# Trojan Lampion is back after 3 months

seguranca-informatica.pt/trojan-lampion-is-back-after-3-months/

May 11, 2020

**Trojan Lampion is back after 3 months. The malware was observed last days with a new obfuscation layer, new C2, and distributed inside an MSI file.**
Trojan Lampion is a malware observed at the end of the year 2019 impacting Portuguese users using **template emails from the Portuguese Government Finance & Tax** and **EDP**.

The latest campaigns in Portugal were observed during February 2020, according to the threat indicators available at ***0xSI_f33d*** – *The Portuguese Abuse Open Feed*. A new modified version of this malware was observed during May 2020 using template emails that **impersonate** an **invoice from a Bank transaction**, an **invoice from Vodafone Group**, and in another scenario, **emergency funds provided by the Portuguese Government to help the COVID-19 fight**.

Below, the email templates on how Lampion has been distributed in May 2020 in Portugal are presented.

## Lampion email templates – May 2020

**SAPO TRANSFER TEMPLATE**

On May 8th, 2020, a fresh version of Lampion trojan was distributed using templates using the SAPO Transfer Cloud and the email related to a bank transfer.

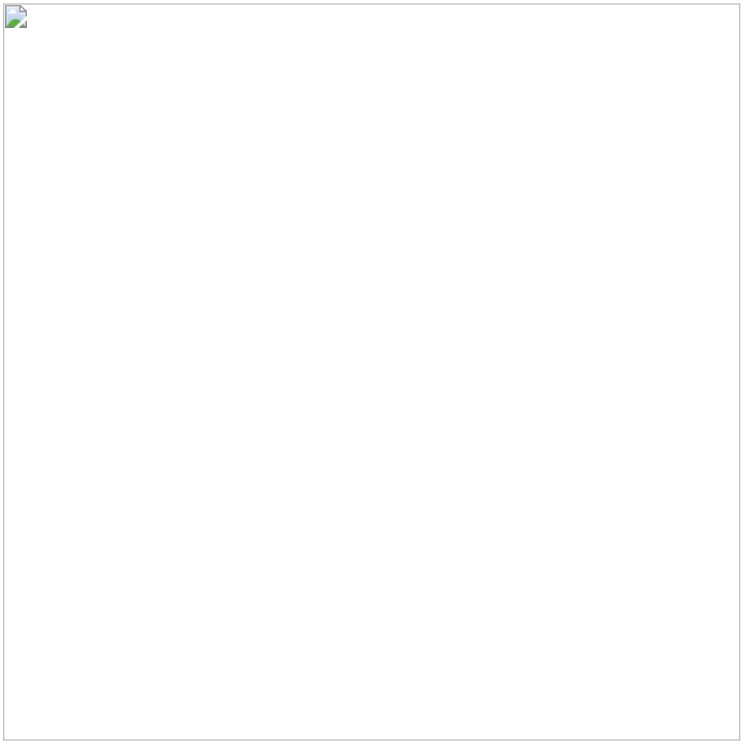


***Figure 1:*** *Lampion malware distributed via SAPO TRANSFER cloud.*

As noted in previous campaigns, the threat is distributed on a VBS file along with other documents to lure victims.

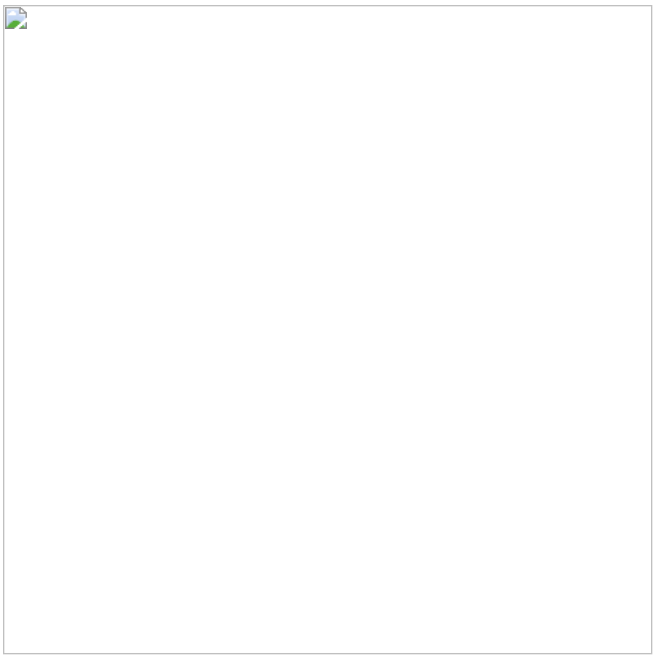


***Figure 2:*** *Message included by crooks inside the PDF file.*

**VODAFONE  GROUP INVOICE TEMPLATE**

In this scenario, a Microsoft Installer (MSI) file was used to disseminate the threat. The malicious file is downloaded from the Google API Cloud.

***Figure 3:*** *Lampion trojan distributed via an MSI file hosted on Google API Cloud.*

**PORTUGUESE GOVERNAMENT TEMPLATE / COVID-19**

Also, an MSI file was used to infect the victims (***formulario_emergencial_gov.msi***). In this case, the malicious file was downloaded from an AWS S3 bucket. The *modus operandi* both malicious MSI file is the same and explained below. We are living in an era where crooks taking advantage of the pandemic situation to launch new waves of phishing and malware every day.

***Figure 4:*** *Malicious MSI file downloaded from AWS S3 bucket and using COVID-19 theme that impersonates the Portuguese Government.*

## Lampion May 2020 – *Modus Operandi*

According to the first appearance of this banking trojan in December 2019, the *modus operandi* remains as documented here. Only the way how the malware is distributed has been changed along the time.

As observed in Figure 2, this is the classic form of Lampion. It poses as a VBS file along with other files, including an image and a PDF file to lure the victims.

Nonetheless, Figure 3 and Figure 4 show another way how Lampion has been spread. Crooks are using an MSI file with the VBS file inside (1st stage), that is executed to infect the victim's device. Also, the VBS file is harder to understand, it is a bit bit more overshadowed in contrast to the initial samples. In brief, these are the only changes observed in these fresh samples in contrast to December 2019.

Analyzing the MSI file from Figure 4, it poses as a file sent from the Portuguese Government to help in the COVID-19 fight.

Inside the MSI file is available the VBS file (Lampion – 1st stage), which is installed on "**C:\Programs File (x86)\Firefox_2020-*\Firefox_2020-***" when the MSI file is executed.

