Hackers are again attacking Portuguese banking organizations via Android Trojan-Banker

seguranca-informatica.pt/hackers-are-again-attacking-portuguese-banking-organizations-via-android-trojan-banker/

April 15, 2020

Hackers are again attacking Portuguese banking organizations via Android Trojan-Banker.
The threat is not new, hackers are again attacking clients of Portuguese banking organizations via a specially crafted Android Trojan-Banker from phishing campaigns launched from Brazil.

The last occurrence this line was recorded on March 13rd, 2020, where a similar Trojan-Banker was disseminated targeting other clients of different banking organizations.

List of some baking campaigns this Brazilian threat group has performed in Portugal:

13/03 – **Novo Banco Trojan-Banker**
12/03 – **Caixa Geral Depósitos**
13/02 – **Millennium BCP e Montepio**
20/01 – **Montepio e Millennium BCP**
14/01 – **Santander e Novo Banco**
12-2019/01-2020: **Lampion Trojan**
(…)

The campaign starts with newly domain names that mimic the target organization. The domains are usually registered on the day before (or on the same day) on which the threat occurs.

All the noticed campaigns have been registered on 0xSI_f33d, an open-sharing feed focused on malicious campaigns only targeting Portuguese citizens.

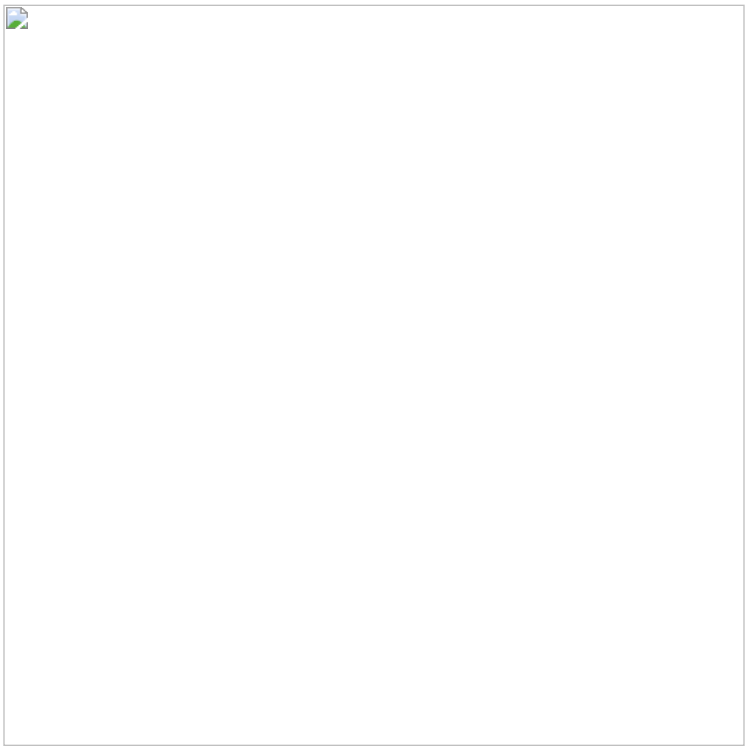


Figure 1: *0xSI_f33d – feed that compiles phishing and malware campaigns targeting only Portuguese citizens.*

These campaigns have been noticed from the beginning of 2020, where phishing and smishing campaigns are launched to target users probably obtained via other malicious waves.

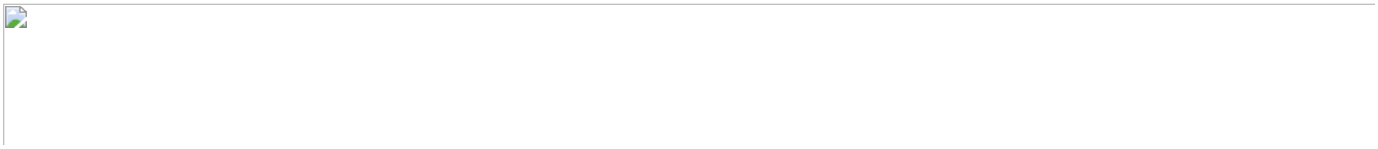


Figure 3: *Templates used in the malicious campaigns in Portugal.*

What is the main advantage of a malicious Android application instead of a simple phishing page asking for credentials?

