

[0X53414D58] THE MEET CHALLENGE - WALKTHROUGH

+ .
o

Miguel Santareno

<https://twitter.com/MiguelSantareno>

<https://www.linkedin.com/in/miguelsantareno/>

CHALLENGE

[0x53414D58] The Meet Challenge

##Information in Analysis

/9j/4AAQSkJRgABAQAAZABkAAD/2wBDAIABAQIBAQICAgICAgICAwUDAwMDAwYEBAMFBwYHBwcGBwcICQsJCAgKCACHCg0KCgsMDAwMBwkODw0MDgsMDAz/2wBDAQICAgMDAwYDA

##Investigation Guide

- 1: In which place is the mural located?
- 2: In which country and city can the mural be found?
- 3: What are the GPS coordinates of the location?
- 4: What is the email address of the entity?
- 5: How many times has the entity email been breached?
- 6: Where was the latest leak of the entity?
- 7: What is the official website of the entity?
- 8: What is the IP address of the website?
- 9: How many open ports does the website have?
- 10: What is the webserver used?
- 11: What is the name of the SSID of the entity?

Note: Collect all information passively; refrain from scanning or attacking the selected identity in any form or context.

<https://pathonproject.com/zb/?5cdf38bc05484c12#q75tGXW1SZsY8DolSe0ka3Zxd7dwpKs8UlaiLtMawm4>

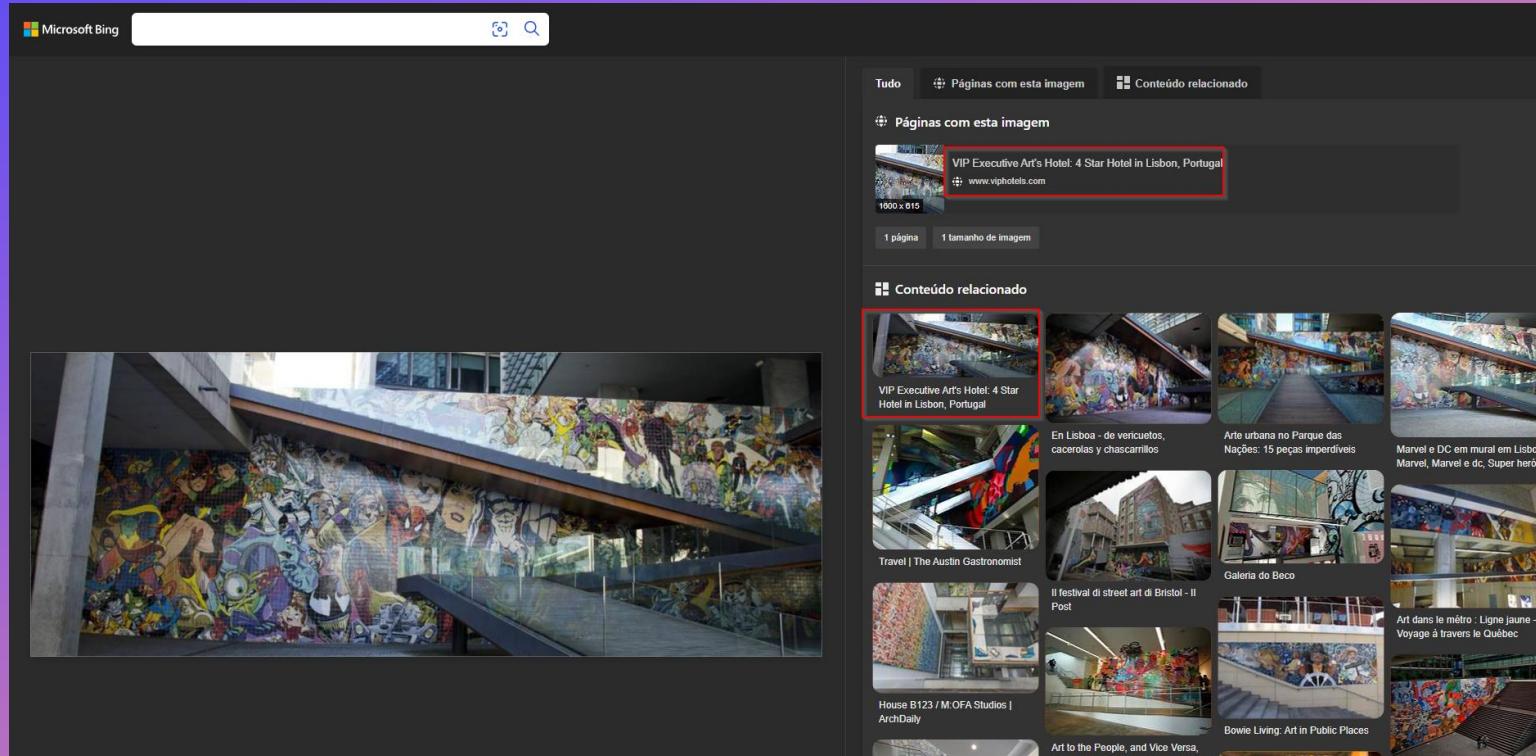
BASE64 JFIF DETECTION

<https://www.base64decode.org/>

BASE64 TO IMAGE

<https://base64.guru/converter/decode/image>

REVERSE IMAGE SEARCH



https://www.bing.com/images/search?view=detailV2&insightstoken=bcid_qEyDeTdZ71OG-A*ccid_TIN5N1nv&form=SBIHMP&iss=SBIUPLOADGET&sbisrc=ImgPicker&idpbck=1&sbifsz=1600+x+615+%C2%B7+73.82+kB+%C2%B7+jpeg&sbifnm=transferir.jpg

WEBSITE INFORMATION

The screenshot shows a web browser displaying the official website of VIP Executive Art's Hotel. The main content area features sections for Services & Accommodation, including Meeting Rooms, Standard Rooms, Junior Suites, and an Address section with GPS coordinates. A NetworkMiner tool window is overlaid on the browser, providing technical details such as IP address, hostname, and open ports (80 and 443). The IP address listed is 176.61.148.19, and the hostname is quintadofurao.com.

Services & Accommodation

MEETING ROOMS
VIP Executive Art's Hotel has 8 meeting rooms with different features to hold a meeting... [KNOW MORE »](#)

JUNIOR SUITES
All Junior Suites have capacity for 2 adults and 2 children maximum...

