How to expose a potential cybercriminal due to misconfigurations

cybergeeks.tech/how-to-expose-a-potential-cybercriminal-due-to-misconfigurations

Summary

We've investigated a new phishing campaign spreading malicious documents that exploit the CVE-2017-0199 and CVE-2017-11882 vulnerabilities.

The purpose of this campaign is to deploy the Lokibot stealer on the infected machines. In our investigation we found misconfigurations on the malicious domains that allowed us to identify a hostname which was a name server for two scam domains registered in Brazil.

We believe that the owner of these domains might be involved in the malicious campaign.

Technical analysis

We begin the analysis with a document that impersonates the Romanian ANAF (National Agency for Fiscal Administration) called "Factura fiscala ANAF270622.xlsx" (SHA256: 098335ca421ca8501fd243714fd02457ebbaa40dd6f91cf1ab61a58c415a27a0). The document was downloaded from https://app.any.run/tasks/e5624c90-9c9c-4f35-a80a-3beed6370c35/.

The malicious document is a xlsx file that contains a blurred image which seems to be an invoice, as highlighted below:

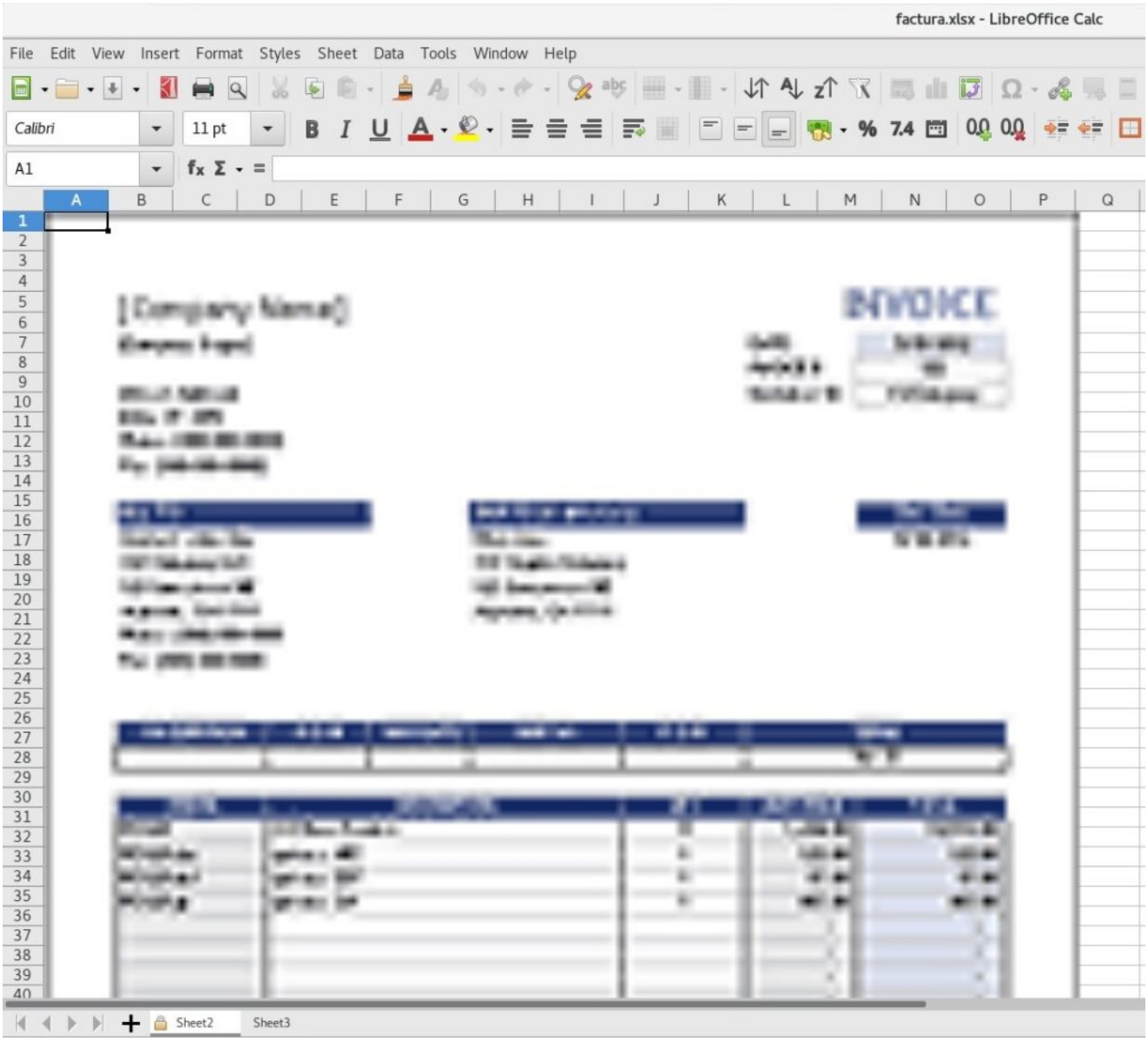

Figure 1

The file is an encrypted Excel document with a common password (“VelvetSweatshop”), as shown below:

```
remnux@remnux:~/Downloads/[redacted]$ file factura.xlsx
factura.xlsx: CDFV2 Encrypted
remnux@remnux:~/Downloads/[redacted]$ msoffcrypto-crack.py factura.xlsx
Password found: VelvetSweatshop
```

Figure 2

```
remnux@remnux:~/Downloads/[redacted]$ msoffcrypto-crack.py factura.xlsx -o factura2.xlsx
