The hidden C2: Lampion trojan release 212 is on the rise and using a C2 server for two years

By Pierluigi Paganini

Published: 2022-03-13 · Archived: 2026-04-05 17:48:28 UTC

The hidden C2: Lampion trojan release 212 is on the rise and using a C2 server for two years.

Lampion trojan is one of the most active banking trojans impacting Portuguese Internet end users since 2019. This piece of malware is known for the usage of the Portuguese Government Finance & Tax (Autoridade Tributária e Aduaneira) email templates to lure victims to install the malicious loader (a VBS file). However, fake templates of banking organizations in Portugal have been used by criminals to disseminate the threat in the wild, as observed in Figure 1 below with a malicious PDF (***151724540334 Pedidos.pdf***).

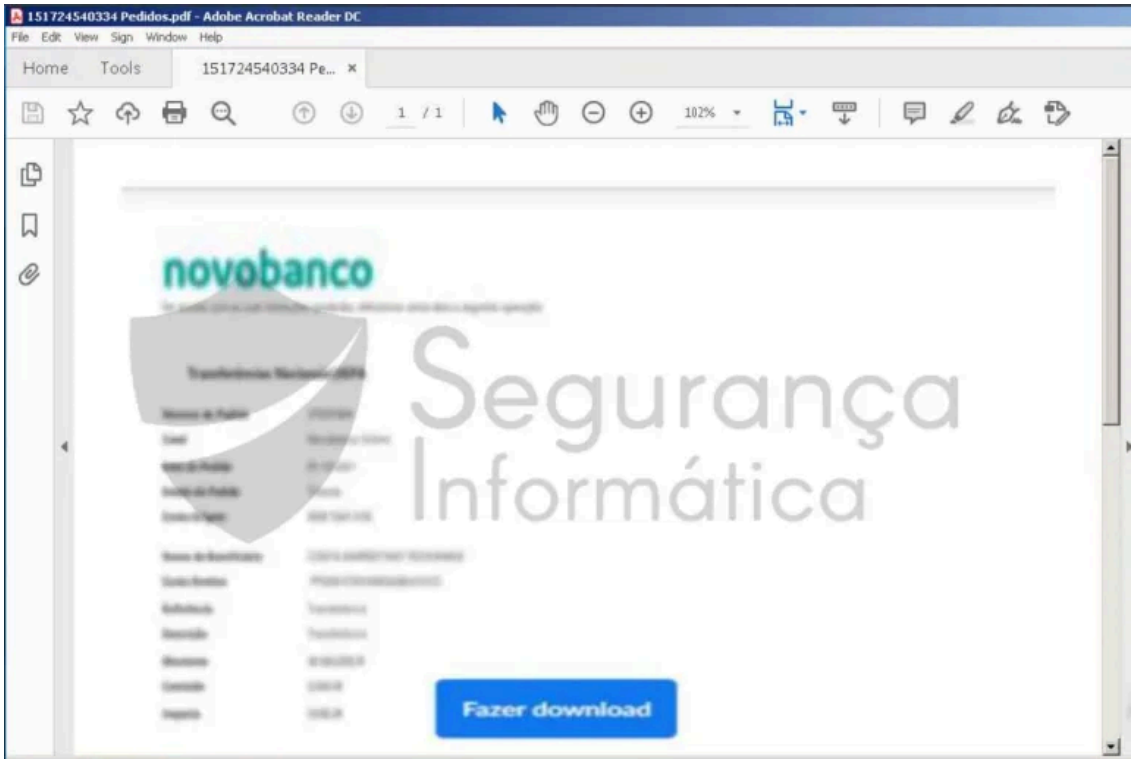


Figure 1: *Emails templates are delivering malicious PDFs impersonating banking organizations in Portugal to spread Lampion trojan.*

The malware TTP and their capabilities remain the same observed in 2019, but the trojan loader – the VBS files – propagated along with the new campaign has significant differences. Also, the C2 server is the same noticed on the past campaigns since 2020, suggesting, thus, that criminals are using the same server geolocated in Russia for two years to orchestrate all the malicious operations.

FUD capabilities of the Lampions' VBS loader

Filename: Comprovativo de pagamento_2866-XRNM_15-02-2022 06-43-54_28.vbs
MD5: 2e295f9e683296d8d6b627a88ea34583

As expected, the Lampions' VBS loader has been changed in the last years, and its *modus operandi* is similar to other Brazilian trojans, such as **Maxtrilha**, **URSA**, **Grandoreiro**, and so on. In detail, criminals are enlarging the file size around 56 MB of junk to bypass its detection in contrast to the samples from 2019 with just 13.20 KB.

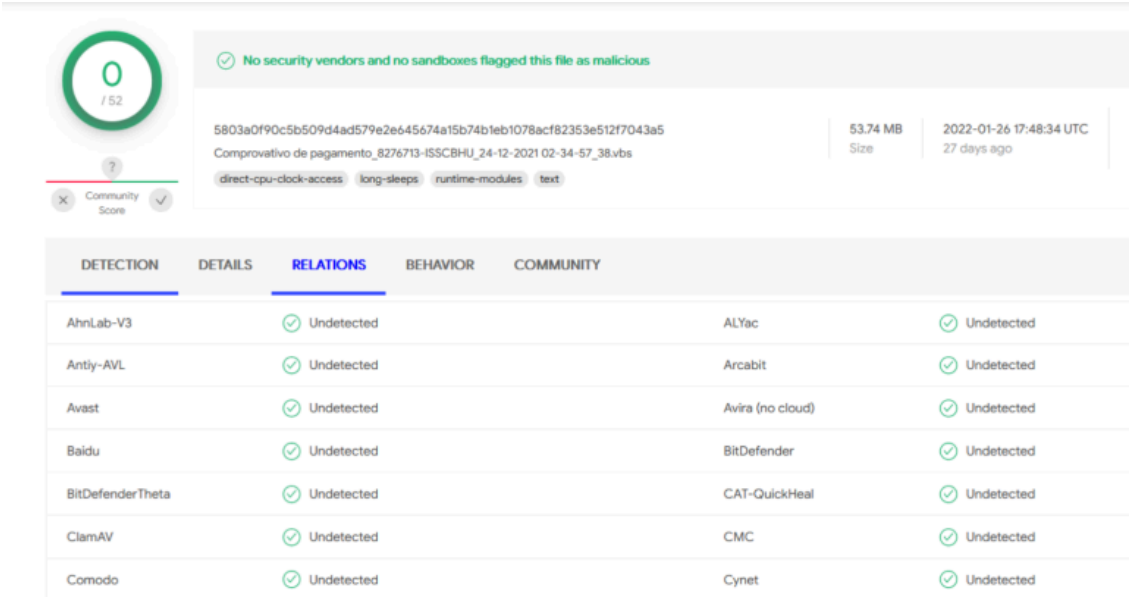
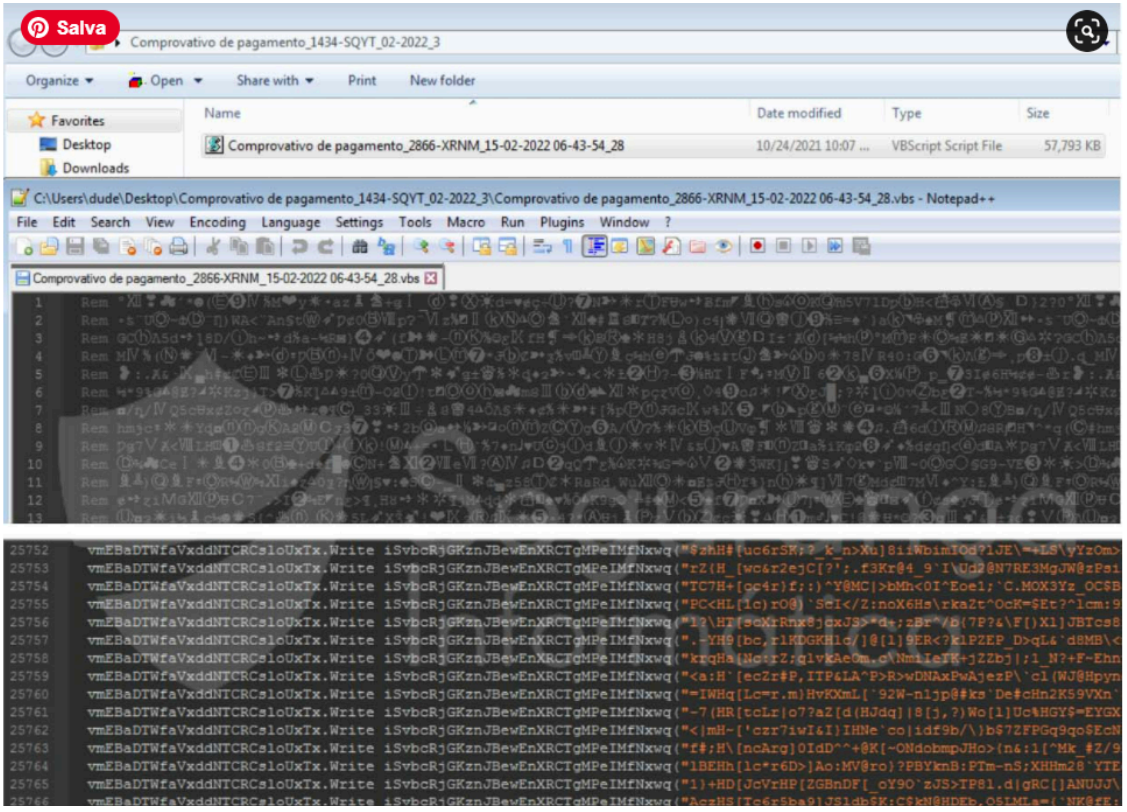


