Sucuri Blog

blog.sucuri.net/2021/01/real-time-phishing-kit-targets-brazilian-central-bank.html

Luke Leal January 14, 2021

We recently found an interesting phishing kit on a compromised website that has QR code capabilities, along with the ability to control the phishing page in real time. What our investigation revealed was that attackers were leveraging PIX, a new payment method created by the Brazilian Central Bank.

Features & Context for PIX

PIX was created and introduced to replace Brazil's old and deprecated transfer methods TED and DOC. PIX's new functionalities made it significantly cheaper and faster for transactions to be completed, allowing transfers to be conducted any time of the day, including weekends — functionality not available in the older, deprecated methods.

Marketed as easier and faster than TED or DOC, PIX allows Brazilian users to pay for items by scanning a QR code. It also includes lower processing rates for merchants in comparison to traditional payment card methods.

To pay with **PIX**, one of the following must be provided: **scan the recipient's QR code** or know the **person's key**, which can be their **cell number**, **social security number**, **email** or a **random key**.

Phishing Kit Details

The phishing kit targets Banco Itau Empresas (business) customers that use ***Itaú Internet Banking***.

This is important, because it comes with increased security requirements like:

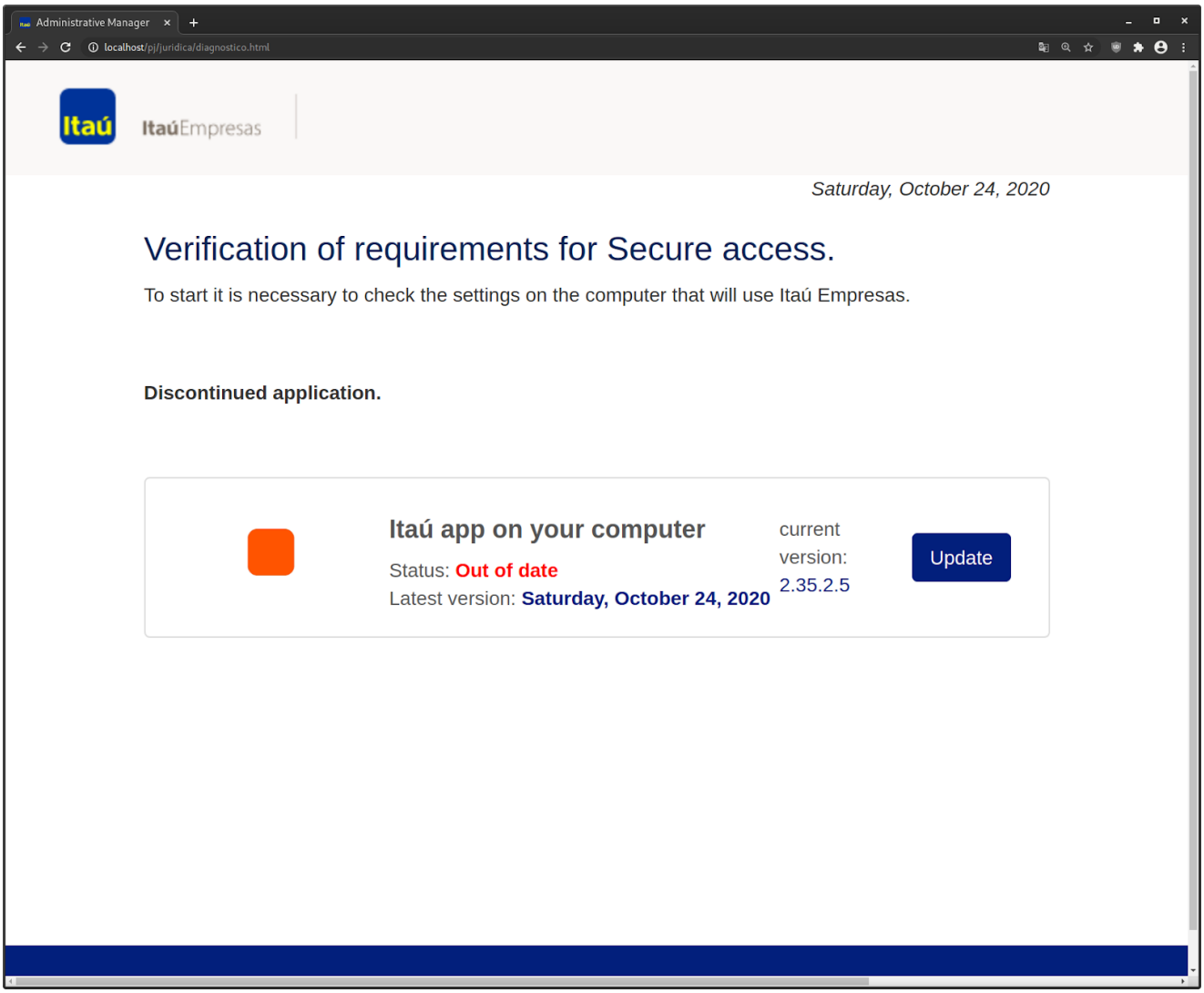
> Download the application in the case of the **Itaú App on the computer** or **Guardião 30 horas**
>
> Unlock / enable the application and **Itoken Itaú**
>
> Register a **six- to eight-digit electronic password** to be used both when **accessing the** application, **website** or Itaú customer service phones