STANDARD ROOMS
All rooms have capacity for 2 adults and 1 child or baby... [BOOK NOW »](#)

ADDRESS
Avenida D. João II, nº 47, 1998-028 Lisboa - Portugal
Phone: +351 210 020 400 (National landline call)
Email: hotelarts@viphotels.com
RNET: 434

GDS CODES
Great Hotels Chain Code: GW
Amadeus: LISALN | Sabre: 405555
Worldspan: 43732 | Galileo: 33463
DHISCO: 6200070 | VFM: 3213

GPS COORDINATES
38° 46' 23.31"N | 9° 5' 52.53"W

Open Ports
80 443

www.viphotels.com
IP Address 176.61.148.19
Hostname(s) quintadofurao.com

<https://www.viphotels.com/en/Menu/Hotels/Portugal/Vip-Executive-Arts/About-Hotel.aspx>

WEBSITE INFORMATION - SHODAN

The screenshot shows Shodan search results for the IP address 176.61.148.19. The results are displayed in three main sections:

- General Information:** This section provides basic details about the host:
 - Hostnames: www.aquanaturamadeira.com
 - Domains: AQUANATURAMADEIRA.COM
 - Country: Portugal
 - City: Gião
 - Organization: Dominios.pt Dedicated Servers
 - ISP: DMNS - DOMINIOS, S.A.
 - ASN: AS33876
 - Operating System: Windows
- Open Ports:** This section lists the open ports:
 - 80 / TCP (highlighted)
 - 443 / TCP
- HTTP Response (Port 80):**

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 13 Nov 2019 10:10:20 GMT
Accept-Ranges: bytes
ETag: "add9dcbea9ad51:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 18 Nov 2023 07:27:07 GMT
Content-Length: 703
```
- HTTP Response (Port 443):**