Figure 2: *Lampions' VBS loader file enlarge technique to bypass its detection.*

The VBS file contains a lot of junk sequences, and after some rounds of code cleaning and deobfuscation, 31.7 MB of useless lines of code were removed.



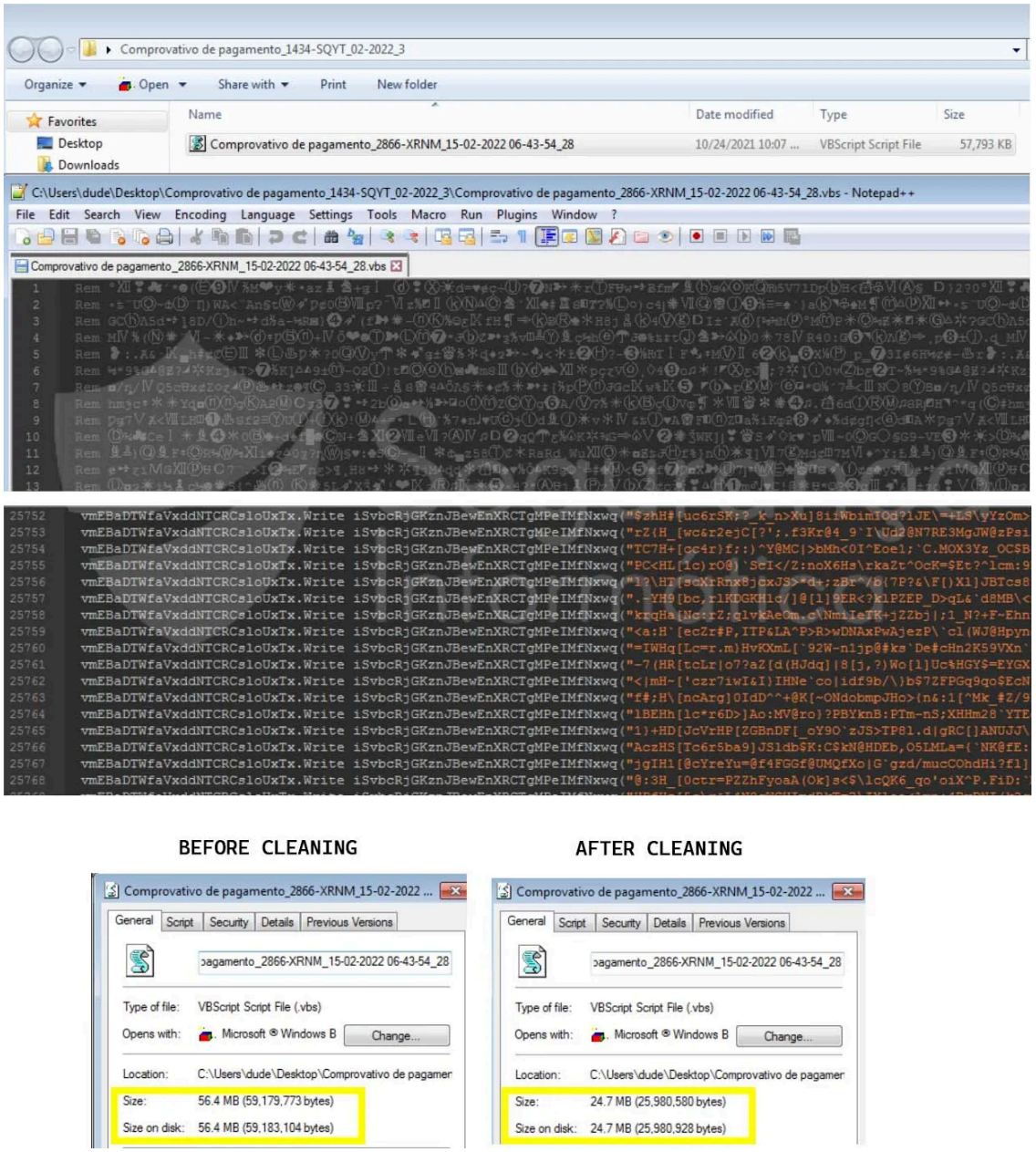


Figure 3: *Lampions' VBS loader size before and after removing the junk sequences.*

The final file after the cleaning process has around 24.7 MB, and it is responsible for creating other files, including:

- a 2nd VBS file with a random name (**2nd_stage_vbs**) that will download the Lampions' final stage – two DLLs from AWS S3 buckets
- other VBS file that will execute the previous file by using a scheduled task also created by the 1st VBS loader.

The next figure presents the structure of the Lampions' VBS loader after the cleaning and deobfuscation process.