When targeting these types of accounts, the biggest hurdle for the attacker is that a special application must be installed and authenticated prior to log in.

So, how does the attacker convince the victim to enter their banking account information outside of the **Guardião 30 horas** special security application?

Phishing Lure

To convince the victim, the attacker uses a fake diagnostics page that pretends to check if the victim has the **Itaú app** installed for secure access to their banking account. It then alerts the victim that their **Itaú app** is out of date and must be updated to the latest version.



Google translated to English.

Once the victim clicks the blue **Update** button, they are redirected to a second page designed to mimic the legitimate banking login page.

Attacker Real-time Control Capabilities

The most notable part of this phishing kit is that it grants the attacker real-time control over the phishing page's actions. This is accomplished through **PHP sessions** — whenever the victim is on the page, requests are submitted every five seconds.

These continuously generated requests use **AJAX** (**asynchronous JavaScript**) which allow the phishing page to receive a response from the attacker's phishing kit (**opera.php**). The response from the kit to the generated **AJAX** request contains **JSON** encoded data which changes the phishing page's actions *asynchronously*, meaning no page reload is necessary from the victim.

Naturally, there will be some time between the input of sensitive data and the phishing page receiving its next action.To provide a less suspicious experience, the phishing page shows the bank's standardized loading GIF image to appear as if it's loading something — in reality, it's just waiting for the attacker to tell the phishing page what to load.

The fake "carregando" loading screen waiting for attacker's command.