Password found: VelvetSweatshop
remnux@remnux:~/Downloads/[redacted]$ file factura2.xlsx
factura2.xlsx: Microsoft Excel 2007+
```

Figure 3

Using oledump it`s possible to determine that there is an embedded OLE object in the document:

```
remnux@remnux:~/Downloads/[redacted]$ oledump.py factura2.xlsx -i
A: xl/embeddings/oleObject1.bin
 A1:       626             '\x01Ole'
remnux@remnux:~/Downloads/[redacted]$ oledump.py factura2.xlsx -s A1 -d > obj
remnux@remnux:~/Downloads/[redacted]$ xxd obj
00000000: 0100 0002 131a 8c23 b822 8f5c 0000 0000  .......#."."\....
00000010: 0000 0000 0000 0000 3601 0000 e0c9 ea79  ........6......y
00000020: f9ba ce11 8c82 00aa 004b a90b 3201 0000  .........K..2...
00000030: 6800 7400 7400 7000 3a00 2f00 2f00 6200  h.t.t.p.:././.b.
00000040: 6c00 6f00 6f00 6b00 6500 7400 2e00 6700  l.o.o.k.e.t...g.
00000050: 6900 7400 6800 7500 6200 2e00 6900 6f00  i.t.h.u.b...i.o.
00000060: 4000 6900 7400 7300 7300 6f00 7400 6900  @.i.t.s.s.o.t.i.
00000070: 6e00 7900 2e00 6300 6f00 6d00 2f00 6600  n.y...c.o.m./.f.
00000080: 5900 5900 6200 4f00 0000 3f6f 27c4 d640  Y.Y.b.O...?o'..@
00000090: a6fe a78e 3a91 5eb2 ea65 6ffa 207c 4ee6  ....:.^..eo. |N.
000000a0: ef27 b96e 4c50 ed39 4daf e9e4 6f15 b742  .'.nLP.9M...o..B
000000b0: d2a5 a196 7c18 74db 94f6 c2fd a4e1 211f  ....|.t.......!.
000000c0: e0ca 6dd4 5b38 0267 4b8b 0515 502c 9b50  ..m.[8.gK...P,.P
000000d0: a8e3 2cfa 7803 abaf 06bc c6fe 0249 34a3  ..,.x........I4.
000000e0: ba41 f1d7 63c8 7a83 53da 1185 4988 fdeb  .A..c.z.S...I...
000000f0: a634 ca3d acd4 82b2 c235 fb7a b938 08f5  .4.=.....5.z.8..