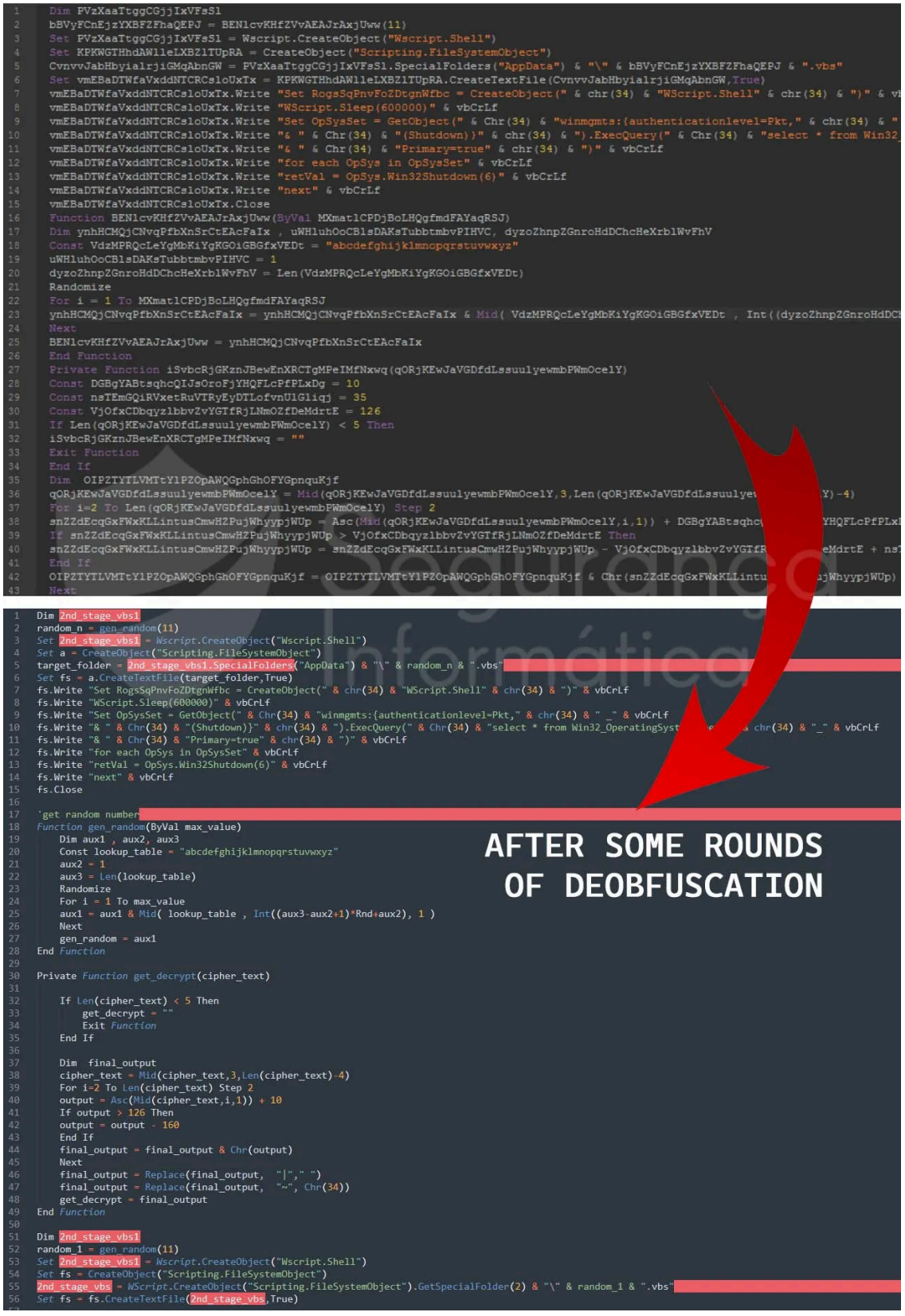


Figure 4: *Lampion's VBS loader after some rounds of deobfuscation.*

As mentioned, the 1st stage (***Comprovativo de pagamento_2866-XRNM_15-02-2022 06-43-54_28.vbs***) creates a new VBS file (2nd_stage_vbs) inside the ***%AppData%\Local\Temp*** folder with a random name (***sznyetzkkg.vbs***).

Also, another VBS (***jghfszcekwr.vbs***) is created with code responsible for executing the previous VBS file (***sznyetzkkg.vbs***) via a scheduled task.

A scheduled task is created with the service description and author ***Administrator*** user associated. This scheduled task will execute the second VBS file **jghfszcekwr.vbs** that contains instructions to finally run the ***sznyetzkkg.vbs*** file (the 2nd VBS stage).

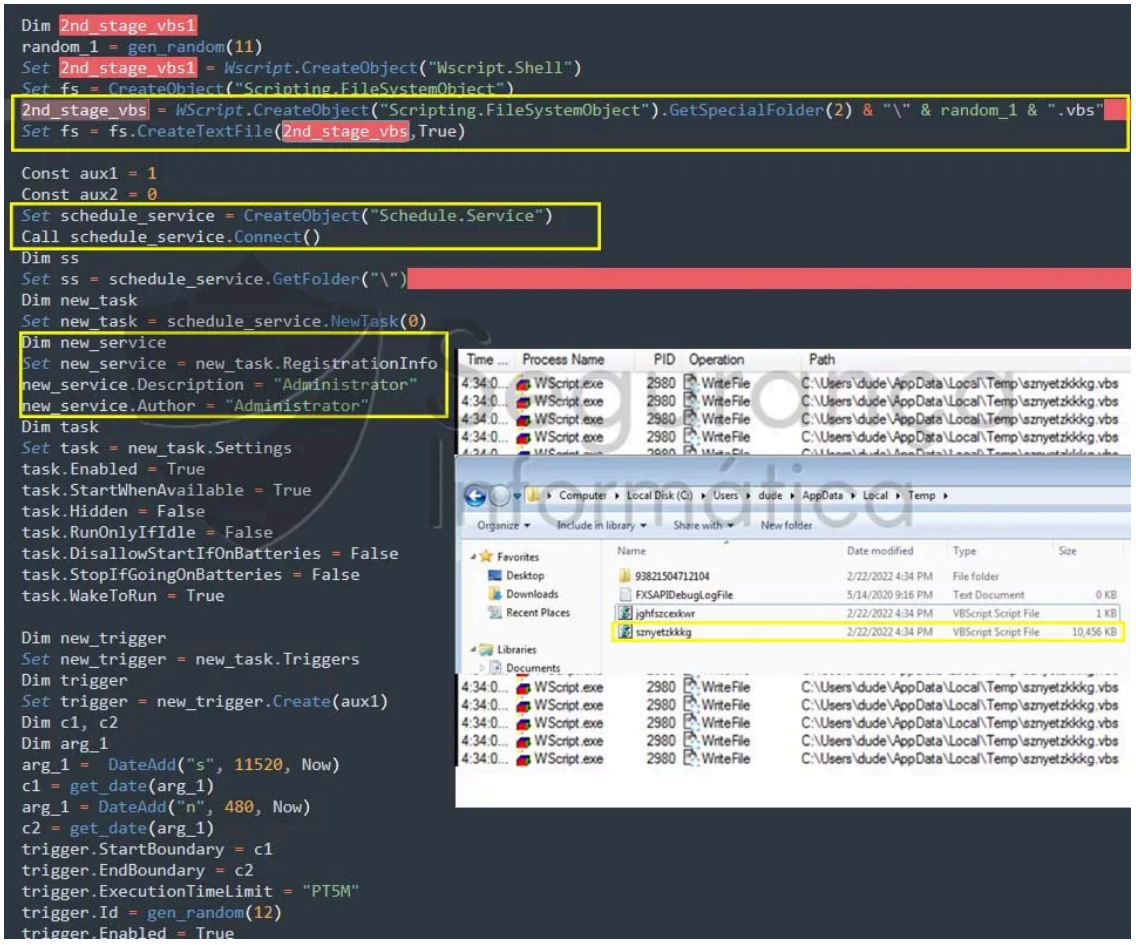


Figure 5: *Creation of the 2nd VBS file and the auxiliary VBS file. Also, the scheduled task responsible for creating the auxiliary VBS file is shown.*

After running the initial VBS file, the two additional VBS files are finally prepared to be triggered. That task is then performed by the scheduled task as presented in Figure 6. The source code of the ***jghfszcekwr.vbs*** file is quite simple and just executes the 2nd VBS file (***sznyetzkkg.vbs***). We believe this is just a procedure to make hard the malware analysis as well as difficult its detection – something we confirmed during the analysis, as the AVs don't detect properly those files during the malware infection chain.

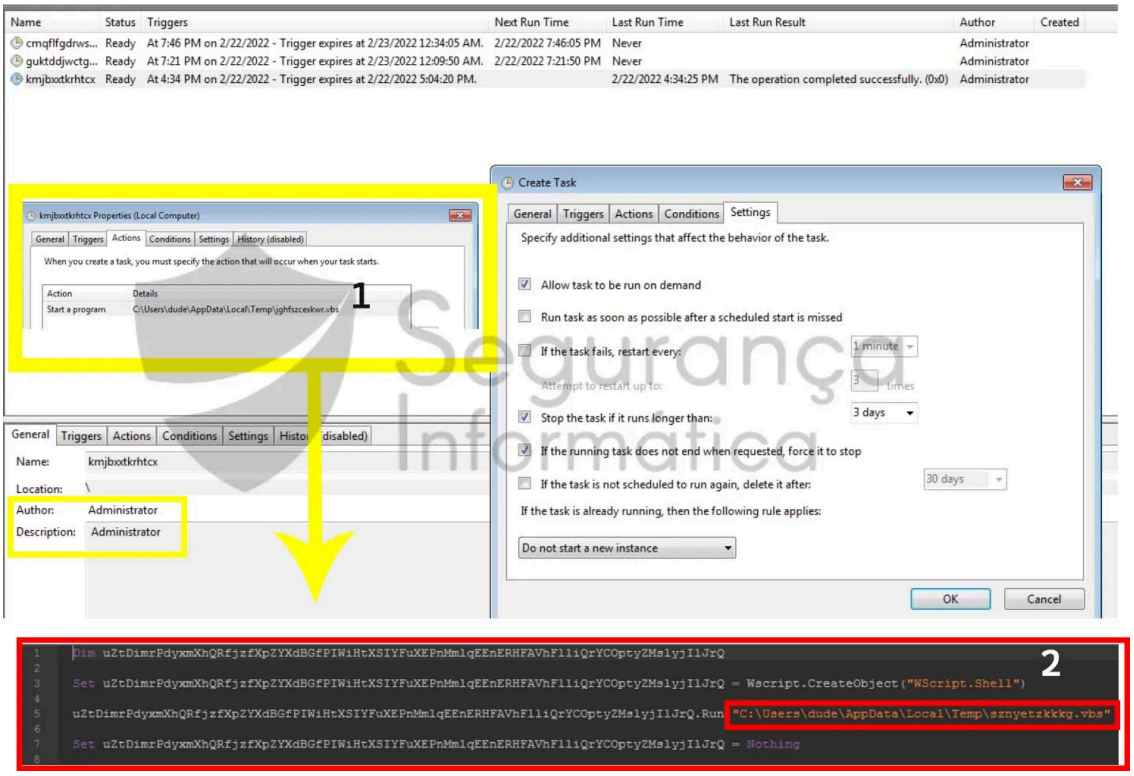


Figure 6: *Schedule task (**1**) responsible for executing an auxiliary VBS (**2**) file which in turn runs the second VBS stage.*