```
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: http://www.aquanaturahotels.com/
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Fri, 17 Nov 2023 10:20:46 GMT
Content-Length: 155
```

<https://www.shodan.io/host/176.61.148.19>

BREACHED INFO

The screenshot shows the Have I Been Pwned? (HIBP) website interface. At the top, there is a search bar containing the email address "hotelarts@viphotels.com" and a button labeled "pwned?". Below the search bar, a large message says "Oh no — pwned!" followed by the text "Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)".

Below this, there is a section titled "3 Steps to better security" with three numbered steps:

- Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.
- Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.
- Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

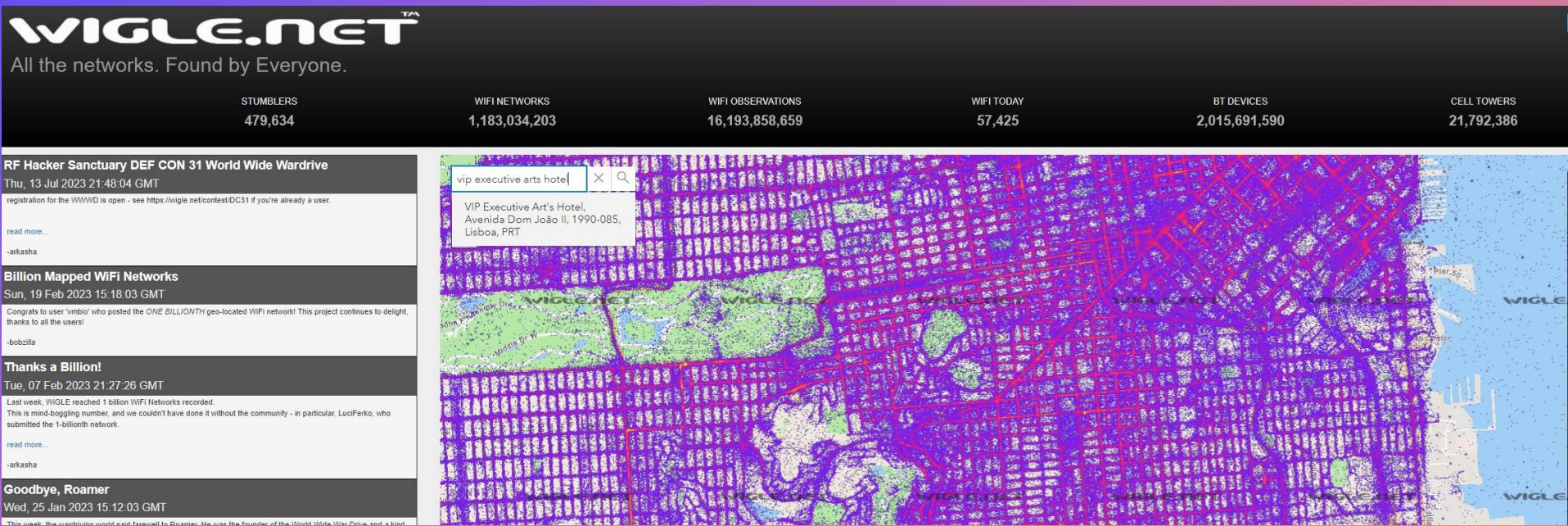
There are also links for "Start using 1Password.com", "Why 1Password?", and social media links for Facebook, Twitter, and Bitcoin.

Under the "Breaches you were pwned in" section, there are three entries:

- Onliner Spambot** (spam list): In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Berkay mosqu3q. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.
Compromised data: Email addresses, Passwords
- Trik Spam Botnet** (spam list): In June 2018, the command and control server of a malicious botnet known as the "Trik Spam Botnet" was misconfigured such that it exposed the email addresses of more than 43 million people. The researchers who discovered the exposed Russian server believe the list of addresses was used to distribute various malware strains via malspam campaigns (emails designed to deliver malware).
Compromised data: Email addresses