The answer is not immediate, but due to the various layers of protection during the authentication process that a system imposes on us today, there is a need to validate authenticity and legitimacy during this action. To do this, a second authentication factor is generally used – which corresponds to an SMS received on the user's mobile phone – which immediately validates the potential trusted authentication in the system.

As an example, a simple phishing landing page, requesting access credentials, requires a semi-automated or fully manual process to collect the next authentication factor – the SMS sent to the victim's mobile phone.

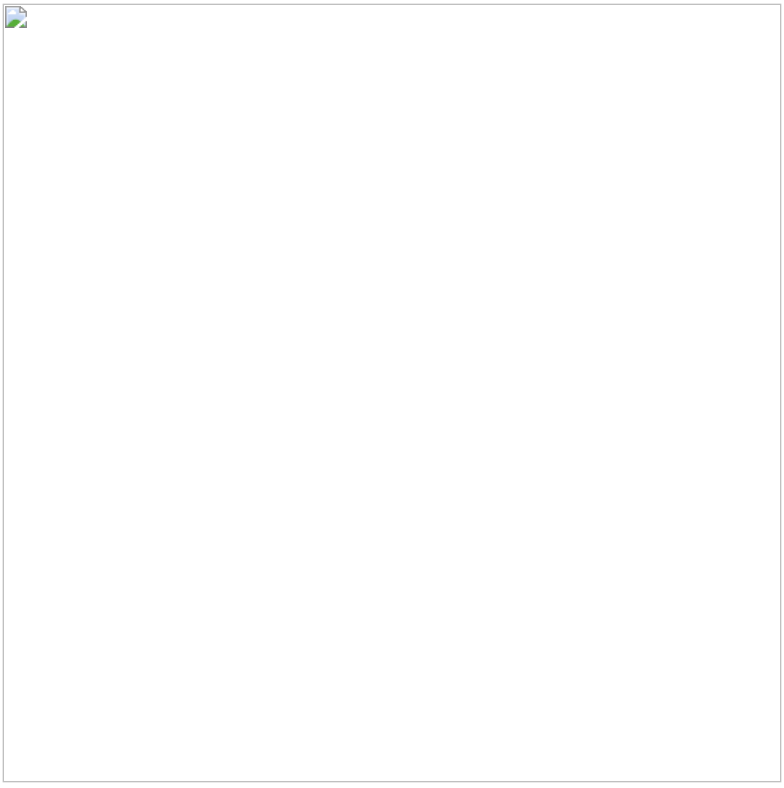


Figure 4: *Semi-automated / manual process of a typical phishing campaign via landing page.*

The diagram in Figure 4, the process is time-consuming, and often complicated to manage by criminals. In a simplified way, 10 steps are necessary for a successful authentication in the target homebanking portal.

1. **The victim accesses the phishing email or SMS.**
2. **Victim credentials are introduced in the landing-page.**
3. **Credentials are sent to a backoffice managed by the attackers.**
4. **Attackers (in operator mode) are warned that a new "customer" is online – this represents a new infection.**
5. **The attackers grab the actual process with the victim's credentials, thus carrying out the first authentication step on the bank's portal.**

6. **The bank's legitimate service knows the victim's phone number and sends the token (PIN) for the second authentication factor.**
7. **The victim submits the token on the phishing page (landing page requesting the token).**
8. **The token is sent to the backoffice.**
9. **The operator again receives a notification that the authentication process is finished.**
10. **The attacker completes the second authentication factor on the bank's portal and performs legitimate operations.**

In contrast, the same process performed through an Android application ends up solving the problem of the second authentication factor from the attacker's point of view, since the malicious android application, by itself, can manage the SMS of the victims' devices.

Figure 5: *Infection process during a phishing campaign via malicious APK.*

As observed, through these types of scenarios it only takes 6 steps to get valid authentication on the bank's portal.

Trojan Banker – *Modus Operandi*

In this section, some IOCs are shared regarding the last Android Banking-Trojan sample affecting a banking organization in Portugal (April 15th 2020).