After that, the VBS file dubbed ***sznyetzkkg.vbs*** is executed. All the steps highlighted in Figure 7 are typically known from the last Lampions campaigns. This VBS file is quite similar to their predecessors, and it performs some tasks:

- Deletes all the files from the startup folder with the following extension: ***lnk, vbs, cmd, exe, bat and js***.
- Decrypts the URLs containing the final stage of Lampion trojan.
- Creates a .cmd file into the Windows startup folder to maintain persistence.

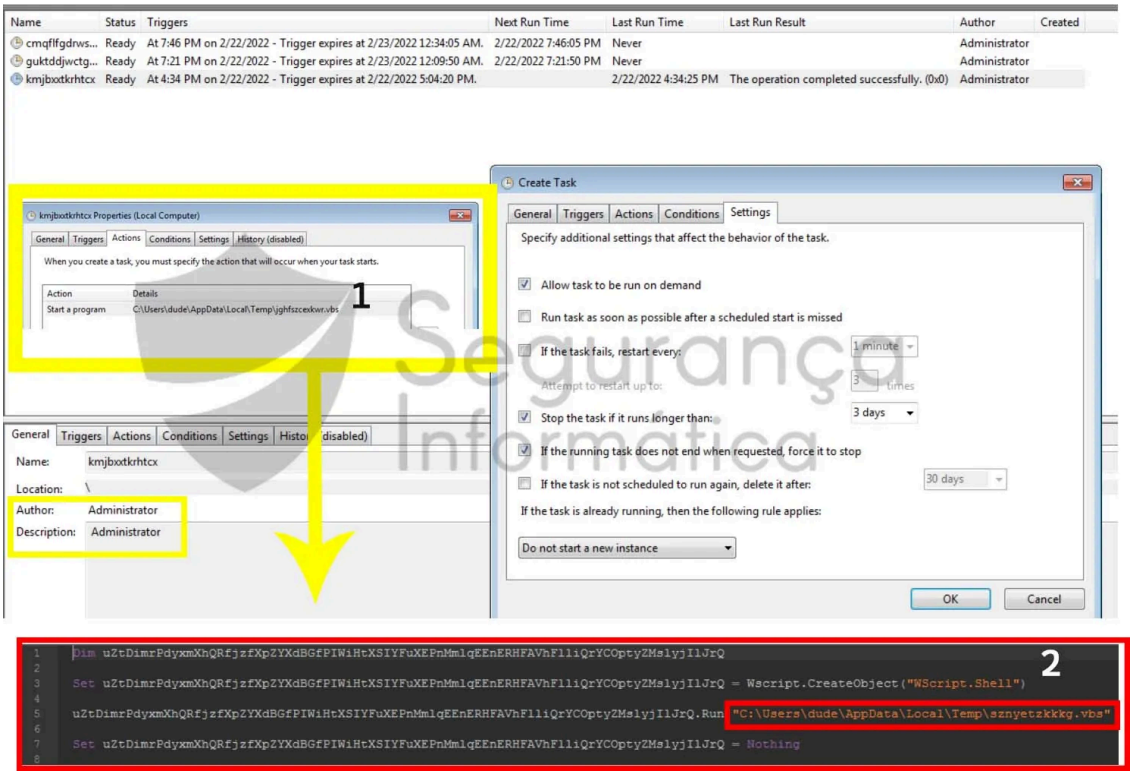


Figure 7: *Source-code of the 2nd VBS file and the encrypted URLs that will download the last stage of the Lampion trojan banker.*

From this point, the modus operandi and TTP are the same observed since 2019. The clear sign is the **same algorithm** used in 2019 to decrypt the hardcoded strings with the malicious URLs was used. The script can be downloaded from GitHub **here**.

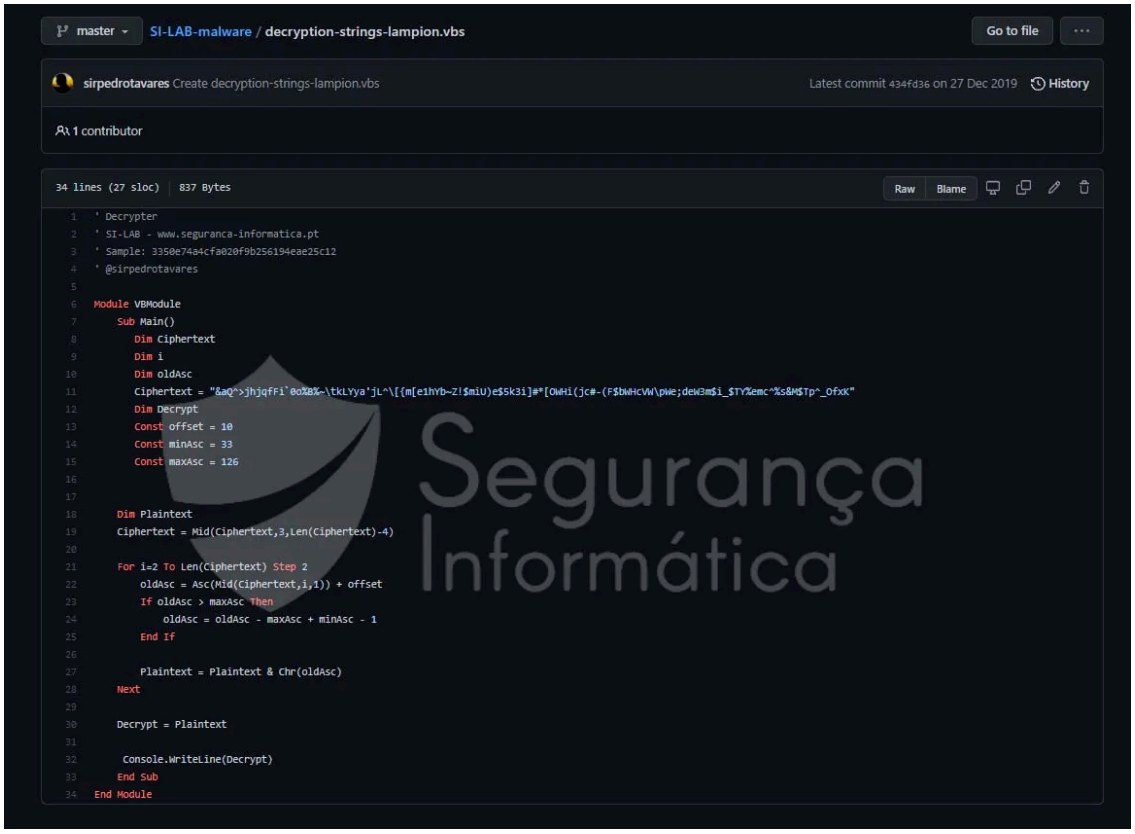


Figure 8: *Lampion trojan VBS decryptor.*

After running the script, we obtained the malicious URLs that download the next stage of Lampion trojan. Once again, the AWS S3 buckets were the criminals' choice, as observed in the last releases of this malware.

```
1. encrypted: "O{'^Yj7jRf:i_0<%r%#c=o{f=[Rhbi:e6dUWDb3isjRkt\U\0ik$zit)i$?kYi`#\
[DWcifjR#e(n$$WxcwW2pPe;dqWomFi3$ZYDeZc8%TiTeNflhYW>j][5ivj+[B$*pX_Dfl'"
2. decrypted: https://mypersonalstuffs.s3.us-east-2.amazonaws.com/soprateste.zip
3.
4. encrypted: "eg1^xj5jZf}iP0a%r%
<cZo[fU[(h&i8e9dZWmb%ijjOkz\M\+iz$Tiv)E$Qkxiq#M[bW<iDjO#4(A$kWfc2WJp`epdoWgm$i.$
s#F*R-"
5. decrypted: https://mypersonalstuffs.s3.us-east-2.amazonaws.com/P-17-4
```

The first DLL (the trojan loader) is a point of interest in this analysis. This file was also enlarged with lots of random BMP images inside – a well-known technique **that is being used by Latin American gangs** in their malware. This is a clear sign of cooperation between the several groups.

