but continuing to target the same subset of applications as its previous versions.

BrasDex abuses accessibility services to keylog the information that is input in the target application, veering away from the traditional overlay attack mechanism that we have observed for years now, towards what seems to be the next standard in Android banking malware.

This follows a trend that we have started to see in the past year, where different malware families have started abandoning the use of overlays, which require continuous update and additional downloaded data, in favour of more lean and flexible solutions. For example, in the case of Vultur this solution was to perform screen-recording and subsequently accessibility logging, in the case of Cabassous it was to load the real target login page in a browser controlled by the malware, with JavaScript enabled.



However, in most cases, malware families are starting to rely heavily on accessibility logging to exfiltrate logging credentials and other PII from infected victims. This is also the case for BrasDex. This malware family is able to log not only credentials, but also other important information, like account balance, and then use it to perform a DTO (Device TakeOver), which allows criminals to perform fraudulent transactions using the infected device.

What sets BrasDex apart from many other malware families is its ATS (Automated Transfer System) capabilities. ATS allows malware to programmatically use the information stolen from the victim to initiate fraudulent transactions in an automated way, making the whole infection and fraud chain more flexible and scalable.

ThreatFabric has mentioned ATS before in our blogs, as one of the most dangerous features present in modern day malware, specifically when speaking about Bankers such as Gustuff, the first Banker to implement this technique in 2018, and more recently SharkBot.

Targets

BrasDex is a malware family strictly focused on the Brazilian market. The malware contains checks to make sure it only operates on devices from Brazil. To do so, it programmatically checks that the SIM used by the device is operating in Brazil, and only then it properly completes its operations and configurations. If the device has a SIM card from anywhere else, the malware shuts down and never contacts its C2 server.

This hard complete dedication to a single market might be motivated by the fact that BrasDex uses its features to abuse one specific subset of transactions within the Brazilian banking ecosystem. BrasDex specifically abuses the [Pix payment system](#). Pix is a fast payment system from the Central Bank of Brazil that went live in 2020, and allows users to perform payments to other users just by knowing their identifier (which can be an email, CPF, phone number, or random ID).

NOTE: ThreatFabric wants to point out that the Pix system is not vulnerable. Actors are not exploiting any vulnerabilities in the Pix System, but rather abusing the fast payments system and Android known issues to make fraudulent transfers

Pix Payment System

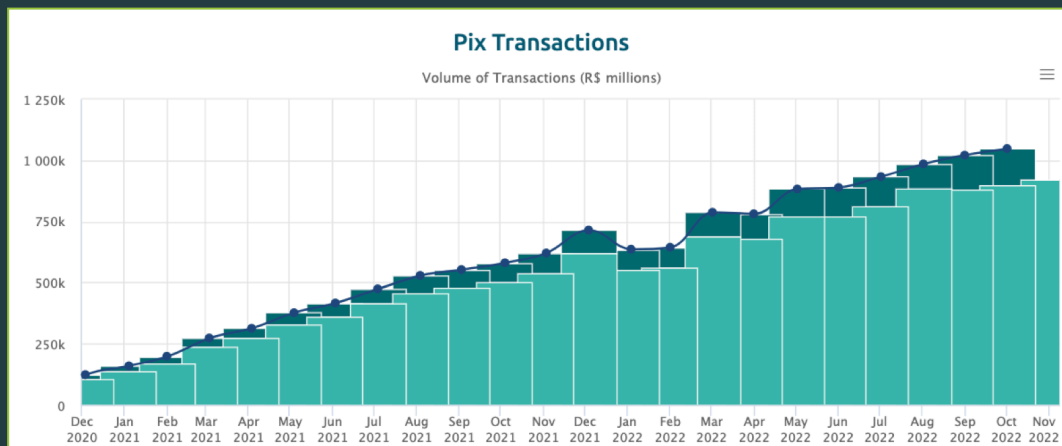
Developed by Banco Central do Brasil



Bloomberg referred to the Pix app as “ubiquitous” in Brazil in October 2021, a year after Pix’s release. As of November 2022, Pix has been reported to perform an average of more than 2 million monthly transactions, with a user base of more than 120 million people. **Only in November 2022, Pix was used to perform transactions corresponding to a volume of more than one billion Brazilian Reals (R\$), which equals to more than 180 million USD (\$).**