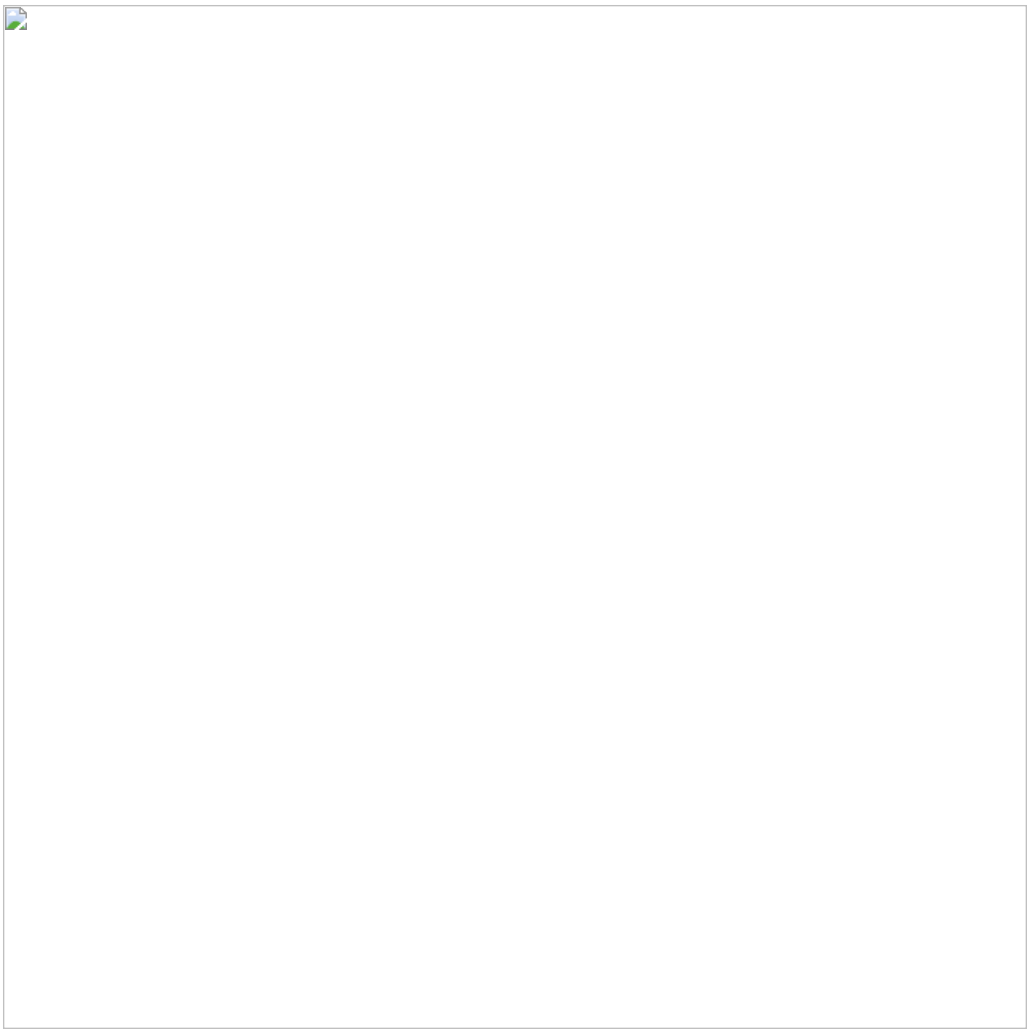


***Figure 5:*** *Lampion MSI file with the VBS file (1st stage) inside.*

***Figure 6:*** *MSI file installation dropping the VBS file (1st stage) inside the C:\Programs Files (x86) folder.*

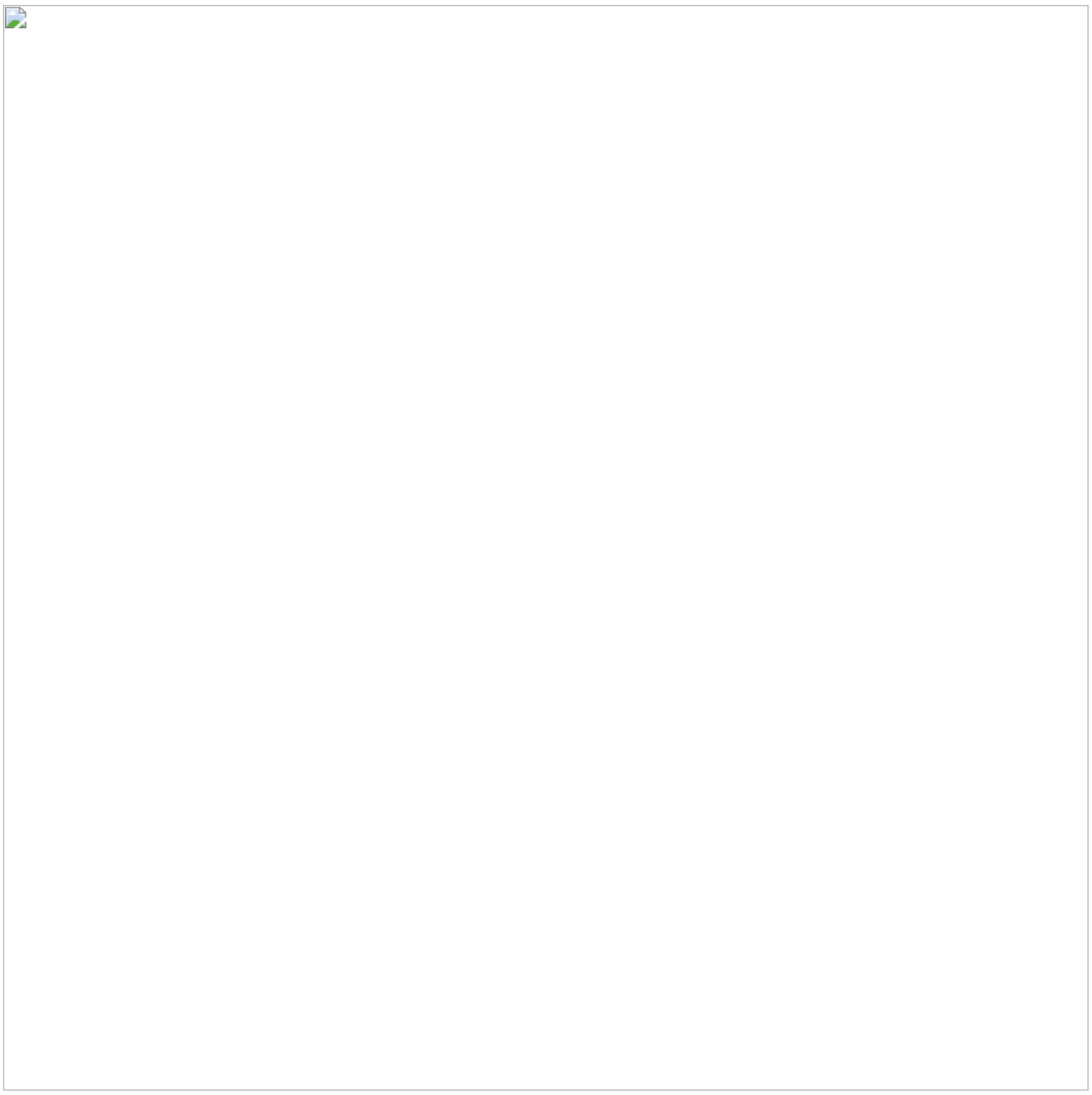


***Figure 7:*** *VBS file (1st stage) available and executed from C:\Programs Files (x86) folder.*

From this point, the malware process is the same how documented in December 2019. However, the VBS file is now harder, with a new obfuscation round (see Figure 8 below).