- Verifications.io**: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.
Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

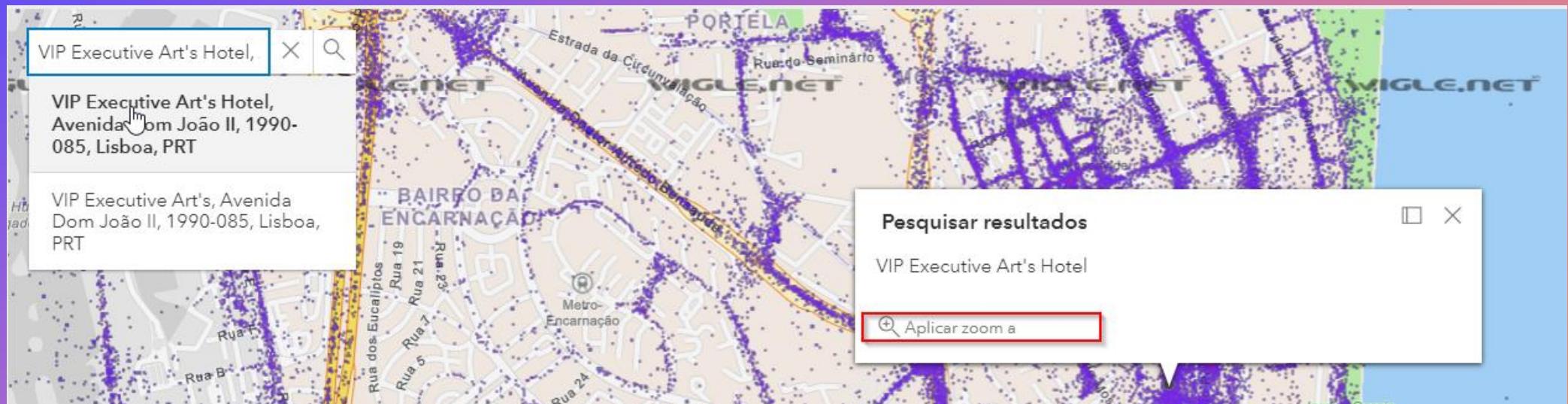
<https://haveibeenpwned.com>

WIFI - WIGLE



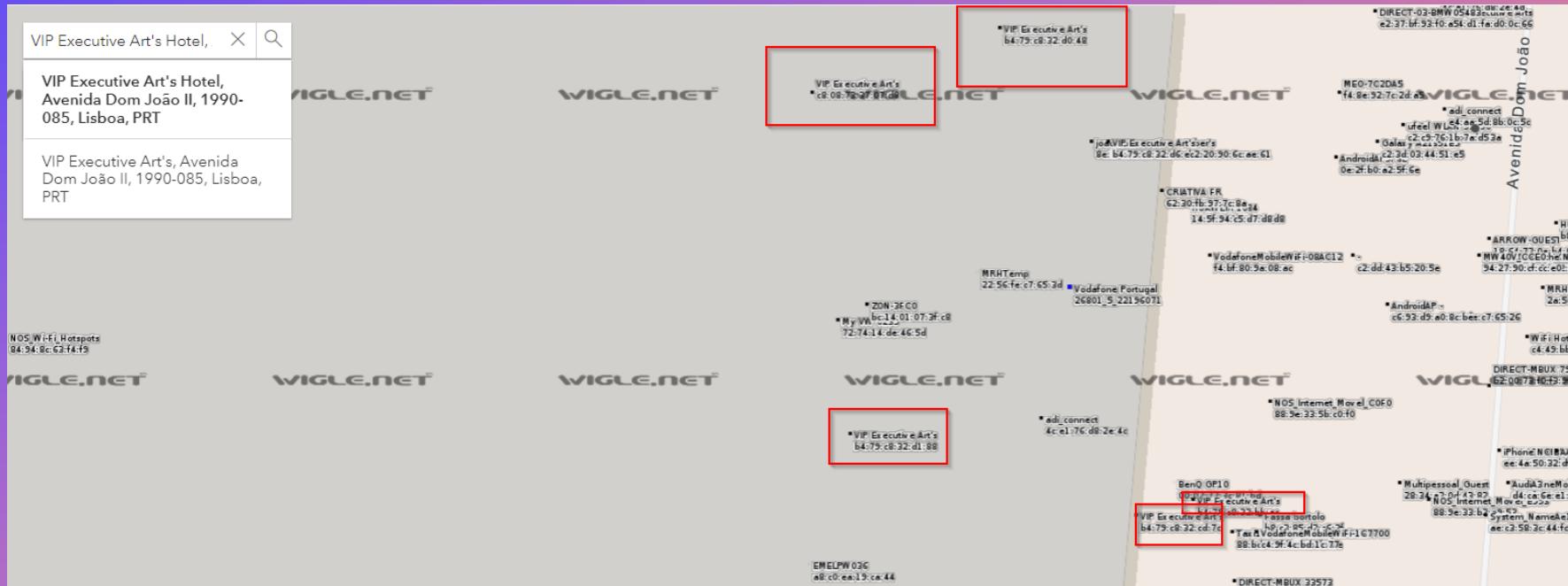
<https://wigle.net/>

WIFI - WIGLE



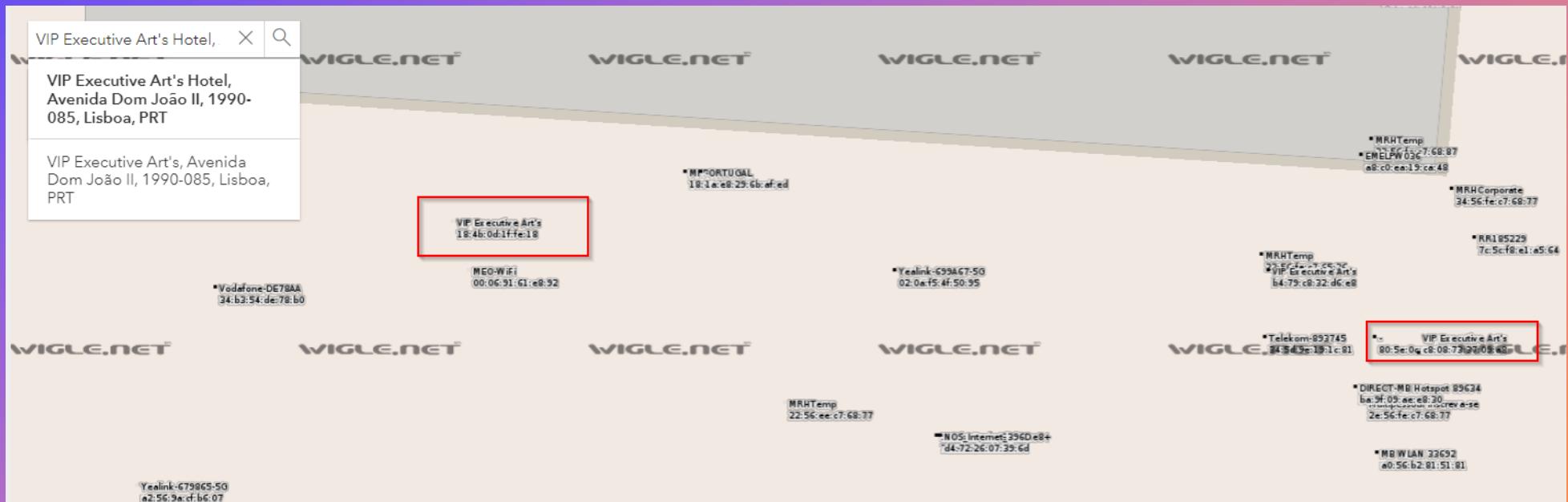
<https://wigle.net/>

WIFI - WIGLE



<https://wigle.net/>

WIFI - WIGLE



<https://wigle.net/>

EXTENDED CHALLENGE

- Extended Version
- + 12: Discover another active website of the entity.
 - + 13: Identify an alternative email for the entity.
 - + 14: Determine the number of times the email has been breached.
 - 15: Retrieve a link with the data leak from 2016 LinkedIn associated with the identified email.
 - 16: Find four social media accounts owned by the entity.
 - 17: Utilize Google dorks and existing information to uncover a previously owned domain of the entity.
 - 18: Retrieve a website snapshot from May 25, 2015.
 - 19: Identify the official booking partner of the entity.

<https://pathonproject.com/zb/?d70ec5a3e4a0fc55#T+ZYCVb83Tzy/v/NWqwNNUbyjINIxFadI5H+mTaLRWM4=>

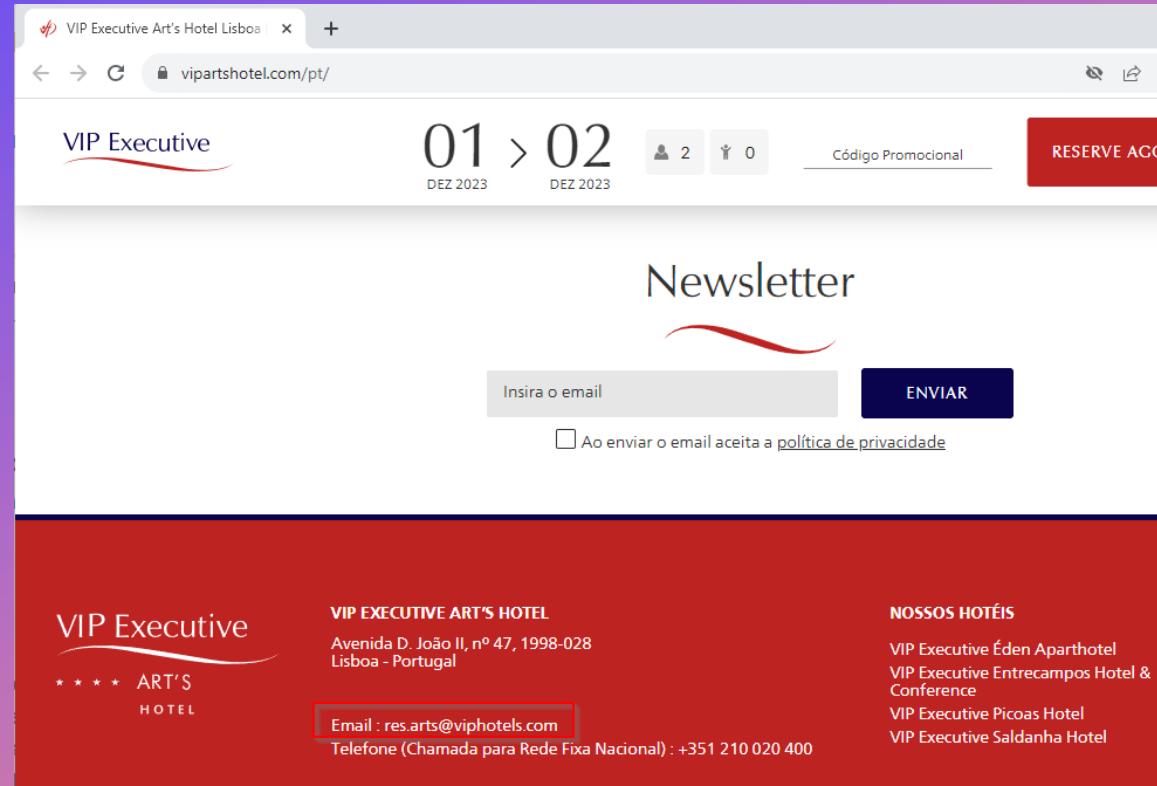
OTHER WEBSITE

A screenshot of a Google search results page. The search bar at the top contains the query "vip executive arts hotel". Below the search bar, there are three items listed:

- **vipartshotel.com**
https://www.vipartshotel.com › ... 
- **VIP Executive Art's Hotel Lisboa | Site Oficial**
O **VIP Executive Art's Hotel** é um hotel 4 de estrelas em Lisboa. Consulte as nossas promoções e reserve ao melhor preço garantido. [Web Oficial]. 

<https://www.google.com/search?q=vip+executive+arts+hotel>

OTHER EMAIL



<https://www.vipartshotel.com/pt/>

BREACHED INFO



<https://haveibeenpwned.com>

FINDING LEAKS