Pix Transactions

Data from Banco Central do Brasil



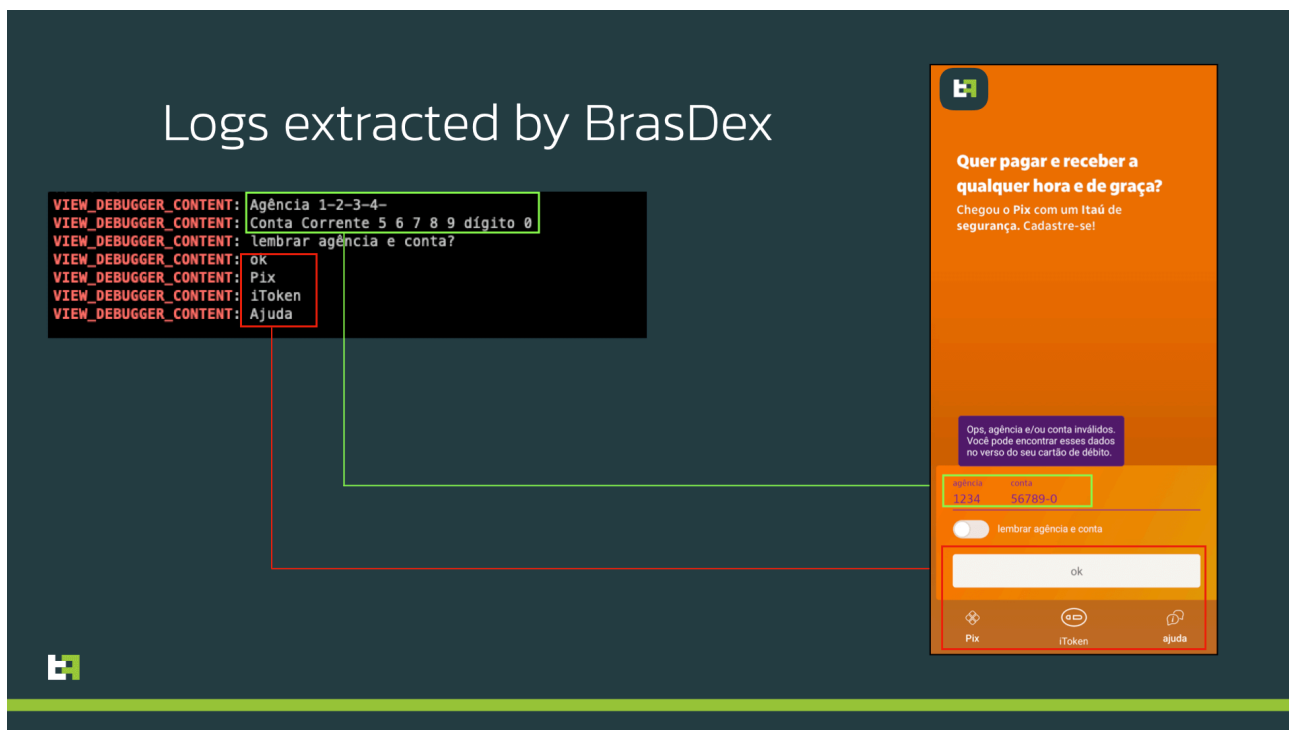
For each targeted bank, the step in the ATS script which is responsible for the actual fraudulent transfer performs it through the Pix technology, not the traditional bank transfer that many other malware families use.

The script will find the UI element corresponding to Pix payments within the banking application, use it to start the transfer procedure, and then navigate through the different screens, selecting the beneficiary and the amount, authenticating with the stolen credentials. This kind of instant payment does not require Multi Factor Authentication, as it can be authorized directly through the banking application itself, making it the perfect target for an Android Banking Malware. We will later cover in detail an example of a transfer procedure with such technology.

Capabilities

Keylogging

The keylogging technique used by BrasDex abuses the accessibility services privileges, and is able to detect and log a large quantity of information from the Operating System. With this technique, BrasDex is able to log and send to its C2 all the information that is shown on the device's UI, including both credentials typed by the user, as well as other information that is displayed by the application itself, like account balance.



If the application on the foreground is one of the banking applications included in the target list, BrasDex also notifies its C2 of events such as opening the application, inserting passwords, or if the malware is incapable of extracting the required information. The malware notifies the C2 whenever one of the following events is detected, with the indicated codes:

Event Code	Description
	(No code) The malware successfully performed a transaction
START	The banking application was started
PW	Password typed (followed by the password as event value)
STUCK	The malware encountered an error and is frozen
ABORT	The malware aborted its operation for lack of permissions or outdated APIs

The logged message is formed in the following way (in case of no parameters, the message ends with the event code):

FORMAT: < BANK_CODE > - < EVENT_TYPE > - < EVENT_VALUE > - - - - -

The information that is collected by the keylogging module is stored locally and sent to the C2, and is automatically fed as parameters into the ATS scripts downloaded with the malware configuration when the malware is first launched.