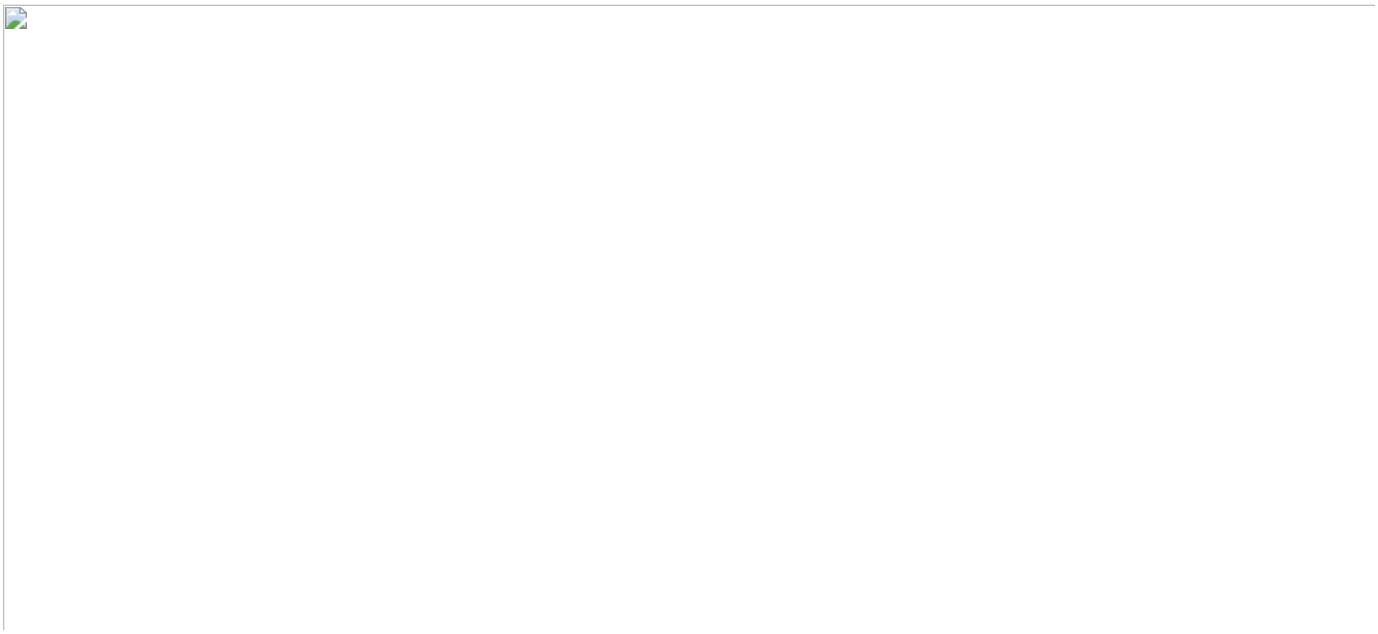


***Figure 8:*** *Snippet of code – obfuscation differences between the VBS samples; December 2019 and May 2020.*

The next stage is downloaded through the execution of the VBS file on the infected device. In order to decode the URLs, we use the snippet of code available here.

The analyzed samples (2nd stage) are download from the Google Cloud instead of AWS S3 buckets; as observed between December 2019 and February 2020.

```
--SAMPLES SAPO TRANSFER TEMPLATE--
~wa^6jfjdfHik0z%S%miBj:emhVW\]+[W$\]Ve0e*];b.[&WifM_BiD$2YBePcj%^j1[bWScc#=cYe/Z+kYbOeEiufz%O&I$pp-_,fA'
hxxps://storage.googleapis.]com/team-modulosp/0.]zip

zH$^Uj[jHf2ir0[%u%YiEj'[email protected]]s[`$5]0e6e:]`bB[<WLf7_Gi*$FYZe+cp%ojP['W;co#lcLeIZ]krb'eTimf(%PF=#Z'c(h#:/^$}Z~bZbjH
hxxps://storage.googleapis.]com/team-modulosp/P-12-9.]dll


-- SAMPLES PORTUGUESE GOVERNMENT TEMPLATE / VODAFONE GROUP TEMPLATE --
hxxps://storage.googleapis.]com/team-modulo/0.]zip
hxxps://storage.googleapis.]com/team-modulosp/P-1-20.]dll
```

The code and behavior of the malware are the same in the samples shared above, however, criminals introduce “new lots of junk” in each sample as a means of bypassing AV signatures.

In order to corroborate that, it is possible to check the size of the PE files below.

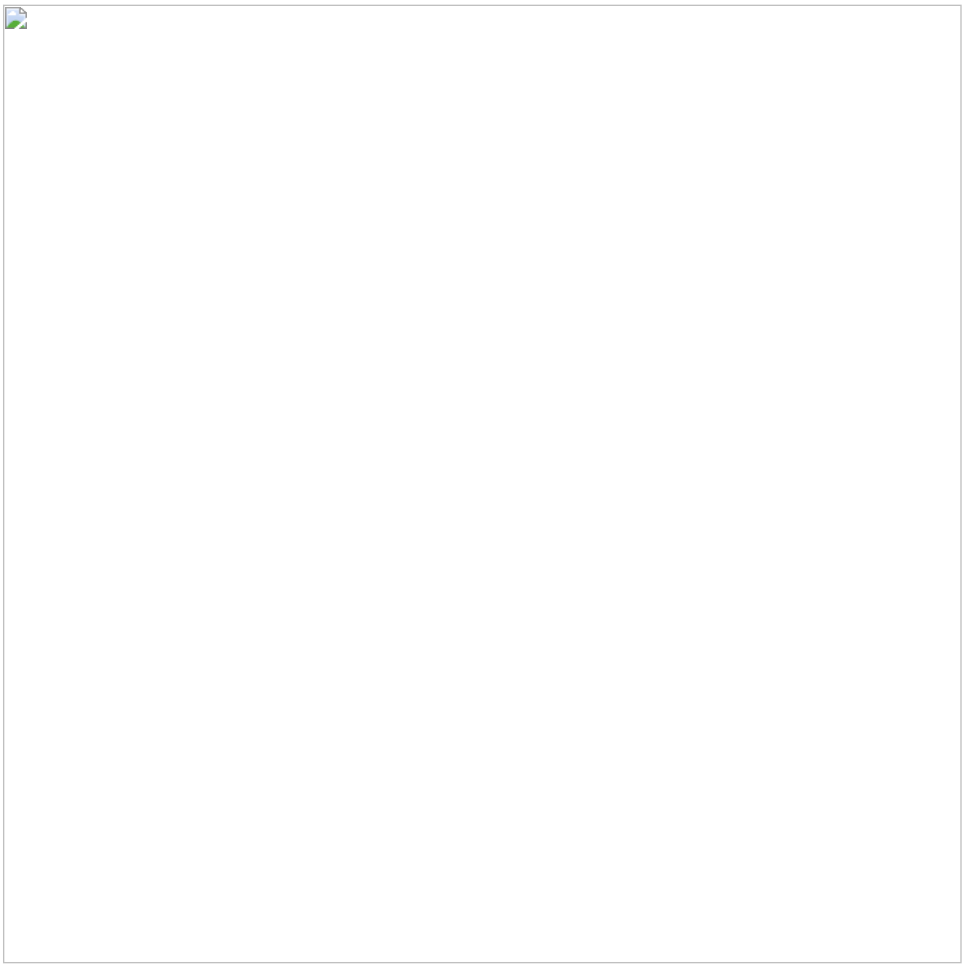


***Figure 9:*** *Size of two samples distributed in Portugal during May 2020.*

Both the files are executable files, with a difference in the size of the file. As mentioned, a lot of junk is put inside the PE file increasing, thus, the file entropy and to bypass AV signatures.