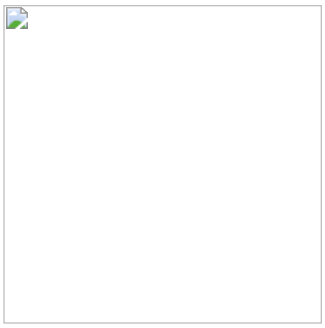


Figure 6: *Targeting landing-page to download the malicious Trojan Banker (April 15th, 2020).*

The Android application runs on any type of device as long as the target SDK is higher than version 5. This detail guarantees an increase in the scope of infection from the malicious point of view.

Figure 7: *File and App information BPI sample (April 15th 2020).*

The application requests too many privileges and is inappropriate for what it proposes to do. These type of details can be seen in the application's manifest file.

Figure 8: *Trojan Banker manifest permissions.*

```
<supports-screens android:anyDensity="true" android:smallScreens="true" android:normalScreens="true" android:largeScreens="true" />
    <uses-permission android:name="android.permission.VIBRATE" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />
    <uses-permission android:name="android.permission.WAKE_LOCK" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE" />
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS" />
    <application android:label="BPIinstall" android:icon="@drawable/icon">
        <activity android:label="BPIinstall" android:name=".main" android:launchMode="singleTop"
android:screenOrientation="unspecified" android:windowSoftInputMode="stateHidden">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <service android:name=".starter" />
        <receiver android:name=".starter$starter_BR" />
        <service android:name=".bulacha" />
        <receiver android:name=".bulacha$bulacha_BR">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED" />
            </intent-filter>
        </receiver>
```

In detail, the victim when installing the application on his smartphone gives the application:

- **Reading SMS (used to obtain the token / PIN for the second authentication factor)**
- **Internet access for communication with C2 and landing page;**
- **Creation of background services on the smartphone;** and
- **Vibration and sleep control to prevent the smartphone from vibrating when receiving the SMS with the token and / or staying asleep, thus preventing the malicious app from accessing the SMS manager and sending the token to C2.**

In detail, there is a set of JAVA classes that contain the core of the malicious application, namely:

- ***pt/bn20/ptz/starter.java***
- ***pt/bn20/ptz/main.java***
- ***pt/bn20/ptz/b4xbitset.java***
- ***pt/bn20/ptz/b4xorderedmap.java***
- ***pt/bn20/ptz/webview.java***
- ***pt/bn20/ptz/msgboxtemplate.java***
- ***pt/bn20/ptz/b4xset.java***
- ***pt/bn20/ptz/httpjob.java***
- ***pt/bn20/ptz/httputils2service.java***
- ***pt/bn20/ptz/bulacha.java***
- ***pt/bn20/ptz/b4xbytesbuilder.java***

These IOCs are the same used in other campaigns this line in Portugal. See all the information here (in Portuguese language).

> Março 2020: Análise reversa da app android entregue com o phishing do Novo Banco

The malicious application has **2 activities**, **3 services** and **3 receivers**. The most important details identified here are listed below.

Activities

.main: Activity launched in the foreground;
.webview: Activity used to launch the bank's phishing landing page.

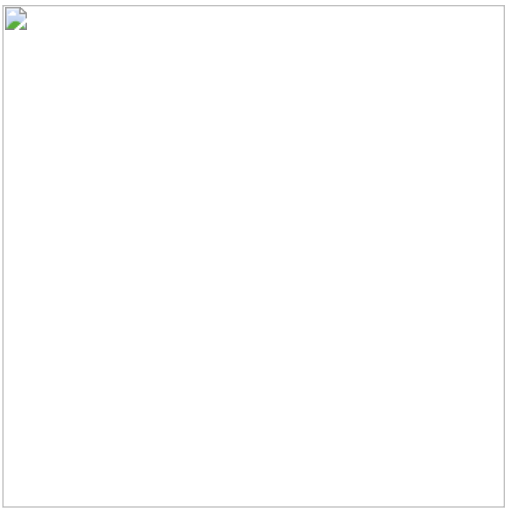
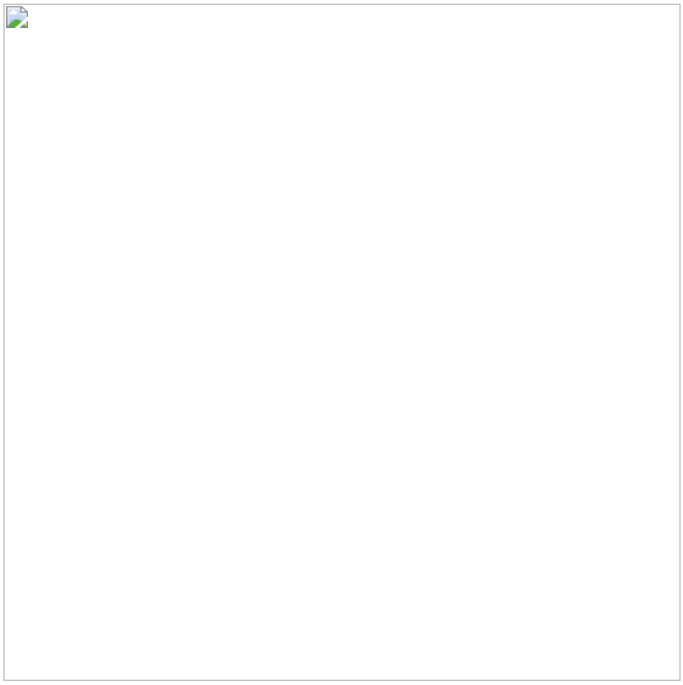