ATS

What really sets apart this newly discovered malware family from its competition, is its advanced and flexible ATS framework. First abused by Gustuff, enhanced and diffused with SharkBot, Automated System Transfer allows the

malware to programmatically use the stolen credentials, detect the amount of funds that are available in the account, and then initiate and approve a transaction, all from the infected device itself.

In the case of BrasDex, the infected device receives multiple scripts, one per targeted application, and each containing all the necessary steps to login and perform fraud. Each script is made of multiple actions, which contain the following fields:

```
{
  "stageId": n,
  "conditions": ["<Condition>-<Parameters>", ...],
  "run": ["<Command>-<Parameters>"...]
}
```

- **stageId** is an integer number which corresponds to the current step of the script. Actions are executed in consecutive stageId numbers and scripts feature multiple actions with the same stageId, in order to support multiple alternative execution patterns (e.g. different login procedures based on the kind of PII exfiltrated).
- **conditions** is a list of “Condition-Parameters” combinations. These make up the conditions required to initiate the actions.
- **run** is a list of “Command-Parameters” combinations. These are the actual actions executed by the malware.

Here is an example of a real action implemented by one of the scripts:

ATS Action

```
{
  "stageId": 1,
  "conditions": [
    "getCounter-blc,1",
    "getCounter-once,0",
    "isNum-text"
  ],
  "run": [
    "setBlc-text",
    "addCounter-once,1"
  ],
},
```

IF

- Counter "blc" = 1
- Counter "once" = 0
- Field "text" is a number

DO

- Set Blc to the value of "text"
- Add 1 to Counter "once"

BrasDex is **able to check for values and type of data contained in all the different fields of the UI** (for example if an account contains any funds). It is also able to understand and check if UI elements can be clicked, and if they contain specific strings used to identify useful information (like finding the “Continue” or “Cancel” button).

If the conditions for an action are satisfied, it also able to navigate within the UI to highlight and focus the wanted elements, wait a set amount of time, assign specific values to password fields or beneficiary fields, click buttons within

the app.

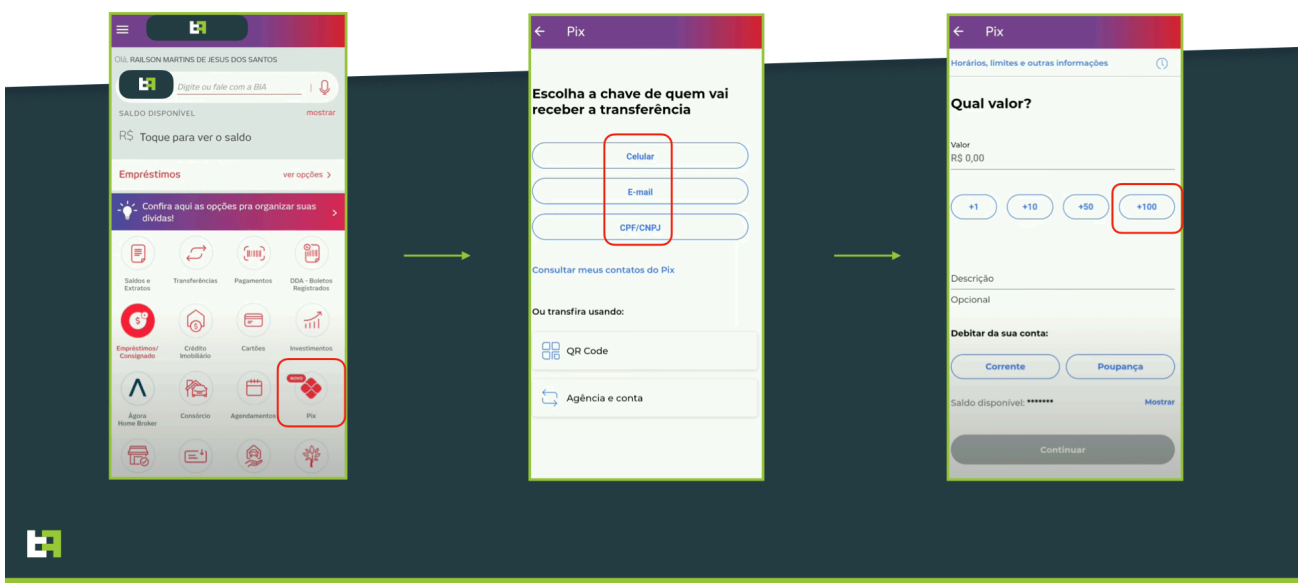
In the [Appendix of this blog](#), you can find the full list of accepted conditions and commands supported by the bot.