00000100: fd0b c7f9 e37a d30d e41f 90af dca9 6293  .....z........b.
00000110: 4d1a f7dc 990b 7a62 47e6 e0f5 472a 1e94  M.....zbG...G*..
00000120: 27ad 6cb6 5dd4 8b83 7eda fe18 890f 49c9  '.l.]...~.....I.
00000130: 1d14 3557 be25 143f 164b f7ec 2fa3 f400  ..5W.%.?.K../...
00000140: bca3 6490 4f50 2766 a188 de3e ce39 2e0a  ..d.OP'f...>.9..
00000150: 96a6 062f 9da6 cfc8 aee3 c0df f120 0ab9  .../......... ..
00000160: 3a6e ffff ffff 0000 0000 0000 0000 0000  :n..............
00000170: 0000 0000 0000 dc00 0000 6300 6f00 4800  ..........c.o.H.
00000180: 6f00 4200 6d00 3200 4600 3100 6100 5000  o.B.m.2.F.1.a.P.
00000190: 4900 5800 3700 4700 5a00 6100 4600 6b00  I.X.7.G.Z.a.F.k.
000001a0: 5700 4500 7200 7500 4200 6400 6f00 4400  W.E.r.u.B.d.o.D.
000001b0: 7800 4400 5200 4f00 7700 4700 4b00 6e00  x.D.R.O.w.G.K.n.
000001c0: 4e00 3900 5800 7000 6200 7200 3300 3000  N.9.X.p.b.r.3.0.
000001d0: 6e00 4800 4700 4f00 3600 6900 7800 7600  n.H.G.O.6.i.x.v.
000001e0: 6400 5600 6e00 7800 6e00 3700 6d00 7800  d.V.n.x.n.7.m.x.
000001f0: 4100 5000 6100 6500 5a00 3400 3300 5700  A.P.a.e.Z.4.3.W.
00000200: 7900 5500 3700 6d00 3400 5600 5300 6600  y.U.7.m.4.V.S.f.
00000210: 5700 7600 6700 5a00 5400 4f00 6800 7200  W.v.g.Z.T.O.h.r.
00000220: 7600 5500 4600 5500 3900 4100 6800 6a00  v.U.F.U.9.A.h.j.
00000230: 6800 7000 5300 4300 6e00 3900 4800 4900  h.p.S.C.n.9.H.I.
00000240: 7000 6900 6700 7800 3600 3400 6a00 5900  p.i.g.x.6.4.j.Y.
00000250: 7700 4800 0000 ef77 5021 350f 0107 5309  w.H....wP!5...S.
00000260: ea7a 9655 9e60 065a 3354 b005 3440 e361  .z.U.`.Z3T..4@.a
00000270: 153c                                     .<
```