A screenshot of a Google search results page. The search bar at the top contains the query "linkedin data leak 2016 download". Below the search bar are several filter buttons: "Notícias", "Vídeos", "Imagens", "Livros", "Maps", "Voos", and "Finanças". A summary below the filters states "Cerca de 15 300 000 resultados (0,36 segundos)". The first result is from GitHub, showing a link to "Files/LinkedIn database leaked May 2016 at main". The snippet of the page content describes a data leak from May 2016 where LinkedIn had 164 million email addresses and passwords exposed.

linkedin data leak 2016 download

Notícias Vídeos Imagens Livros Maps Voos Finanças

Cerca de 15 300 000 resultados (0,36 segundos)

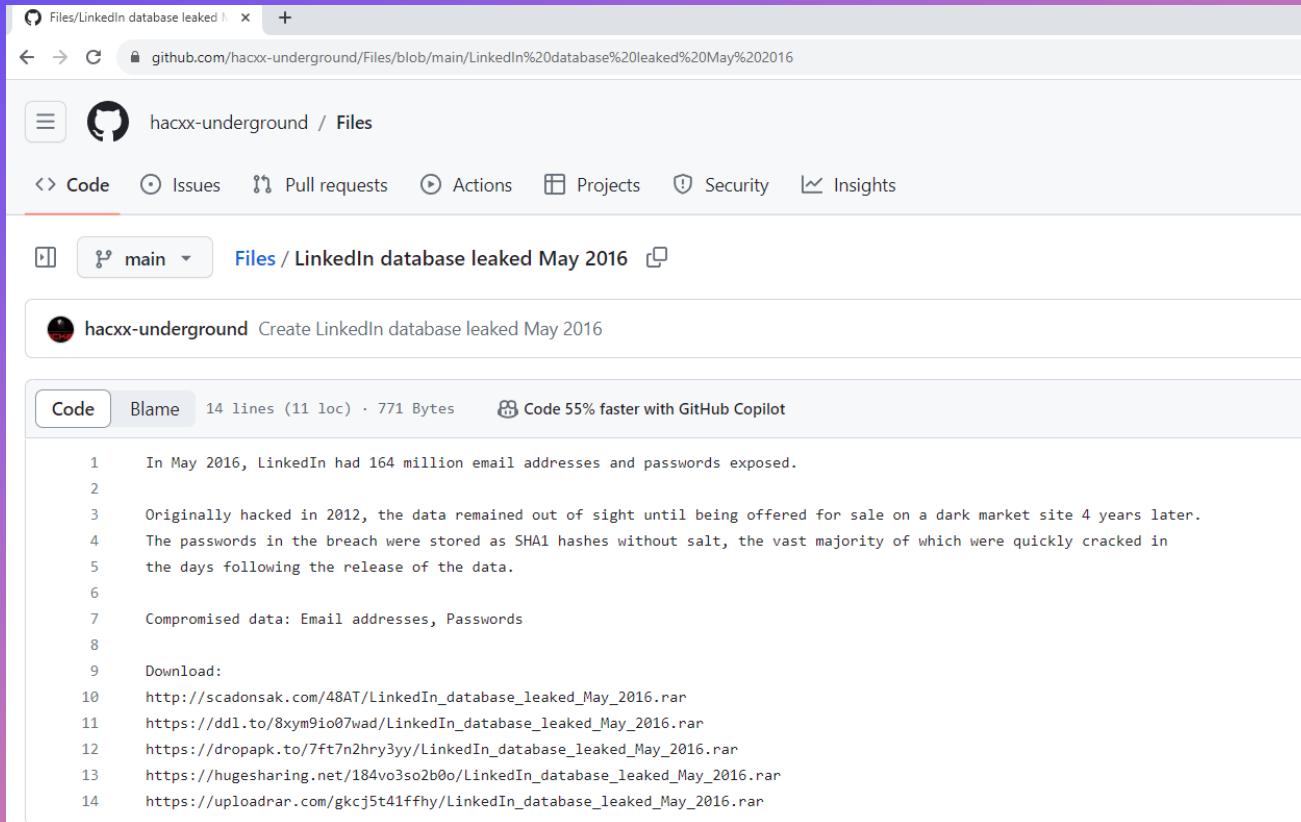
 GitHub
<https://github.com/files/blob> ::

Files/LinkedIn database leaked May 2016 at main

In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered ...

<https://www.google.com/search?q=linkedin+data+leak+2016+download>

FINDING LEAKS



<https://github.com/hacxx-underground/Files/blob/main/LinkedIn%20database%20leaked%20May%202016>

SOCIAL MEDIA

The screenshot shows the homepage of the VIP Executive Arts Hotel website. At the top, there's a red header bar with the hotel's name and a four-star rating. Below the header, there are two main promotional sections:

- OFERTAS**: Shows a deal for "PEQUENO ALMOÇO INCLUÍDO - NÃO REEMBOLSÁVEL" starting at €99,54.
- PROMOÇÃO VIAJANTES**: Shows a deal for "PROMOÇÃO VIAJANTES" starting at €101,28.

Below these sections, there are footer links for "GRUPO VIP", "SUBSCREVA A NOSSA NEWSLETTER", "SAIBA MAIS", and "SIGA-NOS". The "SIGA-NOS" section features a Facebook and YouTube icon, with a callout box highlighting the Facebook icon. To the right, there's a thumbnail of a Facebook post from the "VIP HOTELS" page.