The ***P-17-4 DLL*** is then renamed when downloaded and injected into the memory via the DLL injection technique. The EAT function "***mJ8Lf9v0GZnptOVNB2I***" is triggered to start the DLL loader.C:\Windows\System32\rundll32.dll\"%AppData%\Local\Temp\rand_folder\random_name.dll" mJ8Lf9v0GZnptOVNB2I

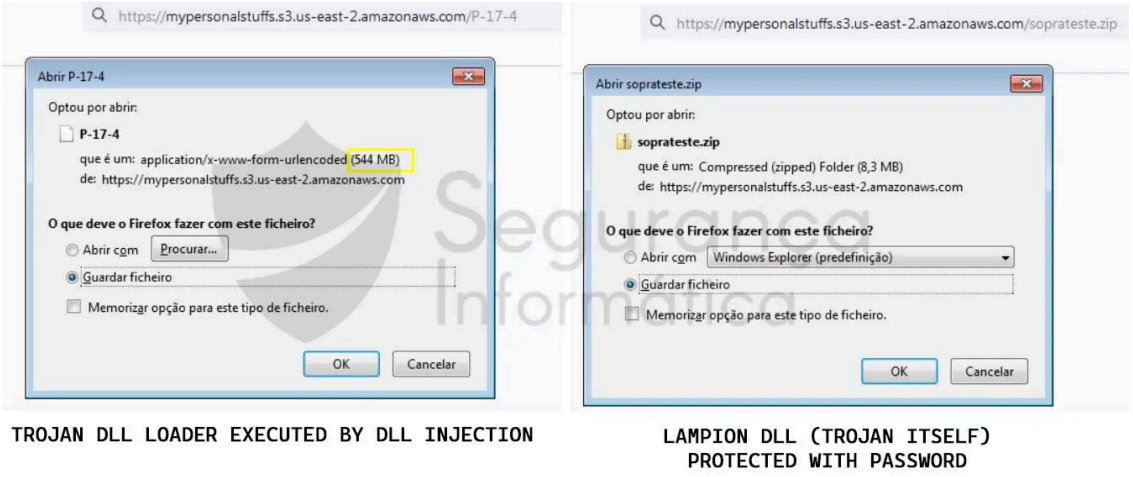


Figure 9: *Lampion DLLs – release 212 (February 2022).*

The main goal of the DLL loader is just to unzip the 2nd DLL called "***soprateste.zip***" which is protected with a hardcoded password. All the process from this point is the same as the last articles we have published, namely:

- **Targeting Portugal: A new trojan 'Lampion' has spread using template emails from the Portuguese Government Finance & Tax** – DECEMBER 2019
- **Lampion malware origin servers geolocated in Turkey**, FEBRUARY 2020
- **Lampion malware v2 February 2020**, FEBRUARY 2020
- **New release of Lampion trojan spreads in Portugal with some improvements on the VBS downloader,** JULY 2020
- **Lampion trojan disseminated in Portugal using COVID-19 template**, FEBRUARY 2021

Details of the Lampion release 212

The single task of the first DLL is just to unzip the 2nd one with a hardcoded password. As usual, the DLL inside **soprateste.zip** carries a message in Chinese for researchers:

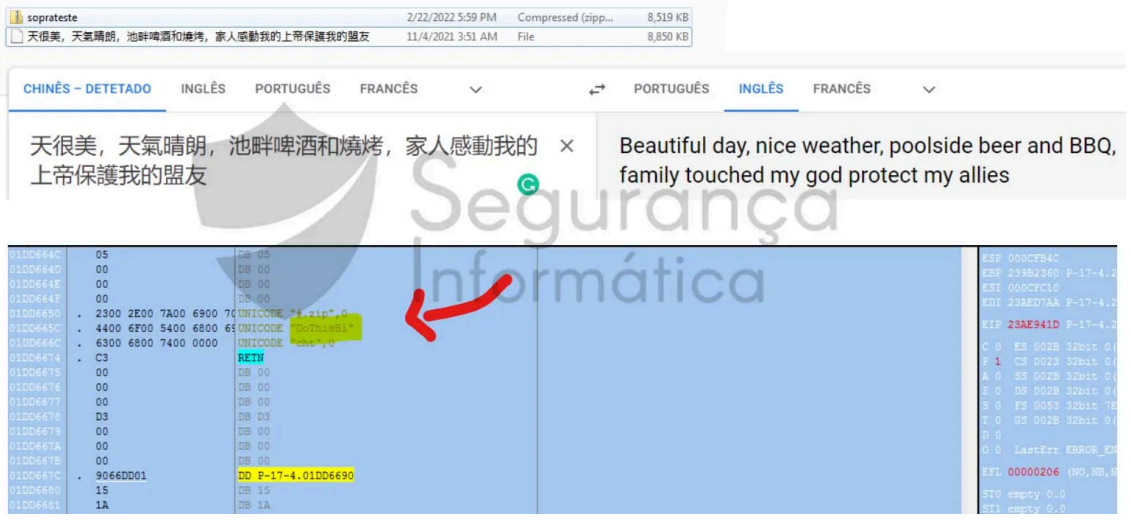
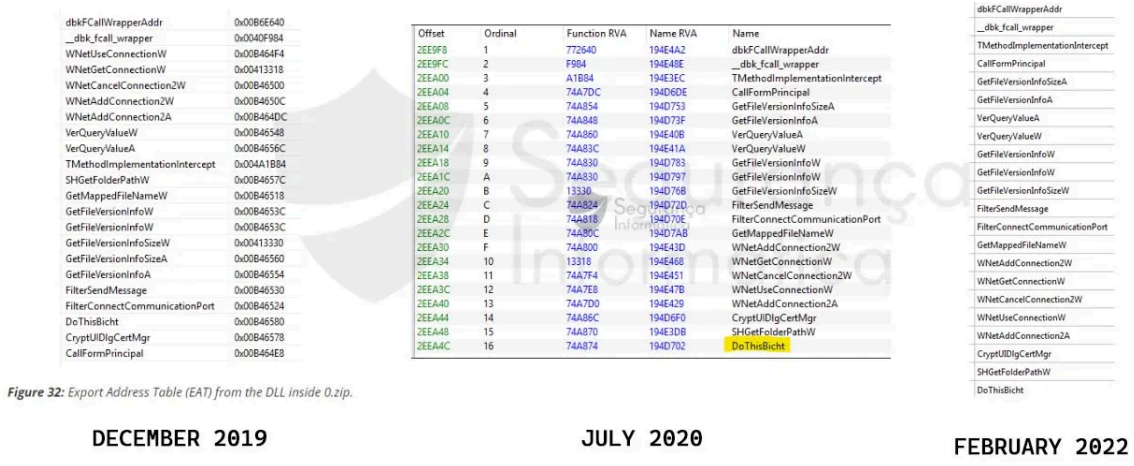


Figure 10: *Message hardcoded inside the soprateste.zip DLL (the Lampion itself) and part of the unzip process.*

As usual, the trojan maintains intact its EAT since 2019. The call "**DoThisBicht**" is invoked from the DLL loader, and the malware starts its malicious activity. Figure 11 below shows the comparison of the EAT between the different versions from 2019 to 2022, and no differences were noticed.