Pix Transfer example

As previously mentioned, BrasDex targets the **Pix payment** system to perform its fraud.

In the image below you can see a few of the different screens that the malware needs to navigate and interact with to successfully perform a successful transaction using Pix.

Transfer using Pix



We report here a subset of the actions described in the ATS script, which interact with the UI elements highlighted in red in the above image:

```
{
  "stageId": 2,
  "conditions": ["textC-Pix. Item"],
  "run": ["clickCurrentNode"]
}, {
  "stageId": 3,
  "conditions": ["textCL-cpf", "acc-CPF"],
  "run": ["clickCurrentNode"]
}, {
  "stageId": 4,
  "conditions": ["textC-+100", "className-Button"],
  "run": ["next", "BRASetVal"]
}
```

As you can see from the above JSON objects, BrasDex in this case transfers funds to an account identified by a CPF code (“Cadastro de Pessoas Físicas”, a unique individual taxpayer identifier in Brazil).

This is another peculiarity of Pix: it allows to perform transactions to **accounts which can be identified by CPF, but also phone numbers, emails, or simple unique identifiers**. The ATS scripts uses the following codes to identify which kind of mule it will be using for the transaction (which is communicated by the C2 during its initial config):

Destination Code	Description
CEL	Phone number
EMAIL	Email address
CPF	Cadastro de Pessoas Físicas

All kinds of accounts identifiers have been observed being used by BrasDex mules.

Once the malware finally inputs the necessary passwords to finalize the transaction, funds are transferred to the destination mule account.

Panel

While investigating this malware family, ThreatFabric also managed to get certain visibility of the Panel hosted on the C2 server. Based on the information displayed on the panel, the malware seems to be quite successful, more than a thousand of reported infections. The panel contains multiple pages, e.g. the list of infected devices with extensive information, which includes the service providers, the device model, and the Android version. In another page, actors can access logs obtained from the infected devices, with the exfiltrated information, as well as reports of successful transactions.

However, what really caught our attention was the main landing page. Here, we found a dashboard reporting extensive information about a different malware campaign, only this time targeting Desktop devices.

BrasDex Panel

InfosContador

Painel Infos - 2022 by Dark Seja bem vindo

1.0 Última versão	0% % Máquinas com Plugins	8 Total de Casas	1490 Total de Clientes
-----------------------------	-------------------------------------	----------------------------	----------------------------------

Id	Data	Versão	IP	UserName	ComputerName	OS Version	Casa(s)	AV	ISP
1	08/09/2021	1	Brazil, Sao Paulo, São Paulo	[Redacted]	[Redacted]	Microsoft Windows 10 Pro (64)bit		Windows Defender	Vivo
2	9/8/2021	1	Brazil, Minas Gerais, Belo Horizonte	[Redacted]	[Redacted]	Microsoft Windows 10 Enterprise		Windows Defender	Claro S.A.

This discovery led to another investigation, which allowed us to connect this malware family to another malware family: **Casbaneiro**.

Casbaneiro: old but gold

The analysis of the drop points used to distribute BrasDex led us to a campaign of desktop samples distributed through similar links in Q1 2022. We analyzed those samples and identified Casbaneiro, infamous Windows banking Trojan discovered in 2018, as the partner of BrasDex.

Since the campaign is quite old, it could be just a coincidence, but our analysis showed clear similarity between BrasDex and Casbaneiro in regards to the communication with their C2 (namely the common use of a specific header).

However, to put an end to the debate, while writing our blog we discovered an ongoing campaign of BrasDex and Casbaneiro distributed through the same drop point, thus allowing us to conclude that Casbaneiro is the a desktop malware operated by same actors behind BrasDex.

The latest desktop campaign is the same in MO as previous ones, and we will briefly highlight the most notable parts of the desktop campaign.

It was delivered through **phishing e-mails** about a failed delivery, pretending to be from the Brazilian postal service and containing a link to a form to be filled in.