Figure 10 shows image resources included inside the binary. In detail, 52.5MB from the total (63.3MB) are only populated by 12 images, including a BPM image file of around 27 MB.

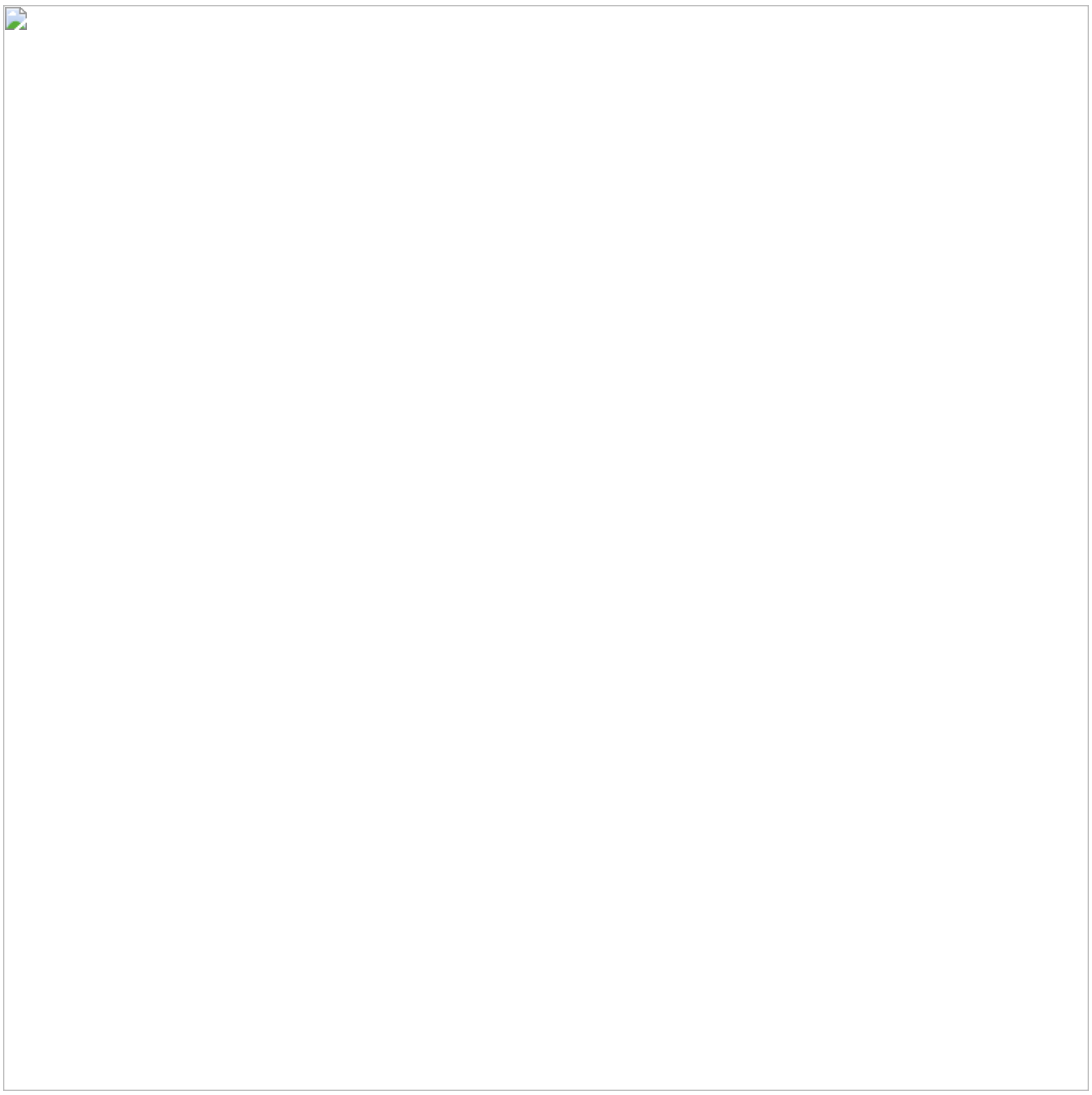


***Figure 10:*** *Image resources inside the malware to increase the file size.*

As noticed on other Trojans from Brazil, it was also coded in Delphi using the Embarcaredo IDE to build the executable file. In addition, the IDE version used to build these samples is the same used to build the sample of December 2019.