dbkFCallWrapperAddr	0x00B6E640
__dbk_fcall_wrapper	0x0040F984
WNetUseConnectionW	0x00B464F4
WNetGetConnectionW	0x00413318
WNetCancelConnection2W	0x00B46500
WNetAddConnection2W	0x00B4650C
WNetAddConnection2A	0x00B464DC
VerQueryValueW	0x00B46548
VerQueryValueA	0x00B4656C
TMethodImplementationIntercept	0x004A1B84
SHGetFolderPathW	0x00B4657C
GetMappedFileNameW	0x00B46518
GetFileVersionInfoW	0x00B4653C
GetFileVersionInfoW	0x00B4653C
GetFileVersionInfoSizeW	0x00413330
GetFileVersionInfoSizeA	0x00B46560
GetFileVersionInfoA	0x00B46554
FilterSendMessage	0x00B46530
FilterConnectCommunicationPort	0x00B46524
DoThisBicht	0x00B46580
CryptUIDlgCertMgr	0x00B46578
CallFormPrincipal	0x00B464E8

Offset	Ordinal	Function RVA	Name RVA	Name
2EE9F8	1	772640	194E4A2	dbkFCallWrapperAddr
2EE9FC	2	F984	194E48E	__dbk_fcall_wrapper
2EEA00	3	A1B84	194E3EC	TMethodImplementationIntercept
2EEA04	4	74A7DC	194D6DE	CallFormPrincipal
2EEA08	5	74A854	194D753	GetFileVersionInfoSizeA
2EEA0C	6	74A848	194D73F	GetFileVersionInfoA
2EEA10	7	74A860	194E40B	VerQueryValueA
2EEA14	8	74A83C	194E41A	VerQueryValueW
2EEA18	9	74A830	194D783	GetFileVersionInfoW
2EEA1C	A	74A830	194D797	GetFileVersionInfoW
2EEA20	B	13330	194D76B	GetFileVersionInfoSizeW
2EEA24	C	74A824	194D72D	FilterSendMessage
2EEA28	D	74A818	194D70E	FilterConnectCommunicationPort
2EEA2C	E	74A80C	194D7AB	GetMappedFileNameW
2EEA30	F	74A800	194E43D	WNetAddConnection2W
2EEA34	10	13318	194E468	WNetGetConnectionW
2EEA38	11	74A7F4	194E451	WNetCancelConnection2W
2EEA3C	12	74A7E8	194E47B	WNetUseConnectionW
2EEA40	13	74A7D0	194E429	WNetAddConnection2A
2EEA44	14	74A86C	194D6F0	CryptUIDlgCertMgr
2EEA48	15	74A870	194E3DB	SHGetFolderPathW
2EEA4C	16	74A874	194D702	DoThisBicht

dbkFCallWrapperAddr
__dbk_fcall_wrapper
TMethodImplementationIntercept
CallFormPrincipal
GetFileVersionInfoSizeA
GetFileVersionInfoA
VerQueryValueA
VerQueryValueW
GetFileVersionInfoW
GetFileVersionInfoW
GetFileVersionInfoSizeW
FilterSendMessage
FilterConnectCommunicationPort
GetMappedFileNameW
WNetAddConnection2W
WNetGetConnectionW
WNetCancelConnection2W
WNetUseConnectionW
WNetAddConnection2A
CryptUIDlgCertMgr
SHGetFolderPathW
DoThisBicht

Figure 32: Export Address Table (EAT) from the DLL inside 0.zip.

DECEMBER 2019 JULY 2020 FEBRUARY 2022

Figure 11: *Export Address Table (EAT) from the DLL inside the soprateste.zip file (the Lampion trojan itself).*

The target brands are the same observed in the past campaigns, with the focus on Brazilian and Portuguese banking organizations.

```
0x5106a0c (28): banco montepio
0x5106a38 (16): montepio
0x5106a6c (26): millenniumbcp
0x5106aa8 (18): Santander
0x5106ac8 (14): BPI Net
0x5106ae4 (18): Banco BPI
0x5106b18 (24): Caixadirecta
0x5106b40 (42): Caixadirecta Empresas
0x5106b8c (20): NOVO BANCO
0x5106bc4 (14): EuroBic
0x5106bfa (16): Credito Agricola
0x5106c24 (20): Login Page
0x5106c48 (22): CA Empresas
0x5106c80 (18): Bankinter
0x5106cb4 (20): ActivoBank
0x5107118 (36): itauaplicativo.exe
0x5109568 (14): TravaBB
0x5109586 (32):  Banco do Brasil
0x51095b4 (16): Traazure
0x51095d6 (32):  Caixa Economica
0x5109604 (20): Travsantos
0x510962a (20):  Santander
0x510964c (14): Travsic
0x510966a (14):  Sicred
0x5109688 (14): Travite
```

```
0x51096c0 (18): Travdesco
0x51096e2 (18):  Bradesco
0x5109704 (22): BANRITRAVAR
0x510972a (18):  Banrisul
0x510974c (20): TravaBitco
0x5109772 (32):  Mercado Bitcoin
0x51097a0 (14): Travcit
0x51097be (18):  Citibank
0x51097e0 (18): Travorigs
0x5109802 (30):  Banco Original
0x5109830 (18): SICTRAVAR
0x5109852 (14):  Sicoob
```

When started, the trojan collects information about the opened processes on the target machine. If the title of the pages matches the hardcoded strings presented above, then it starts the malicious overlay process that presents fake messages and windows impersonating the target bank to lure the victims.