Phishing e-mail

Casbaneiro distributed through e-mails impersonating postal service



When the victim clicked the link, a ZIP archive was downloaded. This archive contained a Microsoft Software Installer package (MSI). When analyzing the file, we discovered that it contains an obfuscated script that will download the next stage of the malware.

Casbaneiro is a Windows banking Trojan written in Delphi that targets users of online banking as well as users of desktop banking applications. It is able to collect the data about the infected device, take screenshots and perform keylogging, hijack clipboard data, etc.

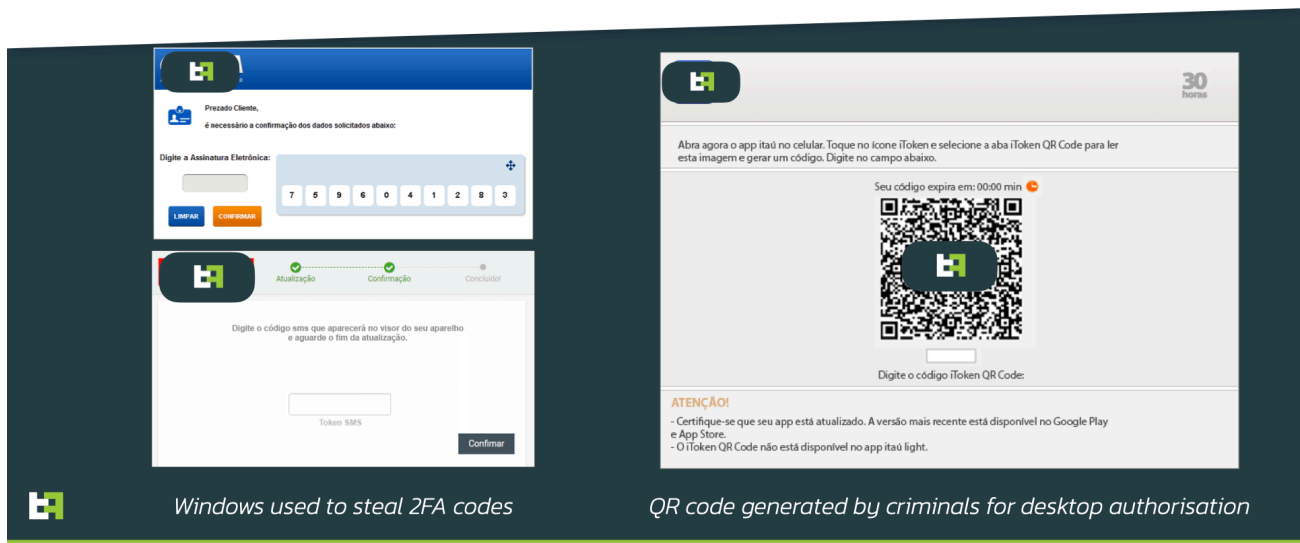
The following Bitcoin wallet is hardcoded in Casbaneiro to be used to replace a cryptocurrency wallet copied by victim in clipboard:

```
bc1q23dsv7wnngxj3prwjdegk9e2j6c4rs39qg86xk
```

When running, Casbaneiro monitors the launched processes and opened URLs to find those related to banking applications. It also downloads bank-specific pictures from Google Drive, and uses them to steal 2FA codes from victim. This last step is done to authenticate to banking application on the actors' device. For one of the banks such pictures contain QR-codes generated by the actors; the victim is tricked into scanning them with the mobile banking application and as a result, a new desktop device (controlled by cyber-criminals) will be authenticated and will have access to victim's banking account.

Phishing screens

Multiple templates to steal 2FA codes



Conclusion

Being independent and full-fledged malware families, BrasDex and Casbaneiro form a very dangerous pair, allowing the actor behind them to target both Android and Windows users on a large scale.

Moreover, the appearance of convenient payment systems not only makes payments comfortable for customers but also opens an opportunity for cyber-criminals to use it for fraudulent operations. The BrasDex case shows the necessity of fraud detection and prevention mechanisms in place on customers devices: fraudulent payments made automatically with the help of ATS engines appear legitimate to bank backends and fraud scoring engines, as they are made through the same device that is usually used by customer. Thus, a proper solution is needed on the very first border to identify suspicious behavior during the transaction combined with visibility of threats present on customer's devices.