Figure 9: *Snipet of webViewWrapper. Here the landing-page is launched and presented.*

Services

.starter: Service that obtains the landing-page link from C2 (can be dynamic) and then be rendered in the *.webview* activity. This service also defines the data structure used and which stores information about the victim later sent to C2, as well as additional validations on the mobile device.



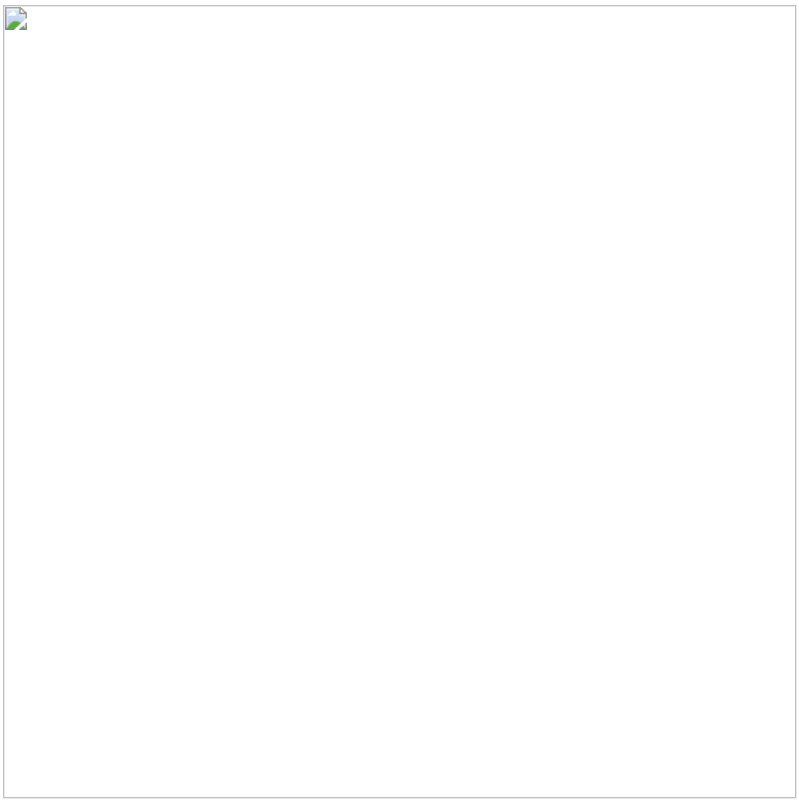


Figure 10: *Piece of code from the* ***.starter*** *service.*

In detail, the **_service_create ()** routine validates whether the target version of the victim's Android is included in the hardcoded list, and then downloads the C2 landing-page URL.

```
public static String _service_create() throws Exception {
      Common.LogImpl("3393219", "inicia tudo", 0);
      _nomemaquina = _xgerarstringsaleatorias(14);
      _versaoandroid = _getandroidversion();
      _url2 = "http://186.235.91.100/extras/bpi_link.txt";
      if (_xhttputilsconnect4.IsInitialized()) {
          return "";
      }
```

The URL for C2's phishing page is as follows. Note that it can be changed dynamically in order to avoid blacklists.