<https://www.viphotels.com/pt/Menu/Hoteis/Portugal/Vip-Executive-Arts/Sobre-Hotel.aspx>

SOCIAL MEDIA

The screenshot shows a web browser window for 'VIP Executive Art's Hotel Lisboa' at vipartshotel.com.pt/. The page features a large white 'Newsletter' input field with a red wavy underline, a 'RESERVE AGORA' button in red, and a 'Código Promocional' input field. Below the input fields, there is a checkbox for accepting the privacy policy and a link to it. At the bottom, there is a footer with hotel information, social media links, and a contact section.

VIP Executive

01 > 02
DEZ 2023 DEZ 2023

RESERVE AGORA

Código Promocional

Newsletter

Insira o email

ENVIAR

Ao enviar o email aceita a [política de privacidade](#)

VIP Executive

ART'S HOTEL

VIP EXECUTIVE ART'S HOTEL
Avenida D. João II, nº 47, 1998-028
Lisboa - Portugal

Email : res arts@viphotels.com
Telefone (Chamada para Rede Fixa Nacional) : +351 210 020 400

NOSSOS HOTÉIS

VIP Executive Éden Aparthotel
VIP Executive Entrecampos Hotel & Conference
VIP Executive Picoas Hotel
VIP Executive Saldanha Hotel

VIP Executive Santa Iria Hotel
VIP Executive Zurique Hotel
VIP Grand Lisboa Hotel & Spa
VIP Inn Berna
VIP Executive Azores Hotel

CONTATO | POLÍTICA DE COOKIES | RESOLUÇÃO DE CONFLITO ALTERNATIVO | POLÍTICA DE PRIVACIDADE | MAPA DO SÍTIO | FAQ'S | LIVRO DE RECLAMAÇÕES | RNEE 434

[f](#) [i](#) [in](#)

<https://www.vipartshotel.com.pt/>

SOCIAL MEDIA

The screenshot shows the Instagram profile of 'viphotels'. The profile picture is a circular logo for 'VIP HOTELS' featuring a stylized 'VH' monogram. The bio reads: 'Estância hoteleira VIP Hotels has currently 15 properties, 11 in Portugal and 4 in Mozambique. Tag our page to share your photos. www.viphotels.com'. Below the bio are seven circular icons representing different services: MENUS, BREAKFAST, POOLS, COCKTAILS, RESTAURANTS, EVENTS, and FEEDBACK.