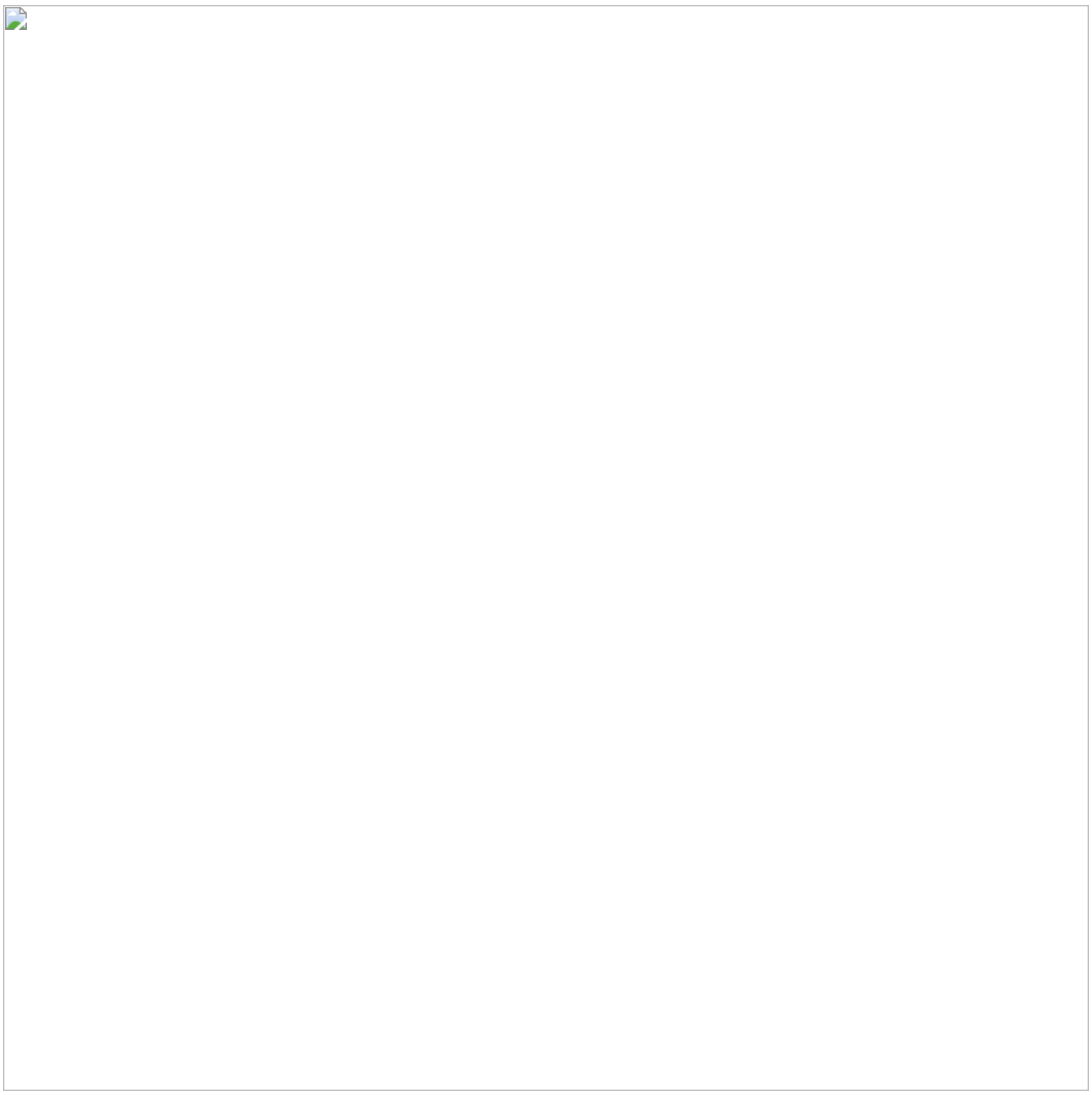


***Figure 11:*** *Embarcadero Delphi version used in December 2019 also observed in May 2020.*

This indicator shows what was observed during the analysis of the Trojan: **only minor changes were made, such as: changing the address of the C2 server**.
The URLs themselves encoded to send information about the victim to C2 have the same name, e.g.: "**PostaEstaBosta.php**".
More IOCs and C2 are presented towards the end of the publication. For more details about this malware see the initial publication from here.

## Additional screens and IOCs on Lampion – May 2020 samples

When installed, the trojan can be used by crooks to launch overlay windows on the victim's device. The number of templates used and affected organizations are huge, including Brazilian, and Portuguese banks as presented below.

***Figure 12:*** *Messages used to create overlay windows and triggered when the victim accesses the target banking portal.*

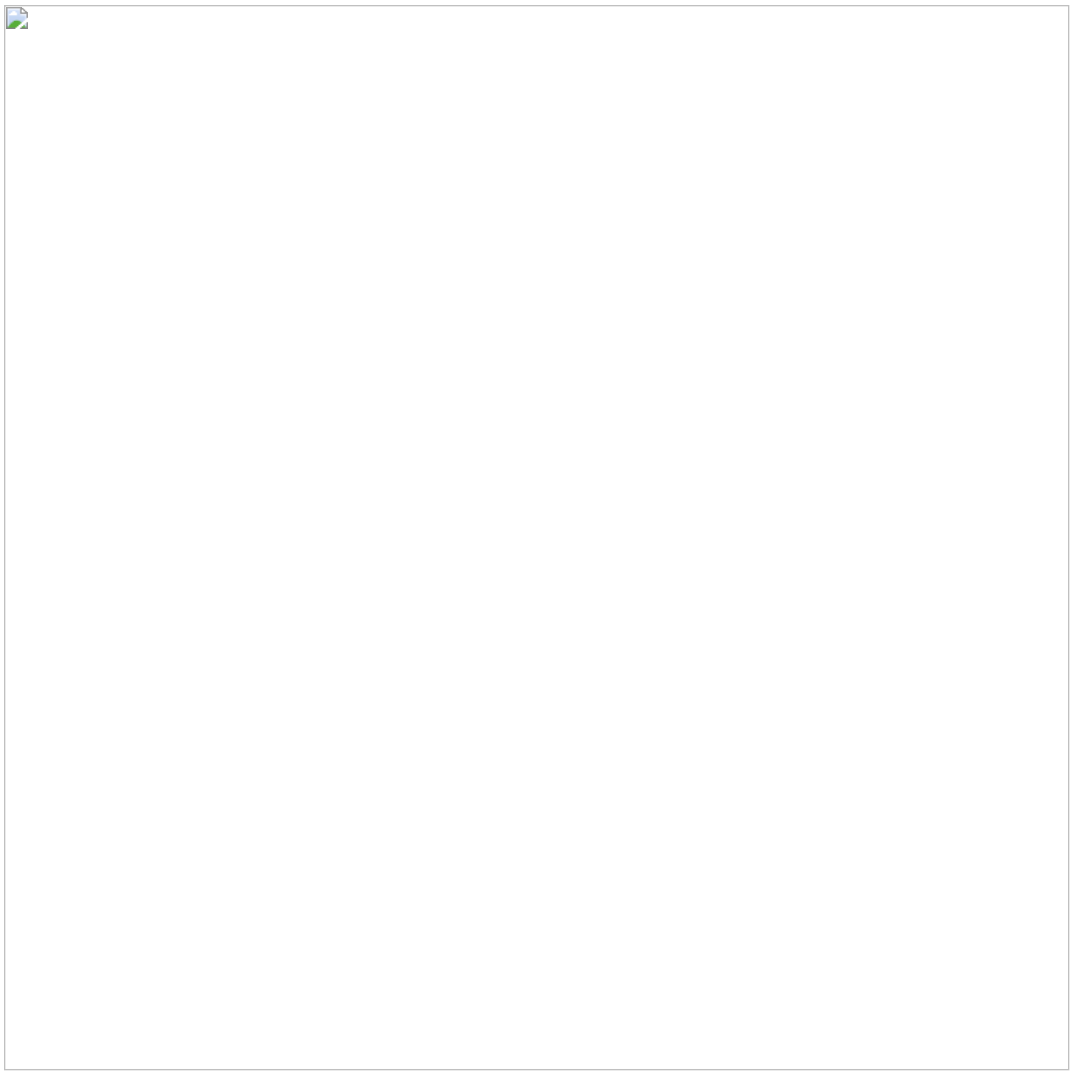


***Figure 13:*** *Lampion overlay screens (courtesy of MllenniumBCP – Portugal).*

The malware is “sleeping” and “resumes” its operation when the following bank portals are accessed by the victim (including bitcoin portals).

```
aplicativo bradesco
banco bradesco
mercado bitcoin
banking bnb
banco montepio
montepio
millenniumbcp
Santander
BPI Net
Banco BPI
BPI
Caixadirecta
Caixadirecta Empresas
CGD
NOVO BANCO
EuroBic
Crédito Agrícola
Login Page
CA Empresas
Bankinter
navegador exclusivo
TravaBB
Banco do Brasil
Caixa Economica
BANRITRAVAR
Mercado Bitcoin
TravaBitco
Banco Original
Citibank
itauaplicativo.exe
```

The **overlay windows are invisible when malware is running** and are triggered when the specific banking portal is accessed.