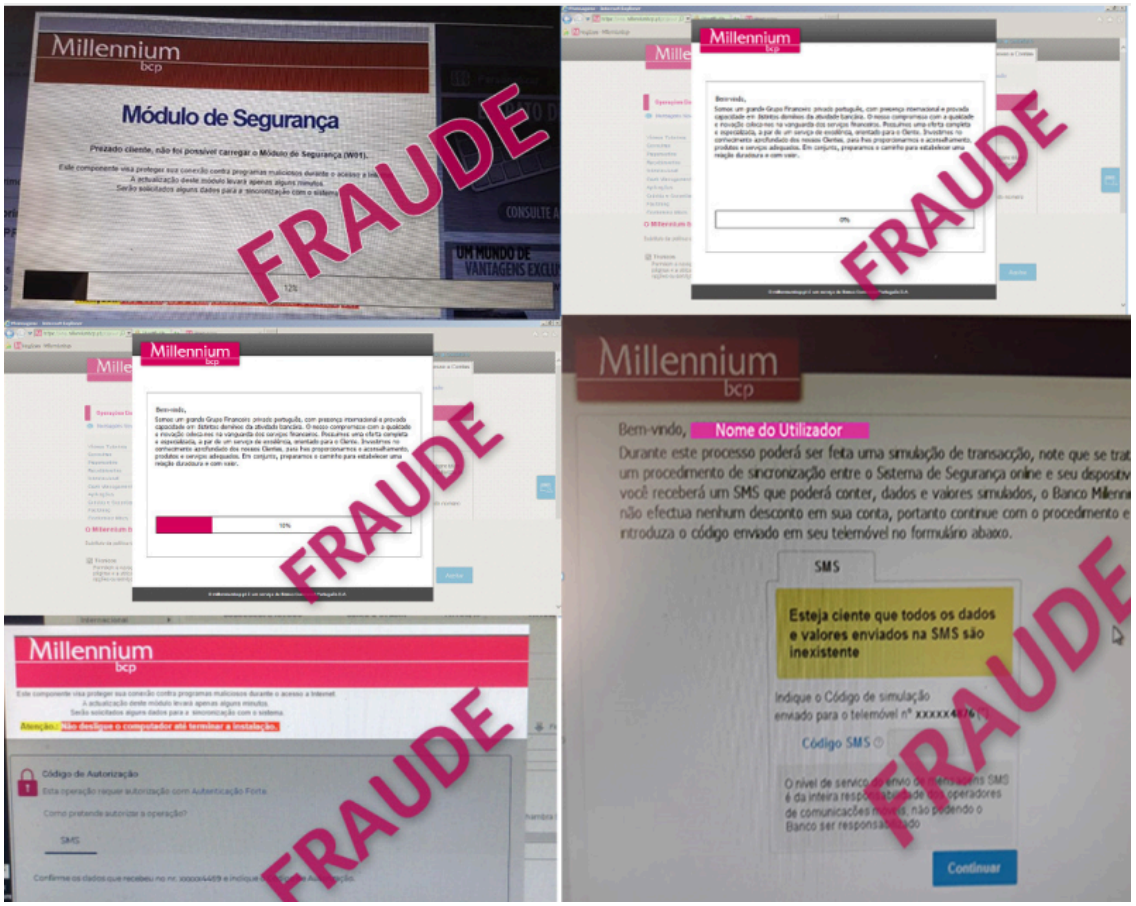


Figure 12: *Lampion overlay screens (courtesy of MllenniumBCP – Portugal).*

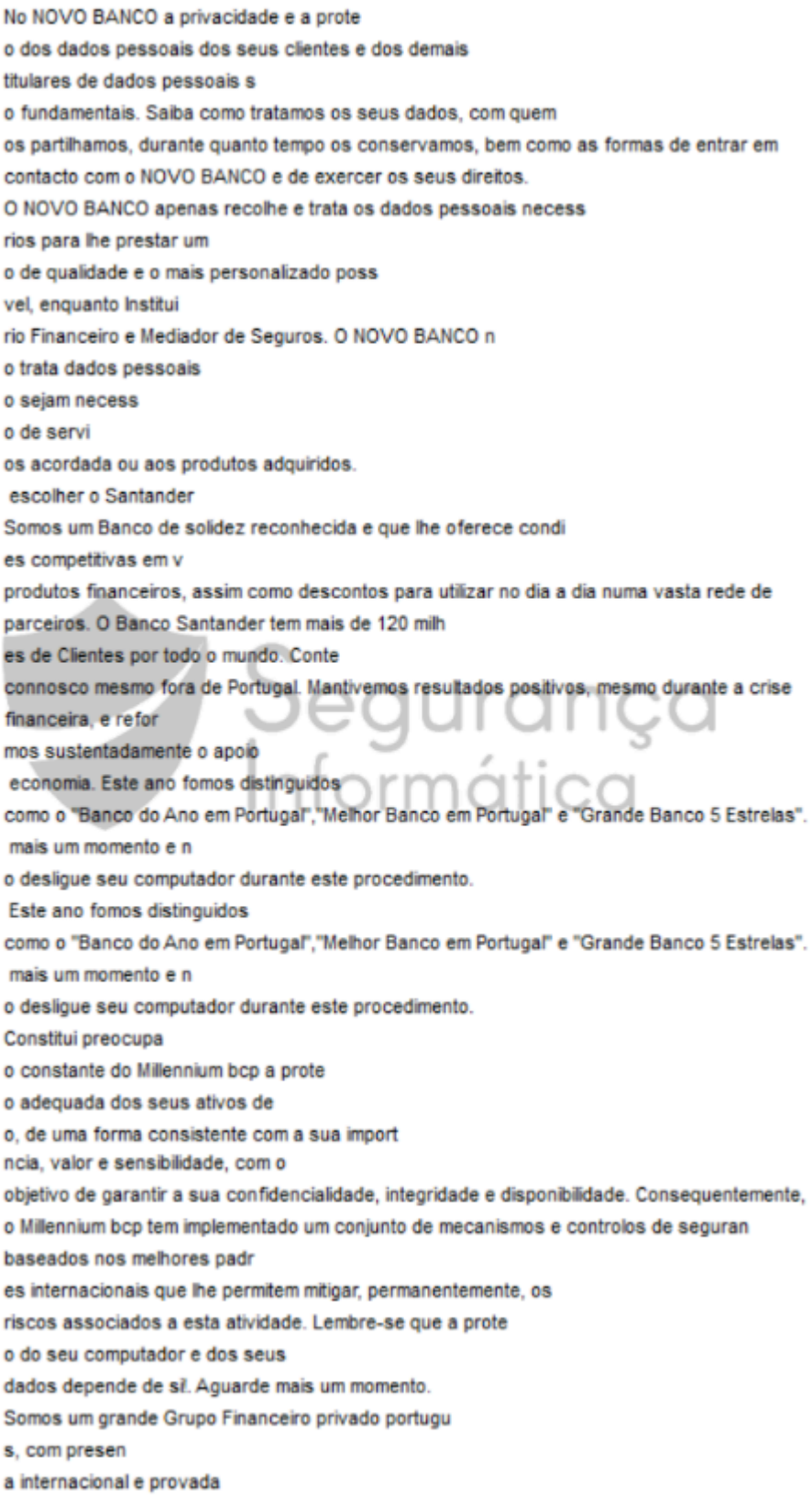


Figure 13: *Part of the hardcoded messages present on the Delphi forms that are exhibited during the trojan execution.*

As mentioned, Lampion is using the same C2 server geolocated in Russia at least for two years. Figure 14 compares the Lampion release 207 – from 2020 – and the new release 212 – February 2022. As presented, the

server “5.188.9.28” has been used at least since 2020 by the criminals’ gang in order to orchestrate all the operations.

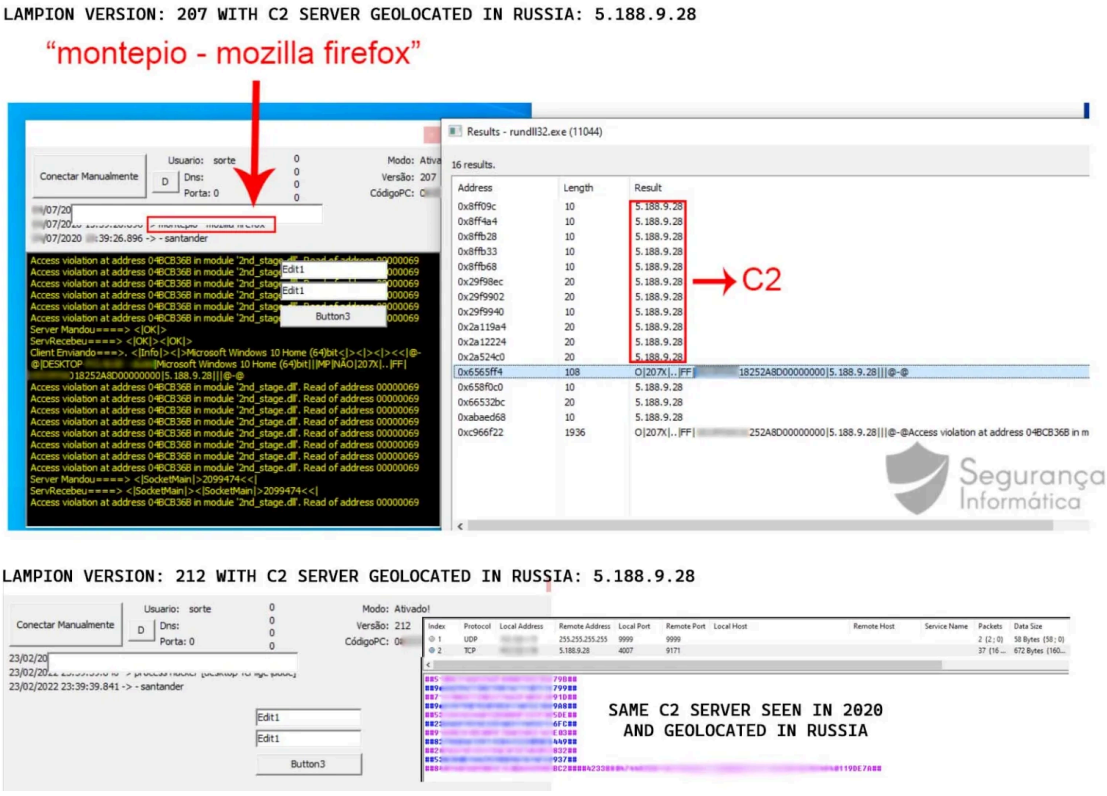


Figure 14: *Lampion is using the same C2 server observed in 2020 and gelocated in Russia.*

Interestingly, the C2 server – a Windows machine – has the Microsoft RPC Endpoint Mapper service exposed, which allows mapping some of the services running on the machine, associated pipes, hostname, etc.