Fraud Risk Suite

ThreatFabric's Fraud Risk Suite enables safe & frictionless online customer journeys by integrating industry-leading mobile threat intel, behavioral analytics, advanced device fingerprinting and over 10.000 adaptive fraud indicators. This will give you and your customers peace of mind in an age of ever-changing fraud.

Appendix

BrasDex Samples

App Name	Package name	SHA256
GoogleDocs XML APK	com.mydocs.documents	7747a9912e2605b64430a27e3c5af3556c26b4cb04c7242ca4e2cad5b6b33363
GoogleDocs XML APK	com.mydocs.documents	26ea3906cd0c724b0e0adb5b6c00144e59aa89aac18cd608c6e5a22c28c8d644
Santander Atualização	com.mydocs.documents	b549733ed3b77d97c7b2f9f651f22abc4df50899c01612a28ec6809d1a2c0040

BrasDex C2

Url
brasdex[.]com

BrasDex Targets

Package name	Application name
com.picpay	PicPay: Pagamentos, Transferências, Pix e Cashback
com.itau	Banco Itaú: Gerencie sua conta pelo celular
com.nu.production	Nubank
com.bradesco	Bradesco
br.com.gabba.Caixa	CAIXA
com.santander.app	Santander Brasil
br.com.original.bank	Banco Original
br.com.intermedium	Inter: conta digital completa
br.com.bb.android	Banco do Brasil
com.binance.dev	Binance (not fully developed ATS Script)

BrasDex Conditions

Conditions	Description
enabled	Is enabled
textEqL	Text is equal (lowercase)
prevNodeDescC	Previous Node Description contains string s
descCL	Node Description contains
descEq	Node Description equals
prevNodeTextC	Previous Node Description contains
getBlc	Get balance value
prevNodeTextEqL	Previous node text equals (lowercase)
textCL	Text contains (lowercase)
textEq	Text equals
getChildsChildDesc	Get description of child of child node
getChildsChildText	Get text of child of child node
isClickable	Node is clickable
clickNodeVerify	Click node passed as parameter
getChildDesc	Get child node description
getChildText	Get child node text
className	Get className
acc	Check type of account (EMAIL,CPF,CEL)
blc	Check balance
clickNodeParentVerify	Click parent node
isParentClickable	is parent node clickable
descC	Description contains
hintC	Hint contains
isNum	Is number
noBlc	Check if no balance
textC	Text contains

Conditions	Description
disabled	Is disabled
resName	Get view id resource name
prevNodeDescCL	Previous node description contains lowercase
prevNodeDescEq	Previous node description equals
prevNodeTextCL	Previous node text contains lowercase
prevNodeTextEq	Previous node text equals
getCounter	Get saved value of specified string
clickCurrentNodeVerify	Click current node
isStuck	Check if engine is stuck on some action (100 secs)
getNodeListSize	Get node list size

BrasDex Actions

Actions	Description
BRASetVal	Set value for com.bradesco
clickNode	Click node
addCounter	Create/add new counter
ORISetVal	Set value for br.com.original.bank
template	Set colors for template to overlay
finish	Finish execution and send data to c2
addNode	Add node to node list
clickNodesParent	Click nodes parent
clickCurrentNode	Click current node
return	Stops recursive search in nodes
setAcc	Set account
setBlc	Set balance value (from either text or description)
NUSetVal	Set value for com.nu.production
INTSetVal	Set value for br.com.intermedium
clickCurrentsChildNode	Click current node child

Actions	Description
CXSetVal	Set value for br.com.gabba.Caixa
SetPwCharAt	Set password char by char
act	Give accessibility focus to the node
back	Press back
home	Press home
next	Press next
wait	Wait set time
setPw	Set password value
increaseCounter	Increase specified counter by one
logTemplate	Present window to log specific data
SANSetVal	Set value for com.santander.app
focusCurrentNode	Get action focus to the current node
recents	Press recents
setBlcBB	Set balance value for banco do brasil bank
ITASetVal	Set value for com.itaú
focusNode	Get action focus to the specified node
sleepTolerance	Set sleep tolerance before aborting
setBlc2	Set balance value (from either text or description)2
setText	Set Text

Casbaneiro samples

SHA 256
5a3b2128c550829ab357abd7c830506df73893e204a8e2578fc1e61a72de3df5
519d76eb6fea8b1a699c3a543b5f5eafab883ed92f6d207b8fa0189482b72ba1

Source: <https://www.threatfabric.com/blogs/brasdex-a-new-brazilian-ats-malware.html>