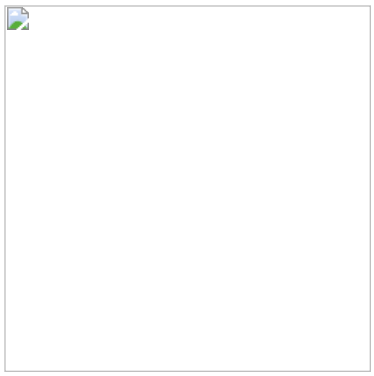


***Figure 14:*** *Overlay windows invisible during malware execution – sleeping.*

Lampion trojan can be also used by crooks to manually launch a specific page remotely.

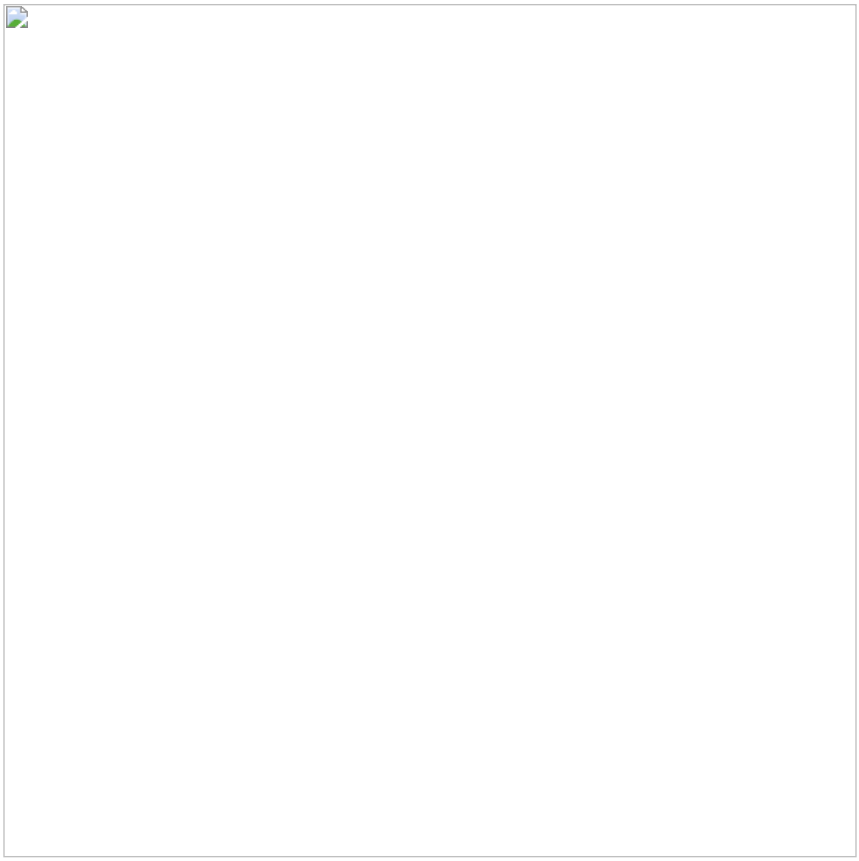
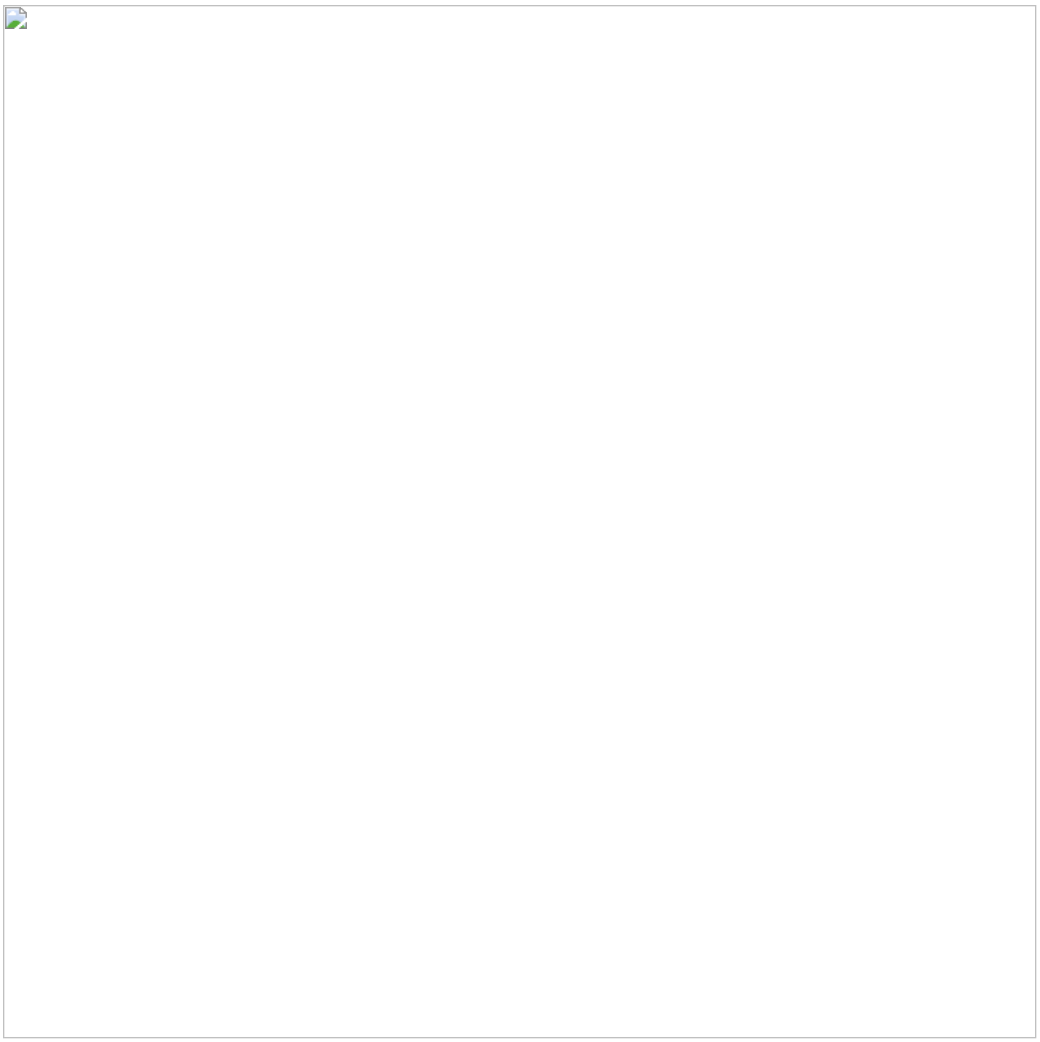


***Figure 15:*** *Trojan feature to trigger manually overlay windows.*

Next, when a specific banking portal is accessed,  the overlay windows are displayed (Figure 12 and 13 above), and data is sent to the C2 server.