Figure 4

The document tries to exploit a vulnerability found in Microsoft Office and WordPad, that is described in CVE-2017-0199 . If successful, the malware would download a file found at http[:]//itssotiny.com/fYYbO (returns 404 at this time). However, according to VirusTotal, the link redirected to http[:]//192.3.239.42/document/77.doc (still active). Figure 5 reveals that there are two documents hosted in the same location:

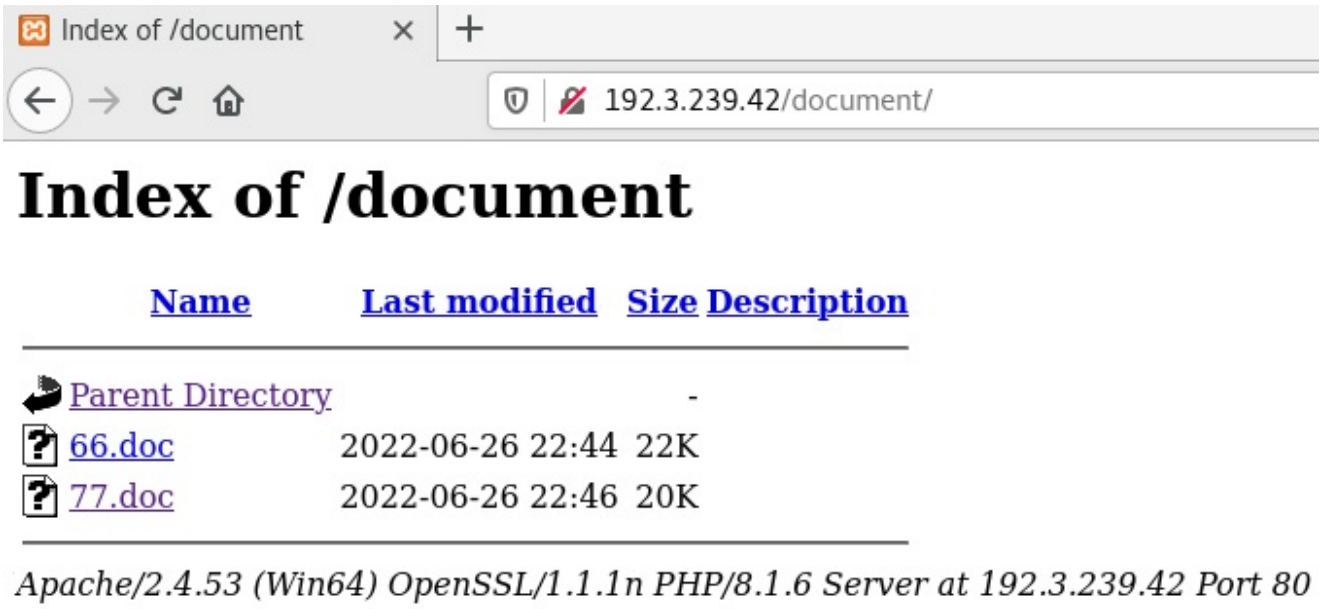

Figure 5

The 77.doc file is an obfuscated RTF file, which exploits the another Microsoft Office vulnerability, CVE-2017-11882 :

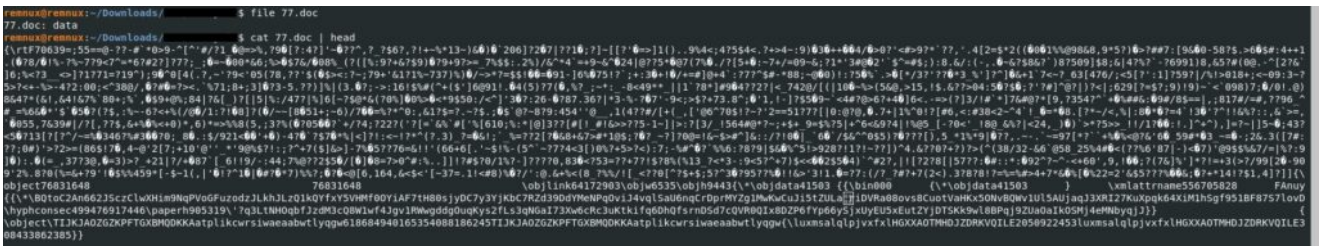

Figure 6

The rtfdump.py script is utilized to list groups and the structure of the RTF file:

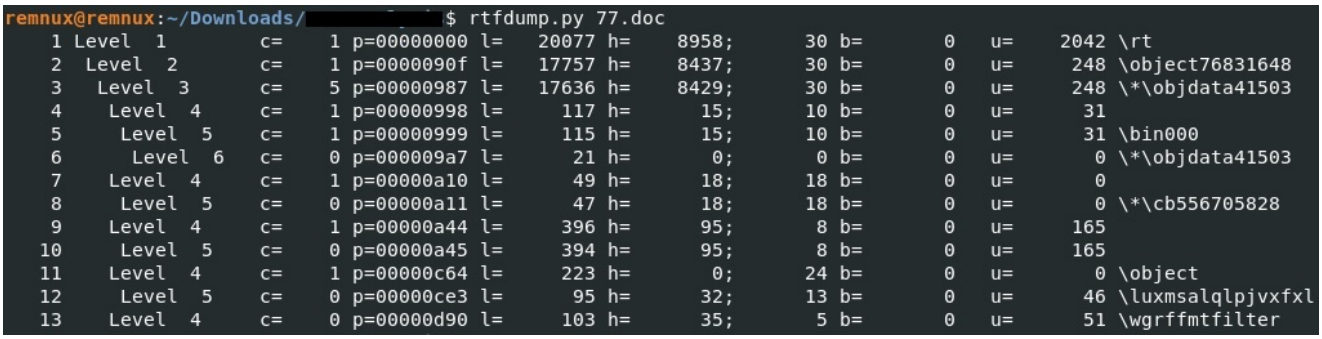

Figure 7

The Microsoft Equation Editor process that can be identified in the sandbox analysis is a strong indicator that the vulnerability is indeed CVE-2017-11882, which is a vulnerability in Microsoft Equation Editor (https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/17-year-old-ms-office-flaw-cve-2017-11882-actively-exploited-in-the-wild).