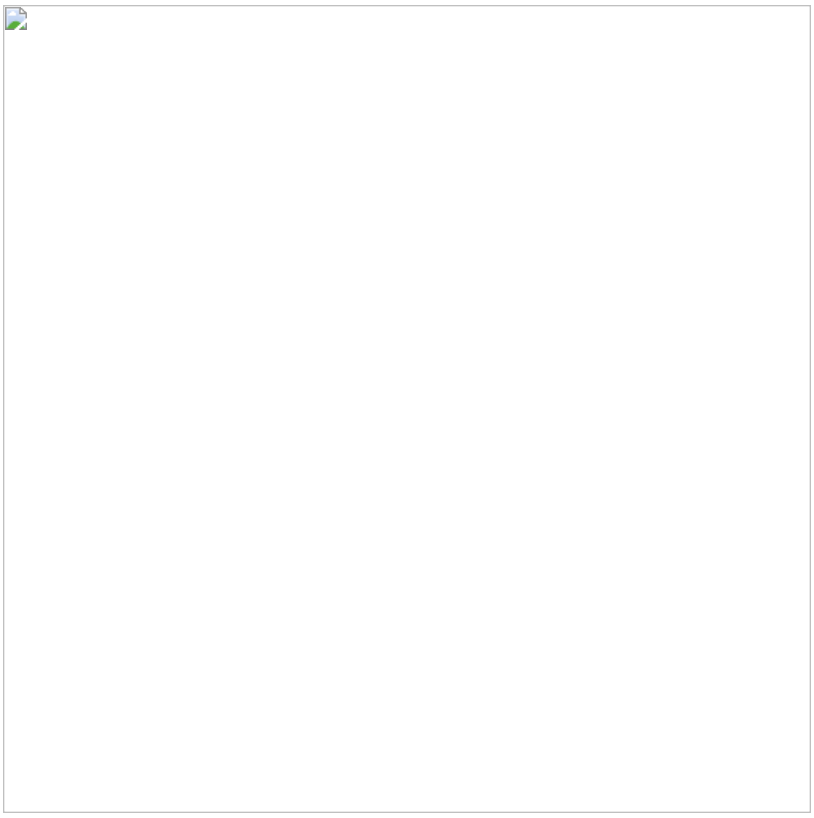


Figure 11: *Landing-page URL provided by the C2 server.*

The C2 server is located in Rio de Janeiro, Brazil, thus confirming the origin of the threat.

Figure 12: *C2 geolocation – Brazil.*

.bulacha: Class that implements the methods used for information exfiltration, SMS management, etc.

When the service is created, the C2 is notified that the device is active, and the volume of the infected device is changed so that the victim is unaware of any potentially suspicious activity.