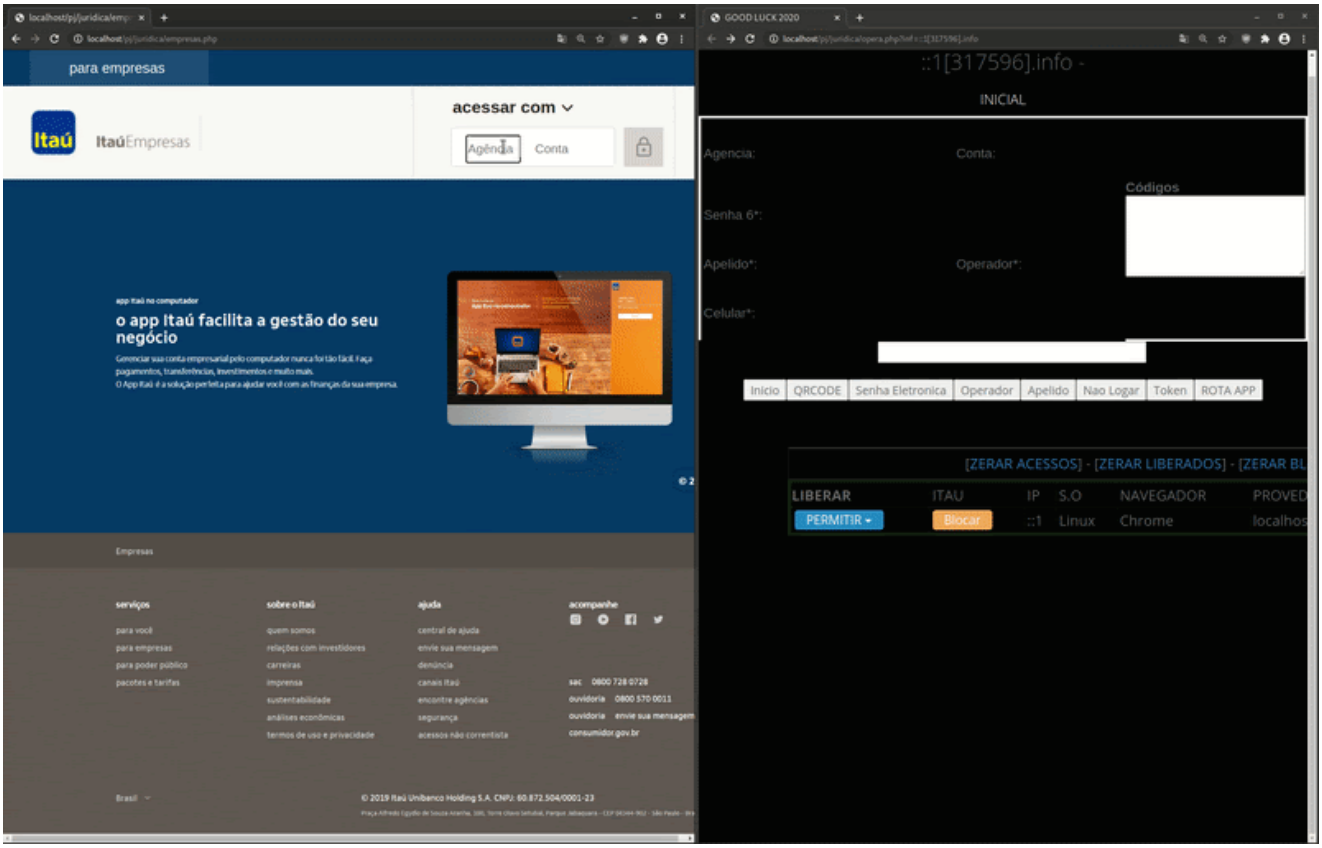
This is also reflected on the attacker's phishing panel. The text **AGUARDANDO** (translates to "waiting for") is displayed next to the victim's IP address whenever the fake "carregando" loading screen is being shown on their browser:

Panel shows a localhost IPv6 address (::1) along with a session number ([317596]).

Phishing Behavior: Login Credentials

I've included a GIF split screen below to demonstrate the behavior and experience for both the victim and the attacker.

On the left browser, I act as a victim on the phishing page. On the right, you can see the attacker's viewpoint.



As seen in this GIF, the victim first inputs their **Banco Itaú** login data (***agencia*** and ***conta corrente***), which are two separate numbers located on their banking payment card.

Afterwards, the fake "*carregando*" loading page (loaded in English) is shown to the victim — but, on the attacker's side they can now see the victim's login inputs ***agencia*** and ***conta corrente.*** They then instruct the phishing page to ask the victim for the ***Senha Electronica*** (electronic password).

Phishing Behavior: Passwords & QR Codes

The ***Senha Electronica*** (electronic password) is a six-digit PIN-style password that allows access, query, and transaction authentication for **Itaú** Electronic channels (internet, mobile and telephone). In addition to this password, the kit allows the attacker to request other sensitive information including the associated **cellular phone number**, **iToken**, **owner's name** — as well as a **QR code**.

Unfortunately, the file responsible for generating the **QR code** — **qrcode.php** — had already been deleted so we could nott fully replicate it, but **Itaú's** support page provides more context about its purpose:

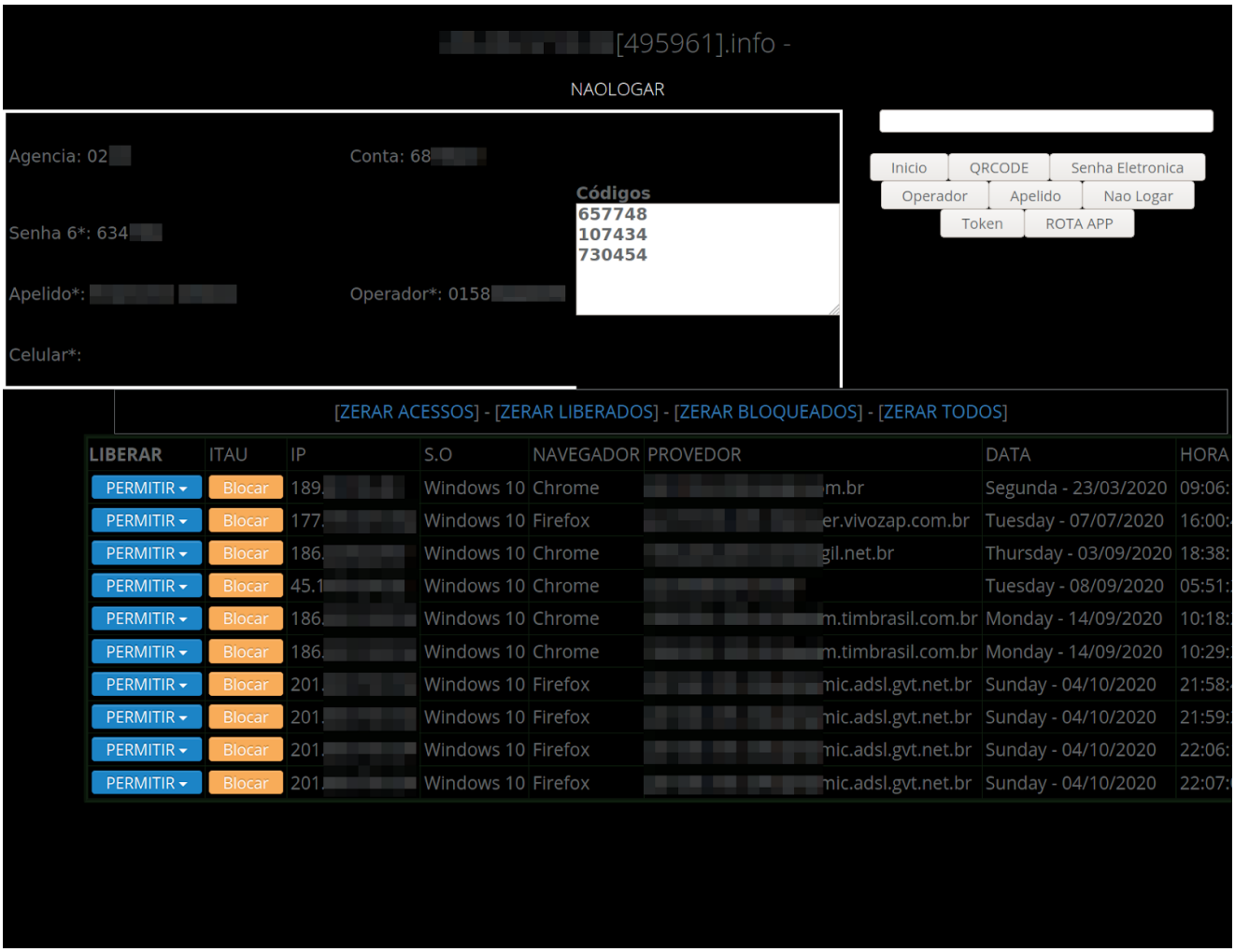
I already have iToken on my cell phone and I want to unlock the Itaú app on my computer. How do I do that?

First, download the Itaú Empresas app on your computer and choose the app on your phone as a way to unlock it. Then, click on "**generate QRCode**".

Now, open the app on your phone and, without accessing your account, click on the "iToken" icon. Then, go to the QRCode tab and point the phone's camera at the code that was generated on the computer. Your phone will display a six-digit code. Now just type these numbers on the computer and confirm. Ready! You can now use the app on your computer.

This feature essentially allows the attacker to use any stolen credentials to request a QR code from **Itaú**. Once the QR code is obtained, they can send it to the victim via the phishing kit for them to scan with their phone's **Itaú app**. This generates a code that the victim types and sends to the attacker, who can then enter it on **Itaú's** legitimate website as if they were the account owner.

Phishing Panel Features



Attacker's view of the phishing panel.