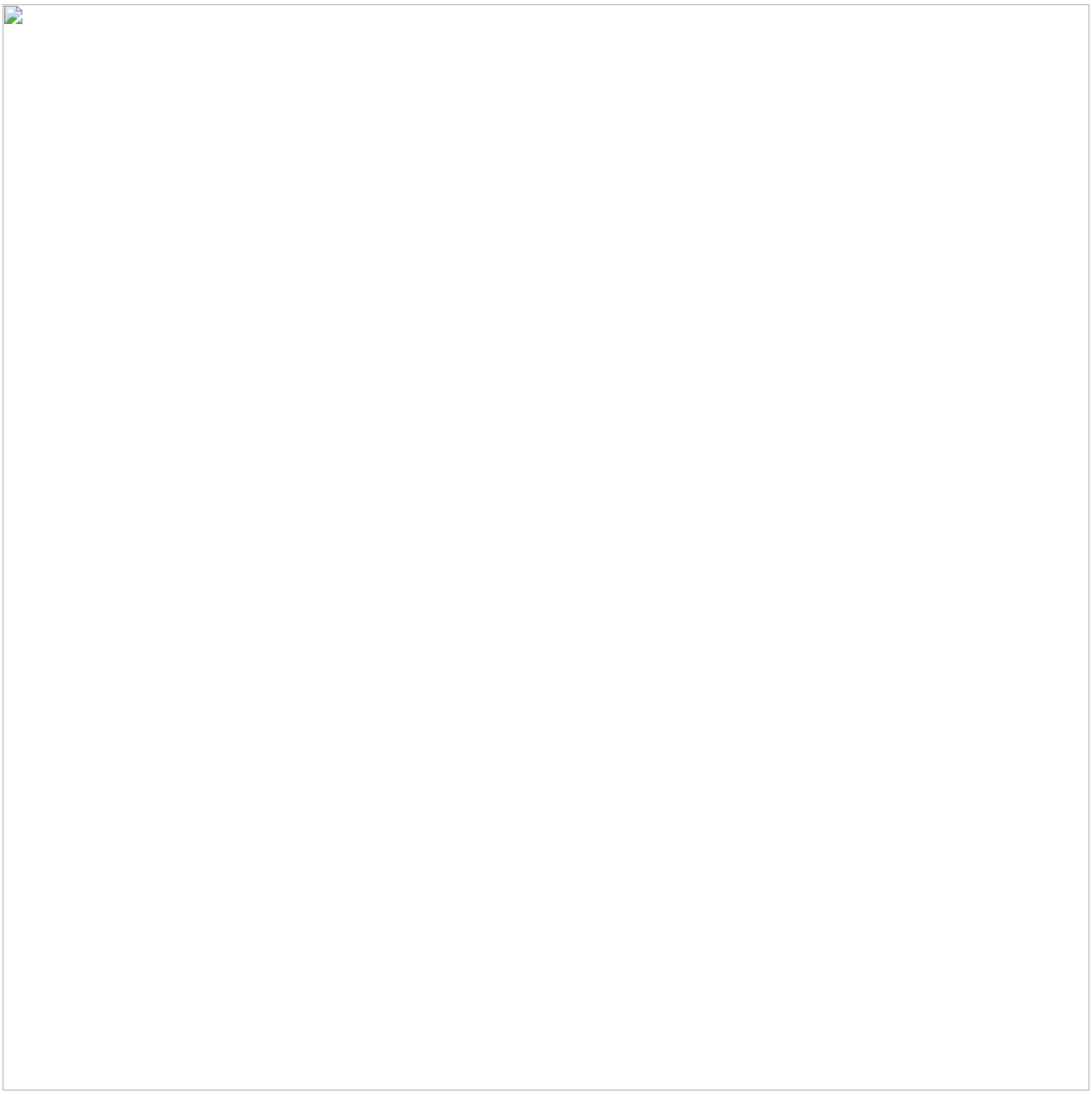
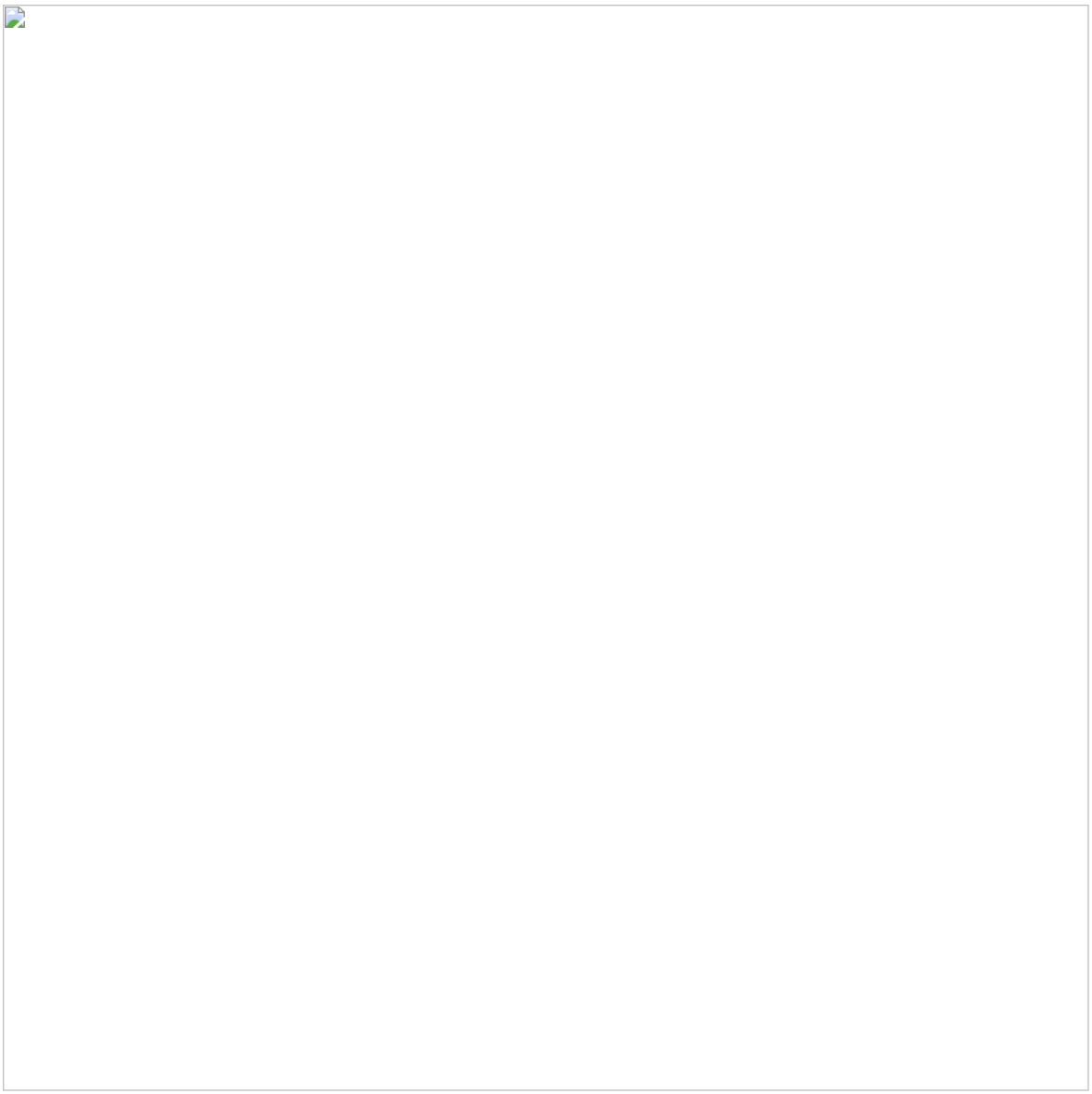


***Figure 16:*** *Overlay windows triggered when a specific banking portal is accessed.*

Next, some details about the infected machine sent to the C2 server, including the computer name, SO, AV, etc.