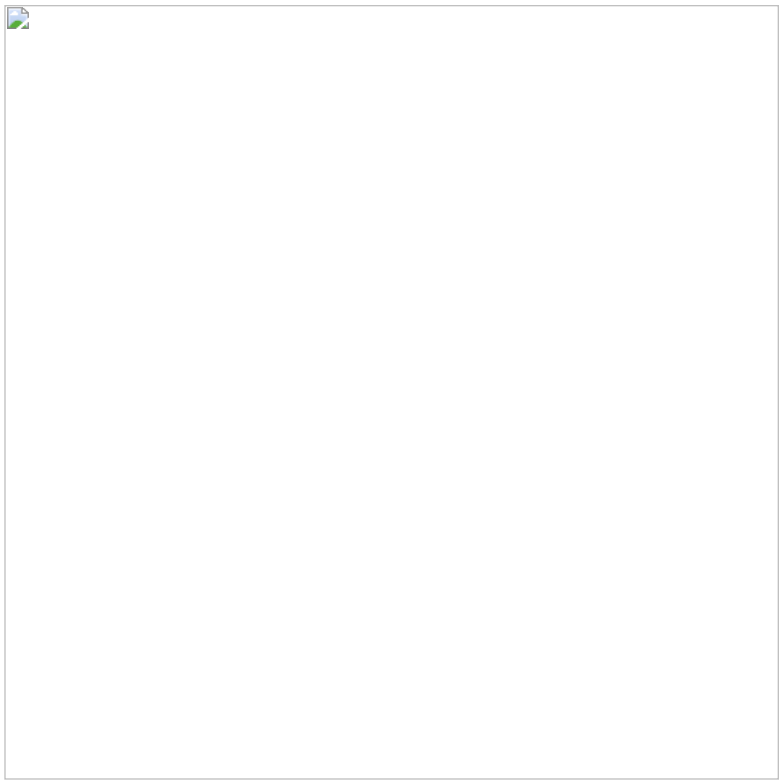


Figure 13: *The volume of the infected device is changed.*

When the SMS is received after the victim enters the credentials on the bank's landing page, the bank's system sends the token / PIN to the user's mobile device now infected.

Figure 14: *Trojan-Banker reading the Token SMS sent from banking system with the token.*

The data is exfiltered and sent to C2 via an HTTP – POST request.

Figure 15: *Victim's details sent to the C2 server geolocated in Brazil, São Paulo.*

The malicious application sends the details to C2 via an HTTP-POST request.

Figure 16: *HTTP request sent to the C2 server.*

Finally, the victims' credentials and tokens are managed on the C2 server available online on: **hxxp://186.235.91[.]100**, the same IP address used on the last campaigns this line in Portugal.

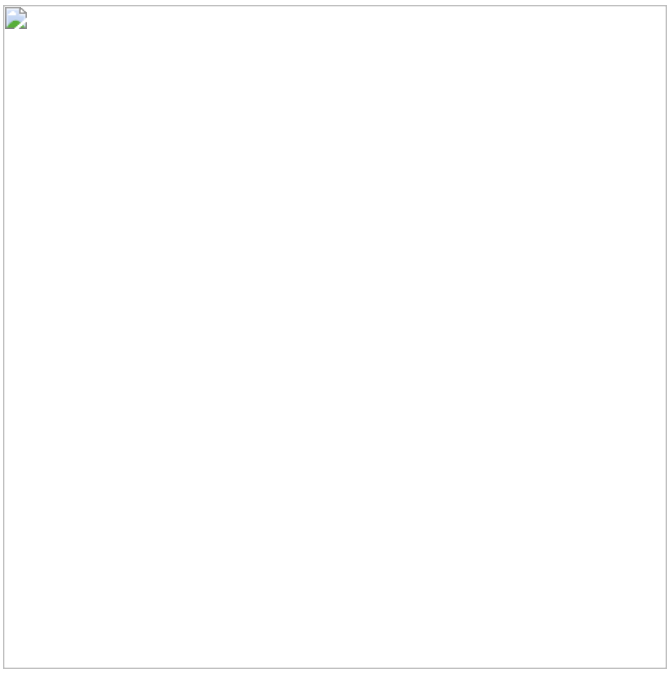
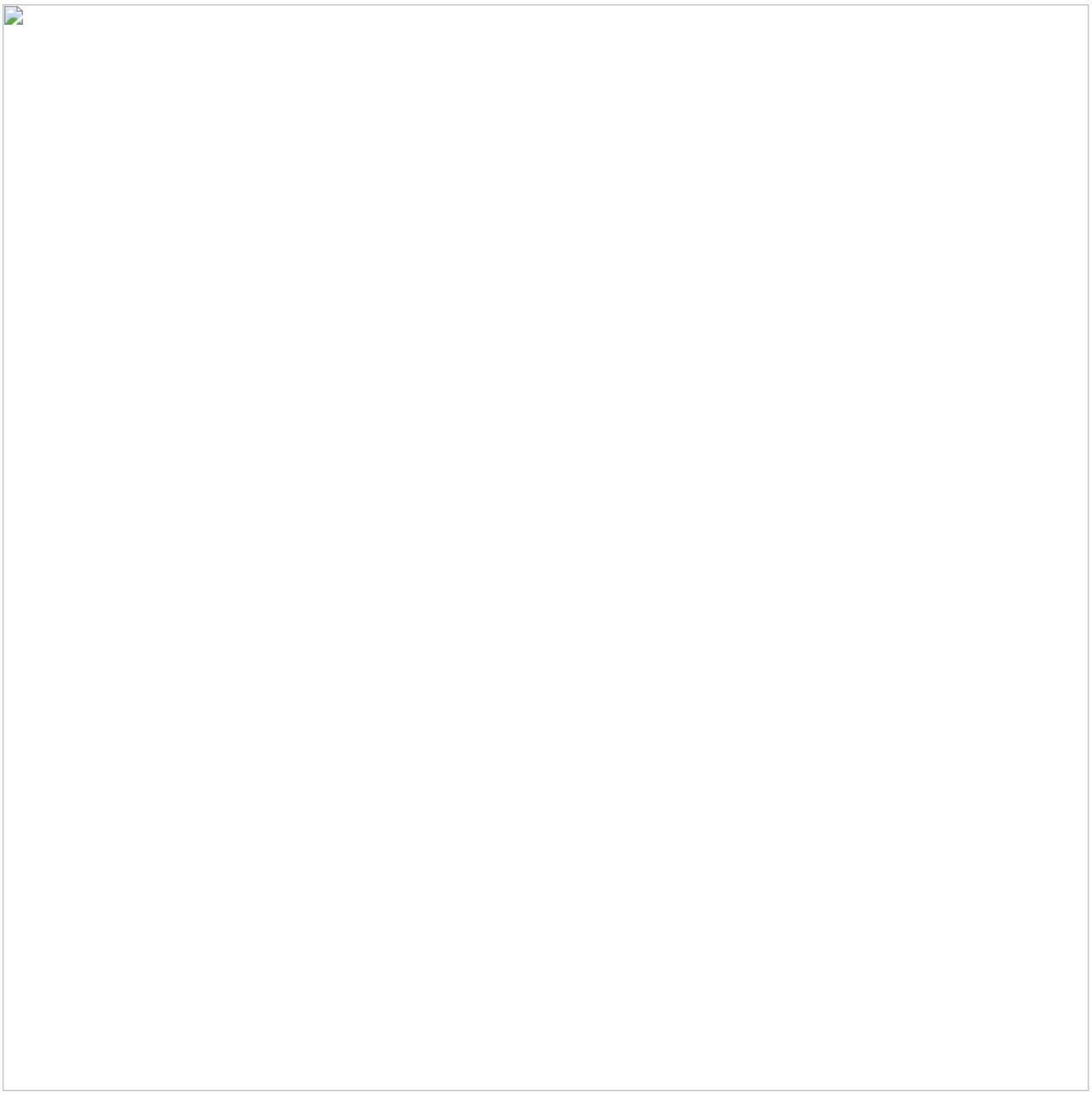