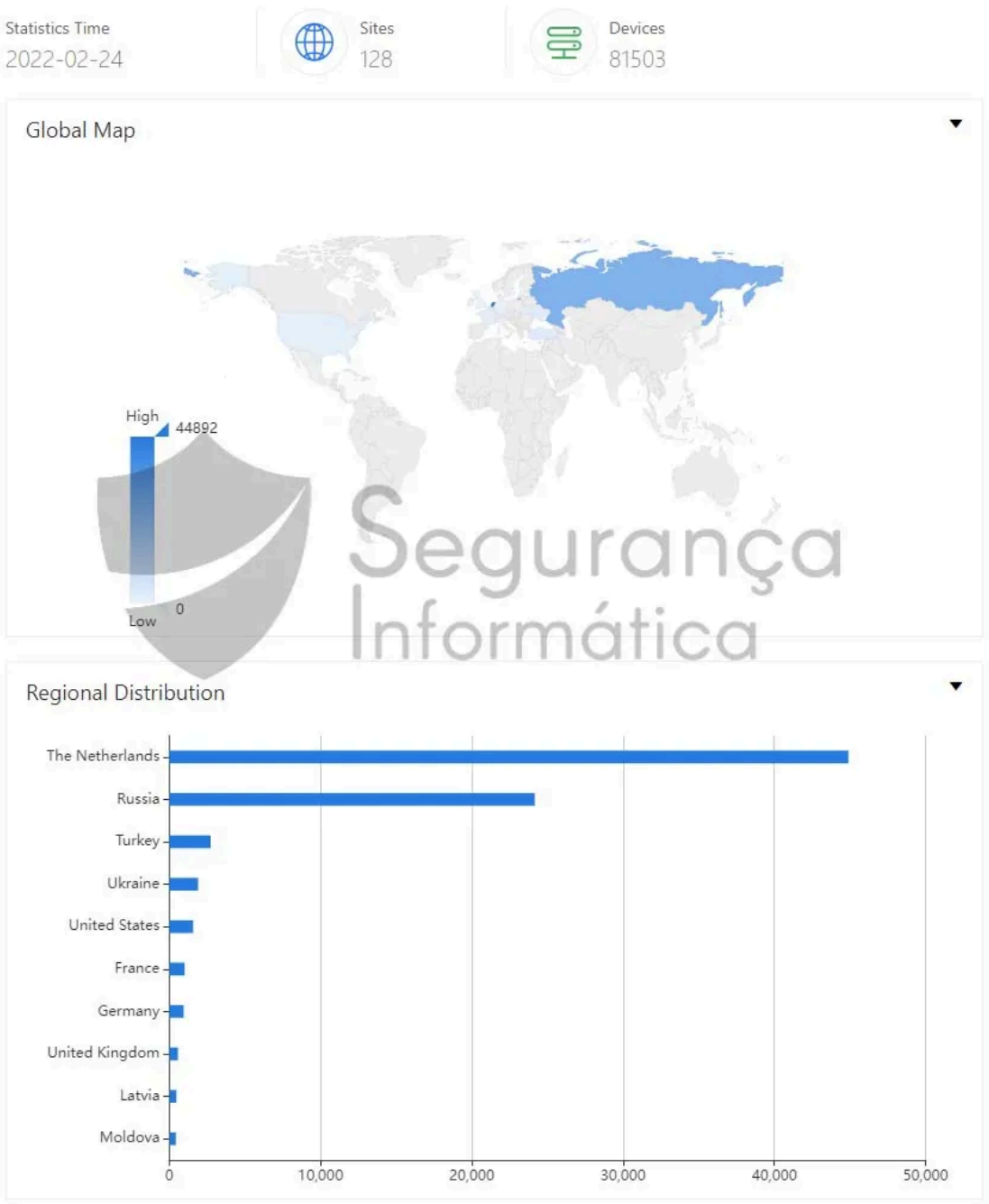
Through this information, it was possible to obtain the hostname of the remote machine: **WIN-344VU98D3RU**.

After a quick search, the hostname seems to have already been associated with other malicious groups operating different types of malware, such as the **bazaar** (see the article here), and also **LockBit 2.0** ransomware (take a look here).

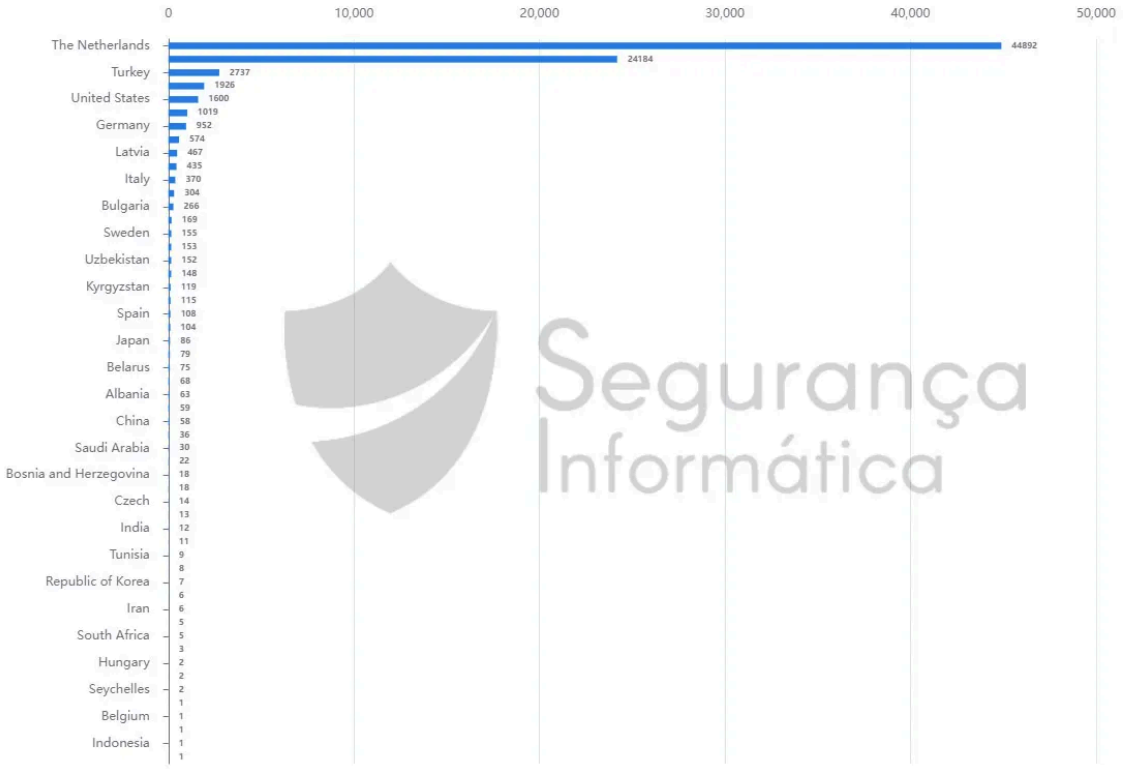
Figure 15: *IoCs related to the hostname used by Lampions C2 server (**__WIN-344VU98D3RU__*).*

Although it is not possible to confirm whether this is a hostname associated with other Cloud machines and used by legitimate systems, it was possible to identify that there are machines spread all over the world with the same hostname, and in some situations, only a few machines available per country.

In total, 81.503 machines were identified, with around 45k in The Netherlands, 25k in Russia, 2.5k Turkey, 2K Ukraine, 1.5k in US, etc.



The complete list of hosts can be found below.



Final Thoughts

Nowadays, we are facing a growing of Brazilian trojans at a very high speed. Each one of them with its peculiarities, TTPs, etc. With this in mind, criminals achieve a FUD condition that allows them to avoid detection and impact a large number of users around the world.

In this sense, monitoring these types of IoCs is a crucial point now, as it is expected that in the coming weeks or months new infections or waves can emerge.

Mitre Att&ck Matrix and Indicators of Compromise (IOCs) are available in the original post published by the cybersecurity researchers Pedro Tavares:

https://seguranca-informatica.pt/the-hidden-c2-lampion-trojan-release-212-is-on-the-rise-and-using-a-c2-server-for-two-years/#.Yi32dnrMK5d

About the author Pedro Tavares:

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

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner=”9″]	[adrotate banner=”12″]

Pierluigi Paganini

(SecurityAffairs – hacking, Lampion trojan)

[adrotate banner="5″]

[adrotate banner="13″]

Source: https://securityaffairs.co/wordpress/128975/malware/hidden-c2-lampion-trojan-release-212.html