*Figure 17: Detais sent to C2 server.*



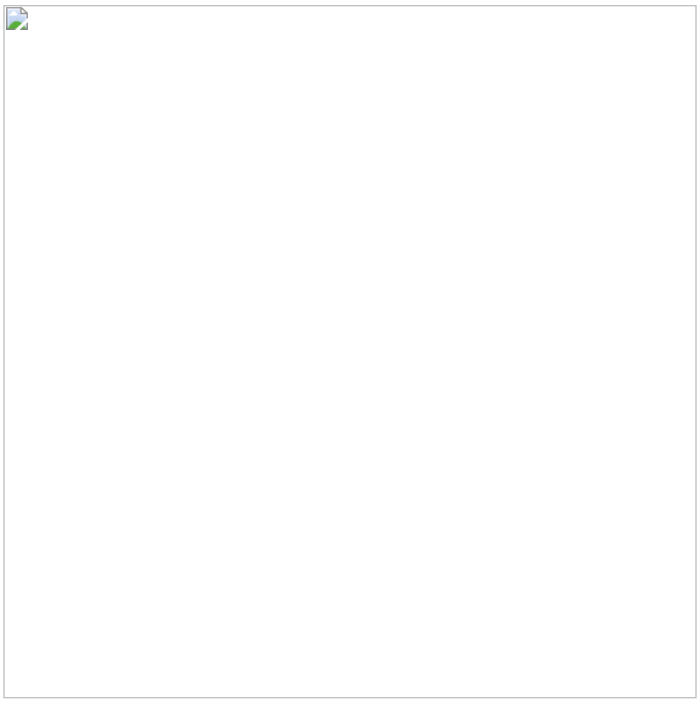


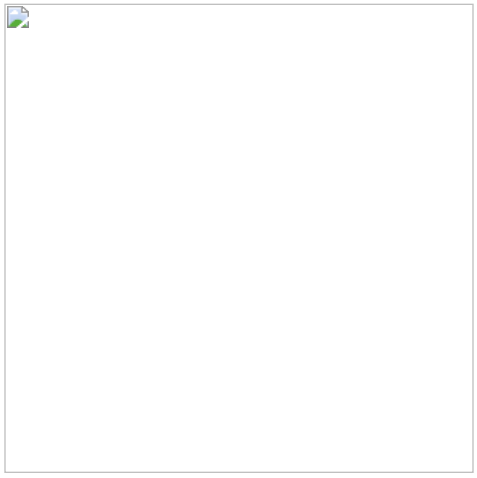
***Figure 18:*** *Lampion C2 authentication portal geolocated in Japan.*

## Final Thoughts

Malware is nowadays one of the major cyber weapons to destroy a business, market reputation, and even infect a wide number of users. The next list present some tips on how you can prevent a malware infection. It is not a complete list, just a few steps to protect yourself and your devices.

- Get outdated software of your system
- Get email savvy; take several minutes looking at the new email and not a few seconds
- Beware of fake tech support, emails related do bank transactions, invoices, COVID19, everything you think be strange
- Keep Internet activity relevant
- Log out at the end of the day
- Only access secured  and trusted sites (not only websites with green lock – please think you are doing, as many phishing campaigns are abusing of free CA to create valid HTTPS certificates and to distribute malicious campaigns over it)
- Keep your operating system up to date
- Make sure you are using an antivírus
- Beware of malvertising

And last but no the least, do not execute files and content from untrusted locations.



**Take-home message**
**Be proactive and start taking malware protection seriously!**

## Indicators of Compromise (IOCs)

```
====/====/===/====Lampion May 2020 samples====/====/===/====

--URLs-and-landing-page-
hxxp://my.vodafone.pt-new.]cf/
hxxps://transfer.sapo.]pt/downloads/04032345-a9ad-4bc5-91aa-129eae12ced4/sapotransfer-5a521f8936f43qW/

--MSI-files--
hxxps://auxiliogov.s3.us-east-2.amazonaws.]com/formulario_emergencial_gov.msi
hxxps://storage.googleapis.]com/pt-ffox/factura_vodafone_2020xg17.msi

--google cloud (2nd stage)--
hxxps://storage.googleapis.]com/team-modulosp/P-12-9.dll
hxxps://storage.googleapis.]com/team-modulosp/0.zip
hxxps://storage.googleapis.]com/team-modulosp/P-1-20.dll
hxxps://storage.googleapis.]com/team-modulo/0.zip

--C2-Japan-
hxxp://108.61.181.]207/PQP/PostaEstaBosta.php
hxxp://108.61.181.]207/PQP/index.php



==June 2020===
https://storage.googleapis.com/pedrotavaresseuparvodeixaosgarotobrincar/0.zip
https://storage.googleapis.com/pedrotavaresseuparvodeixaosgarotobrincar/P-11-10.dll
```

## Online Sandbox (VT)

–MSI–
https://www.virustotal.com/gui/file/f085588cf016993e6298640bf797c1d31b61a8087a3240d517a53a5a58474987/detection
https://www.virustotal.com/gui/file/1b47949eb5769bf224b500e963eeed030d877b6bf5177926563b654b9ff31b21/detection
https://www.virustotal.com/gui/file/a1f4fc0600d0971454d746a6ba87bbde56114a91119e95fc4ddb71f97452bb1a/community
https://www.virustotal.com/gui/file/cd9d625e9fe6116f5f5e938ae9f693e10529df238b4e2bbd974f6d5c41f96aa8/detection
https://www.virustotal.com/gui/file/6fa1cda725c1e19cd140c83c5b1e653222c8846c2bdde7acedb50dc1e8c977ec/detection

–0.zip–
https://www.virustotal.com/gui/file/a5116e651bede78ccf208954f51f0a3bc82fb05f989e10fdb37808d568cc358a/community
https://www.virustotal.com/gui/file/b372b3c141c79da5267df3fcbba251908a3ef1a3bf9da54bbade572d847eecbe/detection

–.dll–
https://www.virustotal.com/gui/file/fbc2645684bb1d1aad9cdf84824811832f8bd74f4515bdceda931e23f08e6f1b/community
https://www.virustotal.com/gui/file/81df2c6c4287d2b9247b589d8e10efeb228270da5b3615642a2b5eaa00d22945/community

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.