***Figure 17**: C2 portal.*

Mitre Att&ck Matrix



Indicators of Compromise (IOCs)

```
File name: BPI_Security.apk
MD5:  3f05afa8e5156d45614834627f652a55
Size:  1.14MB
hxxps://net24apk[.]website
hxxps://sis-ptcadastro[.]com/app/BPI_Security.apk
hxxps[://sis-ptcadastro.]com
hxxps[://ptcadastro-sis.]com
hxxps[://seguropt.]com/site/choose.]php

--BPI banking (April 15th 2020)--
http://186.235.91.100/extras/bpi_link.txt
http://186.235.91.100/controls/bpi/control.php?message=
http://186.235.91.100/controls/bpi/sms.php?apelido
http://186.235.91.100/controls/bpi/sms.php
http://186.235.91.100/controls/bpi/control.php?message=2

-- Novo Banco (March 2020) ---
hxxp://186.235.91[.]100/extras/nb_link_lyly.txt
hxxp://186.235.91[.]100/controls/nb/control.php?message=
hxxp://186.235.91[.]100/controls/nb/sms.php?apelido=
hxxp://186.235.91[.]100/controls/nb/sms
hxxp://186.235.91[.]100/controls/nb/control.php?message=2

C2
hxxp://186.235.91[.]100
Mysql phpmyadmin
hxxp://186.235.91[.]100/phpmyadmin/index[.]php

OtherIOCs:
package="pt.bn20.ptz"
<service android:name=".bulacha" />
<title>Operador MIB 1.0</title>


https://www.virustotal.com/gui/ip-address/51.83.252.64/relations
```

Pedro Tavares

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker/Pentester, Malware Researcher and also a Security Evangelist. He is also a founding member at CSIRT.UBI and Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d – a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.