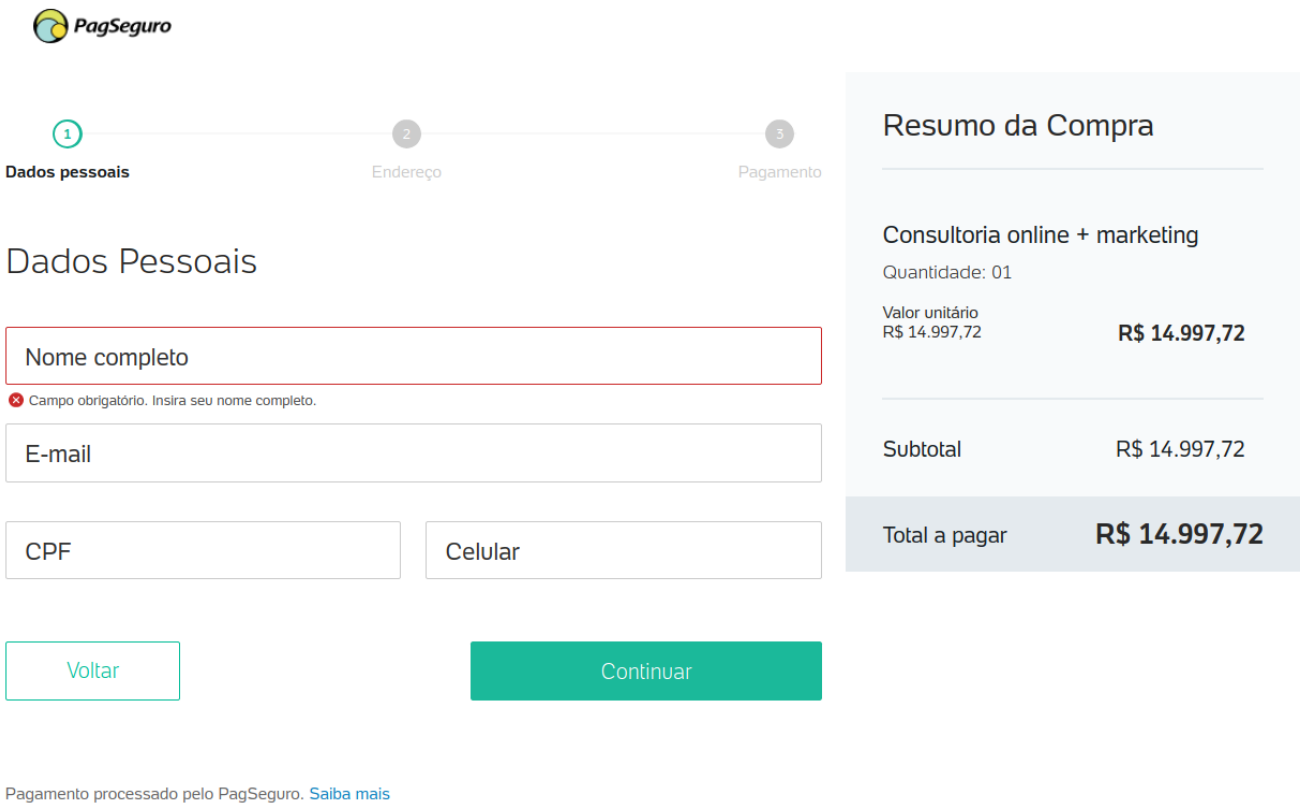
The attacker's phishing panel contains all of the options that are needed to carry out this phishing attack, categorizing the stolen data by IP addresses.

The attacker has the option to allow or block IPs, as well as submit commands to the selected victims phishing page through HTML buttons. For example, the Apelido button is used to request the victim's nickname. The ***Inicio*** button starts/resets the victim's PHP session. If this isn't button isn't activated by the attacker, then the victim will stay at whatever action was last used on the phishing page — even if they refresh it.

HTML Page Reveals Payment Requests

In addition to the phishing kit, we also located a file named **pagamentos.html** which contained some interesting information.

When pressed, the **PagSeguro** button loads a new tab with a shortened URL **pag.ae** (not a malicious website) used to send invoices to request payment from others. This invoice is requesting payment of **$14,997.72 Brazilian reals** for online consulting and marketing services, approximately $**2,830.08 USD** at the time of writing.



I'm not sure if the attacker tricks the phishing victim into paying this invoice or if the attacker logs into the victim's banking account and pays it that way. There wasn't any code referencing this file, so it's hard to say exactly how it was leveraged.

What is certain, however, is that these types of phishing campaigns can have serious implications for victims — and website owners. Phishing is typically challenging to detect because malicious pages are often hidden deep within file directories. Unless you happen to identify the exact URL of the malicious page, it can be tough to identify if your site was hacked.

One trick to detecting malicious behavior is to use Google Search Console, which may notify you about phishing and other security issues. File integrity monitoring and server-side scanners can also help identify any indicators of compromise in your website's environment.

If you think your website is hosting malicious content or phishing pages and you need a hand tackling the infection, we can help.