VIP Hotels (@viphotels) • fotos e vídeos

Instagram

Iniciar sessão Regista-te

viphotels Seguir Enviar mensagem ...

404 publicações 1446 seguidores A seguir 355

VIP Hotels

Estância hoteleira

• VIP Hotels has currently 15 properties, 11 in Portugal and 4 in Mozambique

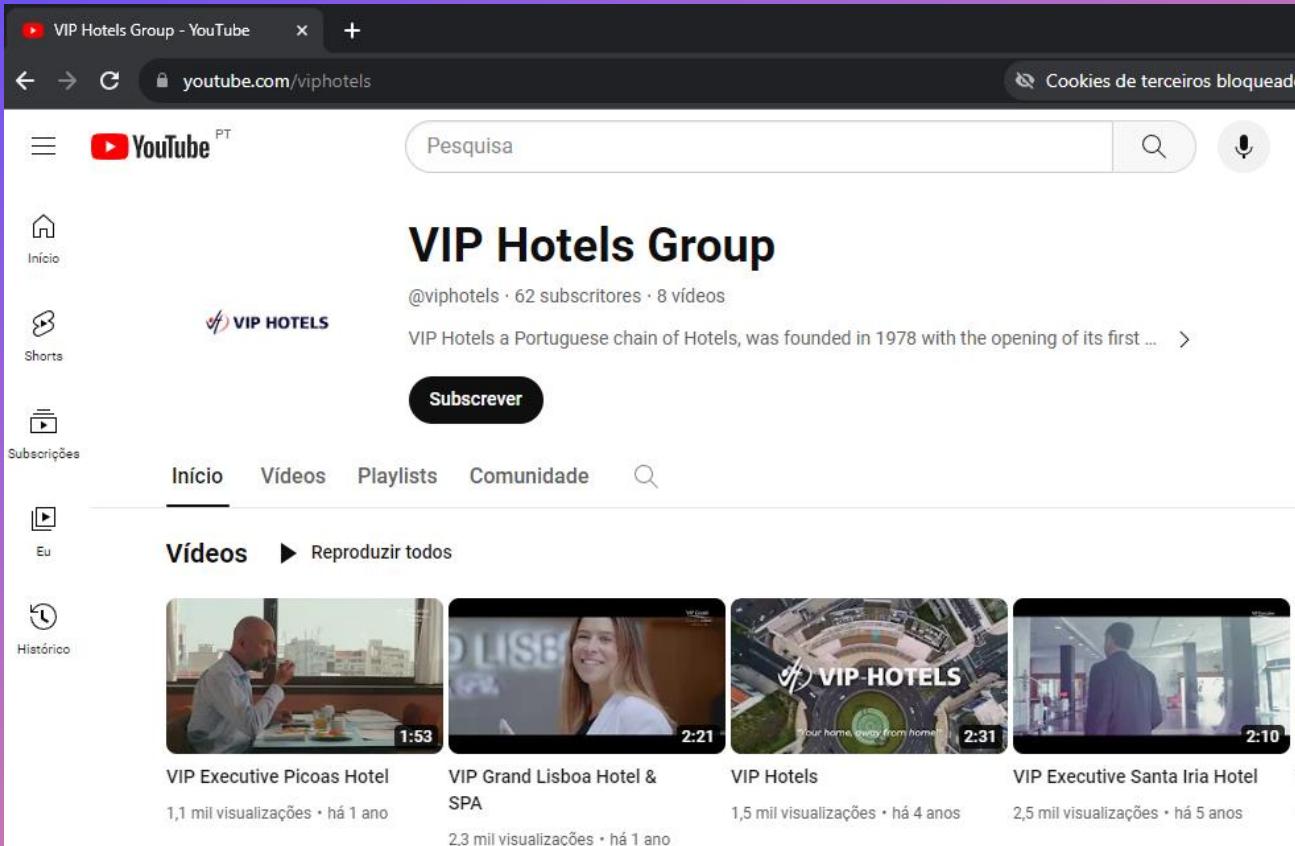
• Tag our page to share your photos

• www.viphotels.com

MENUS BREAKFAST POOLS COCKTAILS RESTAURANTS EVENTS FEEDBACK

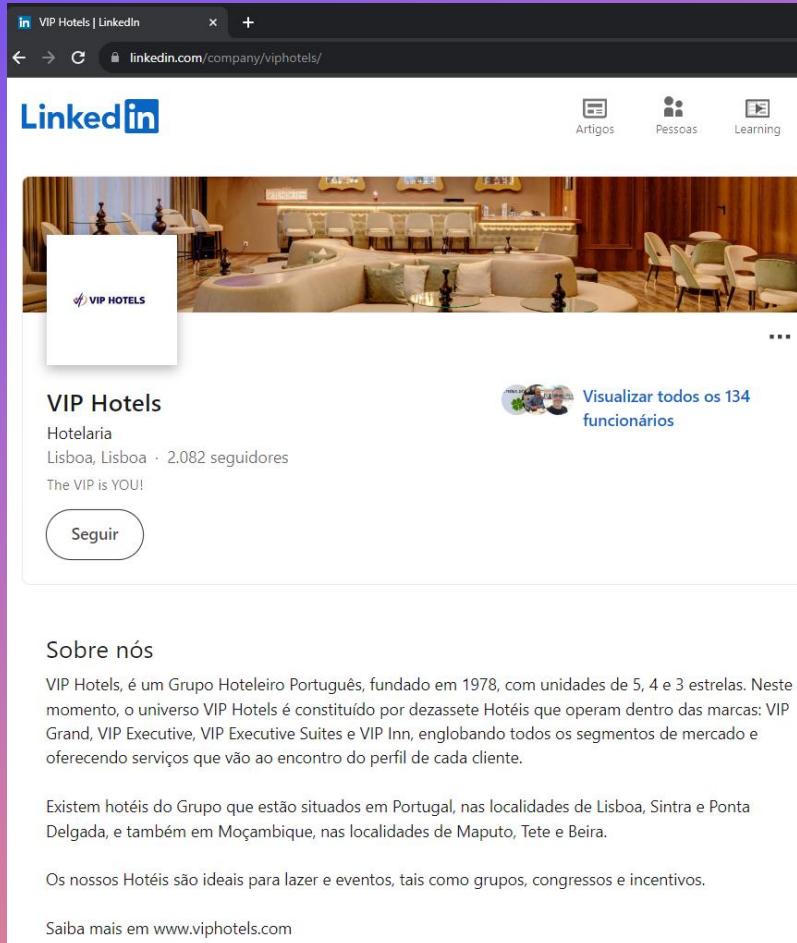
<https://www.instagram.com/viphotels/>

SOCIAL MEDIA



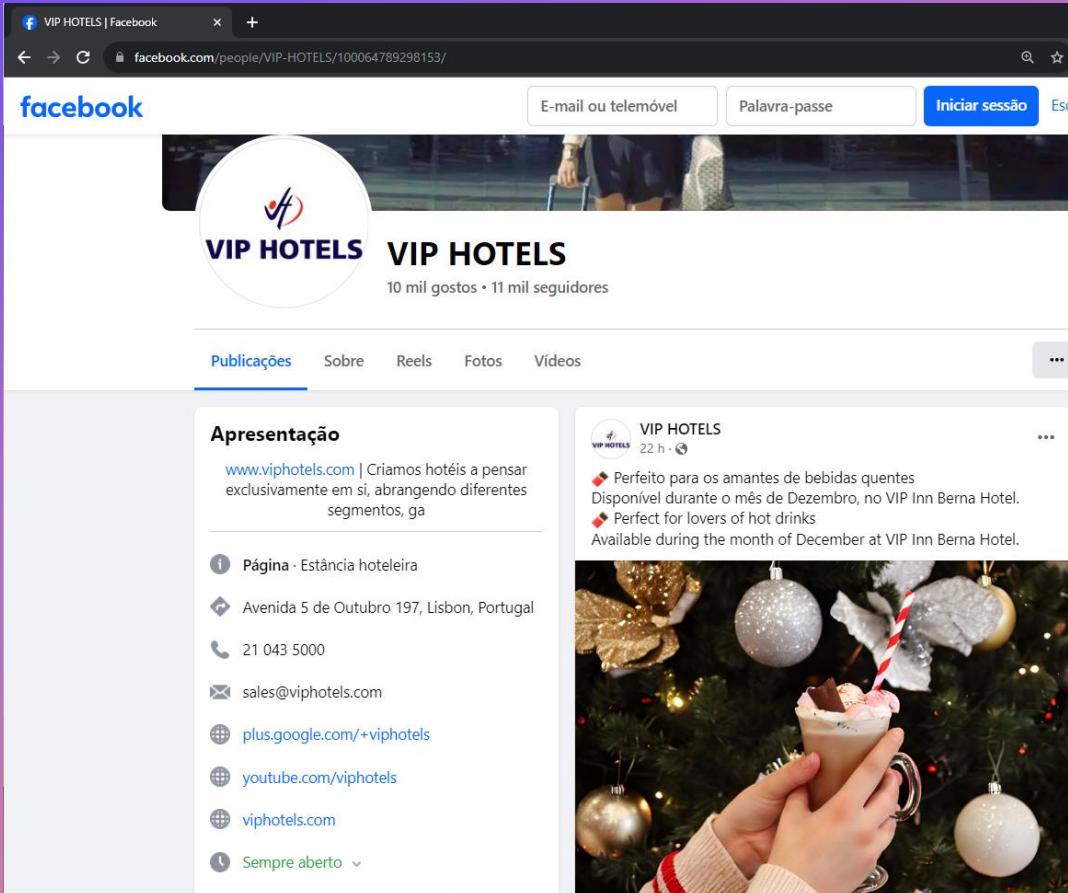
<https://www.youtube.com/viphotels>

SOCIAL MEDIA



<https://www.linkedin.com/company/viphotels/>

SOCIAL MEDIA



<https://www.facebook.com/people/VIP-HOTELS/100064789298153/>

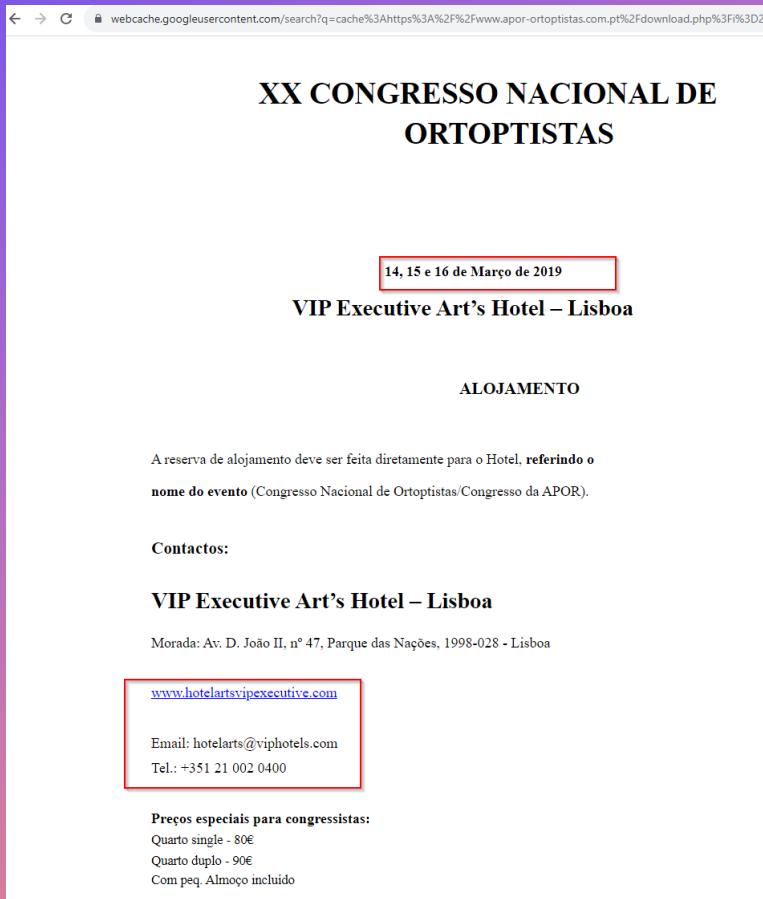
GOOGLE DORKING

A screenshot of a Google search results page. The search query in the bar is "hotelarts@viphotels.com ext:pdf". The results are as follows:

- Associação Portuguesa de Ortoptistas**
https://www.apor-ortoptistas.com.pt › download ...
XX CONGRESSO NACIONAL DE ORTOPTISTAS
16/03/2019 — Email: hotelarts@viphotels.com. Tel.: +351 21 002 0400. Preços especiais para congressistas: Quarto single - 80€. Quarto duplo - 90€. Com peq ...
- International Civil Aviation Organization**
https://www.icao.int › Meetings › Lisbon-2016 ...
Appendix F
Hotel Arts Hotel: <http://www.viphotels.com/pt/Hoteis/VIP-Executive-Arts/Sobre-Hotel.aspx>.
Page 2. 7. Local Transportation. The Hotel Tivoli Oriente is ...
2 páginas
- lisboatours.com.pt**
https://lisboatours.com.pt › uploads › 2023/02 ...
PLAY FESTIVAL - LISBOA TOURS
02/02/2023 — hotelarts@viphotels.com www.viphotels.com. VIP EXECUTIVE ÉDEN.