The final stage consists of downloading the Lokibot stealer from http[:]//192.3.239.42/77/vbc.exe (https://www.virustotal.com/gui/file/d243ac3d475a2e3dad62640525d3b4f102bb8140cc84436

3d61e95ea5fc4f8fb/detection).

Due to the attacker's mistake, phpinfo.php can be accessed by anybody and reveals crucial information about the potential attacker. As we can see in figure 8, the hostname is "WIN-2NF07F1AQLT" and it runs on a Windows Server 2016 machine:

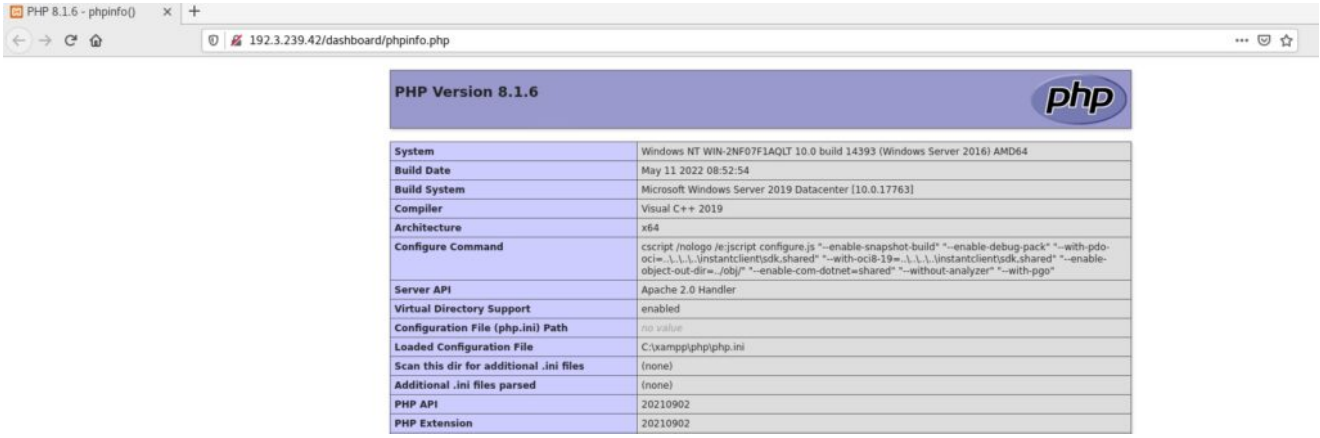

Figure 8

We have expended the attacker's infrastructure via OSINT. The following files/IP addresses could be identified:

http[:]//192.3.239.42/receipt/88.doc

http[:]//192.3.239.42/receipt/99.doc

http[:]//192.227.129.26/document/receipt.doc

http[:]//192.3.239.42/office/100.doc

http[:]//192.3.239.42/office/110.doc

192.227.168.194, 107.175.218.40, 104.168.32.21, 104.168.32.14

As we can see in figure 9, the hostname is the same for a different domain:

Figure 9

We have identified another hostname for an older campaign – “WIN-3JS0MA784YQ”:

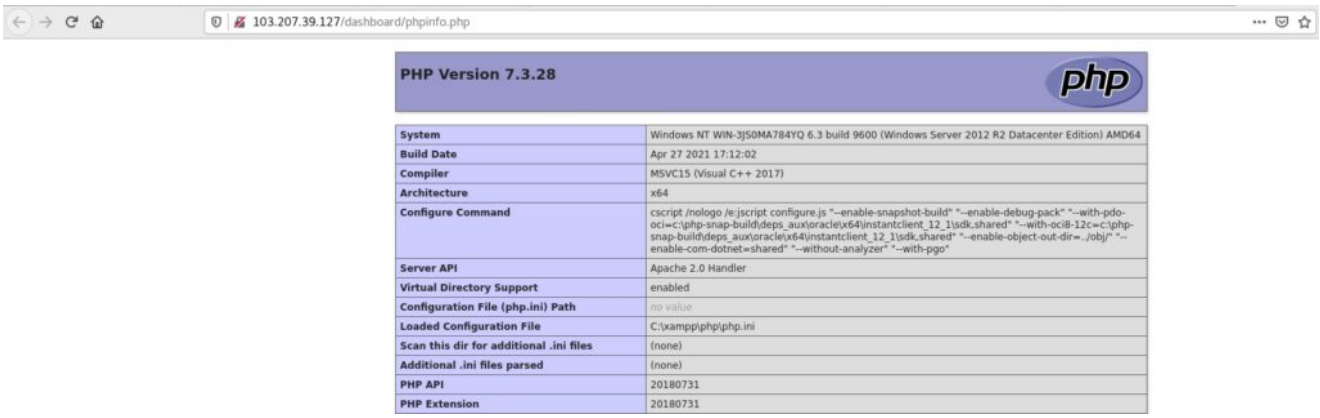

Figure 10

We’ve performed an OSINT investigation and found that the “WIN-2NF07F1AQLT” hostname appears as a name server for two domains registered in Brazil: Webcamer.com[.]br and Citydesconto.com[.]br. According to website.informer.com, these 2 domains were registered by an individual “Noe Yvert Etoua Evina” with the noeyvert@gmail.com email address:

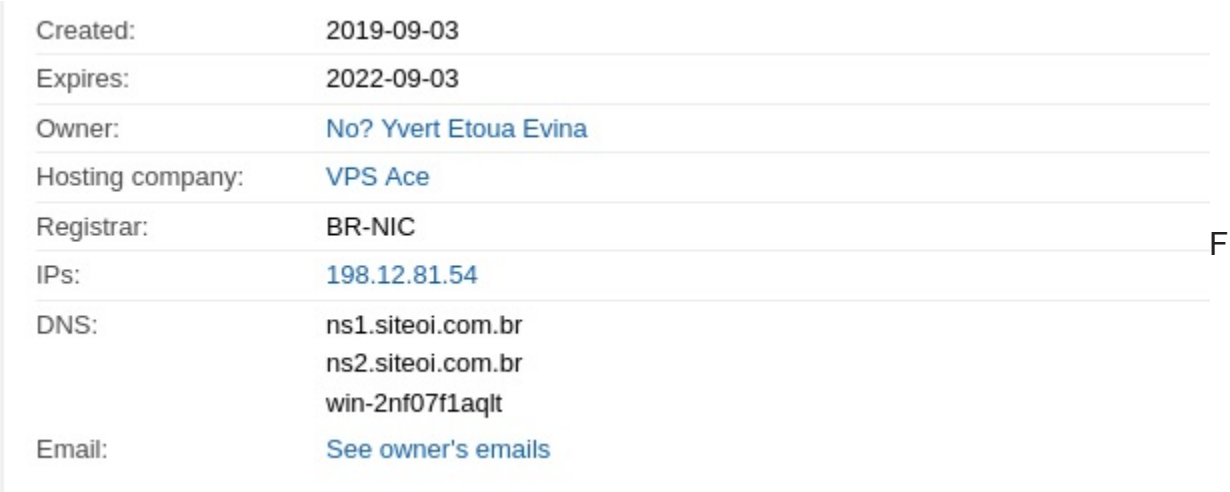

Figure 11

These two domains seem to be scam domains. An individual with the same name appears in multiple judicial processes on jusbrasil.com.br.

Indicators of Compromise

SHA256: 098335ca421ca8501fd243714fd02457ebbaa40dd6f91cf1ab61a58c415a27a0

SHA256: d243ac3d475a2e3dad62640525d3b4f102bb8140cc844363d61e95ea5fc4f8fb

IP addresses:

192.3.239.42

192.227.129.26

192.227.168.194

107.175.218.40

104.168.32.21

104.168.32.14

103.207.39.127