APARTHOTEL. Praça dos Restauradores, 24, Lisboa. T. (+351) 213 216 600 isabelbeja ...
- lisboatours.com.pt**
https://lisboatours.com.pt › uploads › 2023/06 ...
FIESTAS DE LISBOA
01/06/2023 — hotelarts@viphotels.com www.viphotels.com. VIP EXECUTIVE ÉDEN.
APARTHOTEL. Praça dos Restauradores, 24, Lisboa. T. (+351) 213 216 600 isabelbeja ...
- ULisboa**
https://fenix.tecnico.ulisboa.pt › downloadFile ...
hotel de negócios
<https://www.apor-ortoptistas.com.pt/download.php?i=217>

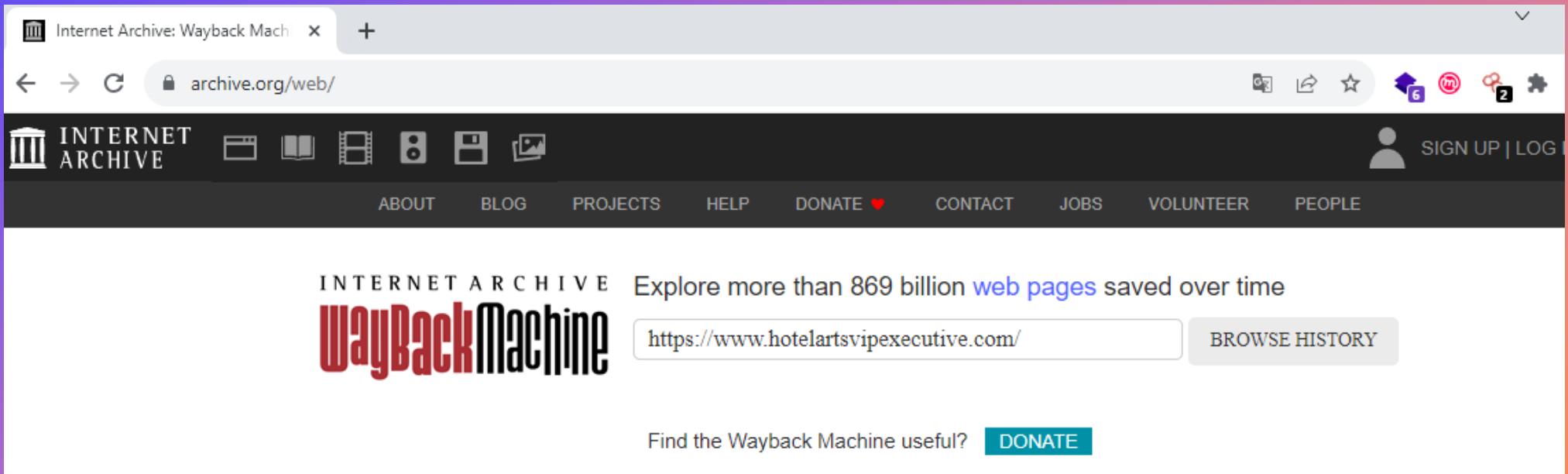
<https://www.google.com/search?q=hotelarts%40viphotels.com+ext%3Apdf>

GOOGLE DORKING



<https://webcache.googleusercontent.com/search?q=cache%3Ahttps%3A%2F%2Fwww.apor-ortoptistas.com.pt%2Fdownload.php%3Fi%3D217>

WAYBACK MACHINE

A screenshot of a web browser showing the Internet Archive: Wayback Machine homepage. The URL in the address bar is archive.org/web/. The page features a dark header with the Internet Archive logo, navigation links like ABOUT, BLOG, PROJECTS, HELP, DONATE, CONTACT, JOBS, VOLUNTEER, and PEOPLE, and a sign-up/login button. Below the header is a search bar containing the URL https://www.hotelartsvipexecutive.com/ and a 'BROWSE HISTORY' button. The main content area includes the text 'INTERNET ARCHIVE Explore more than 869 billion web pages saved over time' and the Wayback Machine logo. A 'DONATE' button is visible at the bottom.

Internet Archive: Wayback Machine

archive.org/web/

INTERNET ARCHIVE

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

SIGN UP | LOG IN

INTERNET ARCHIVE Explore more than 869 billion web pages saved over time

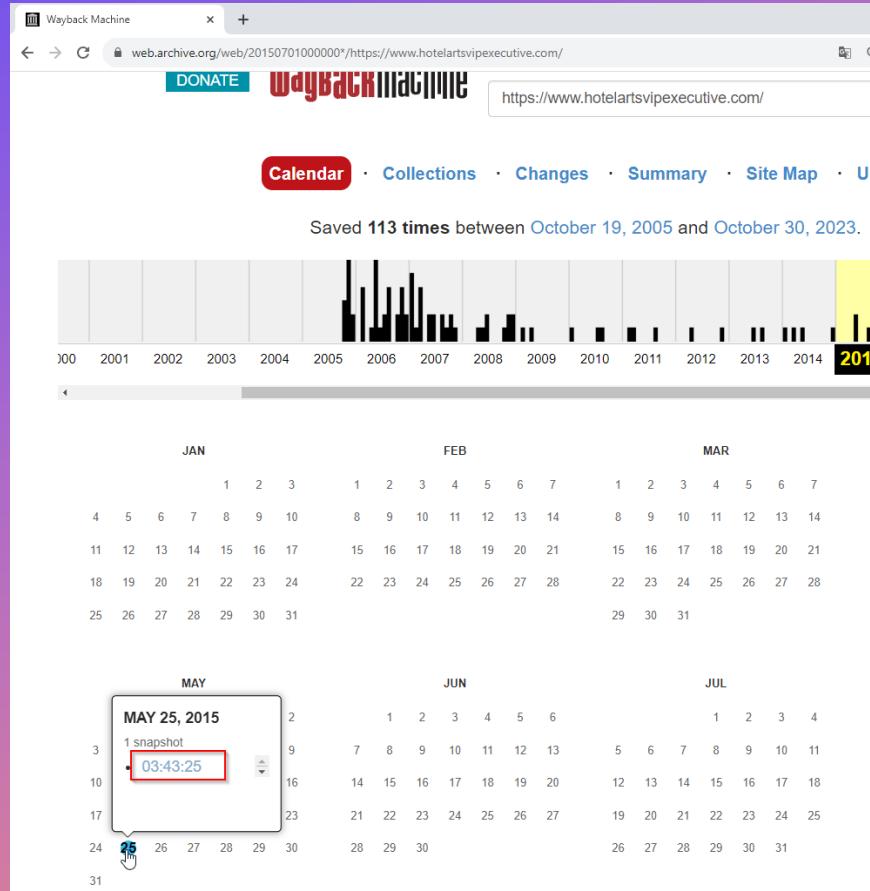
WayBack Machine

https://www.hotelartsvipexecutive.com/ BROWSE HISTORY

Find the Wayback Machine useful? [DONATE](#)

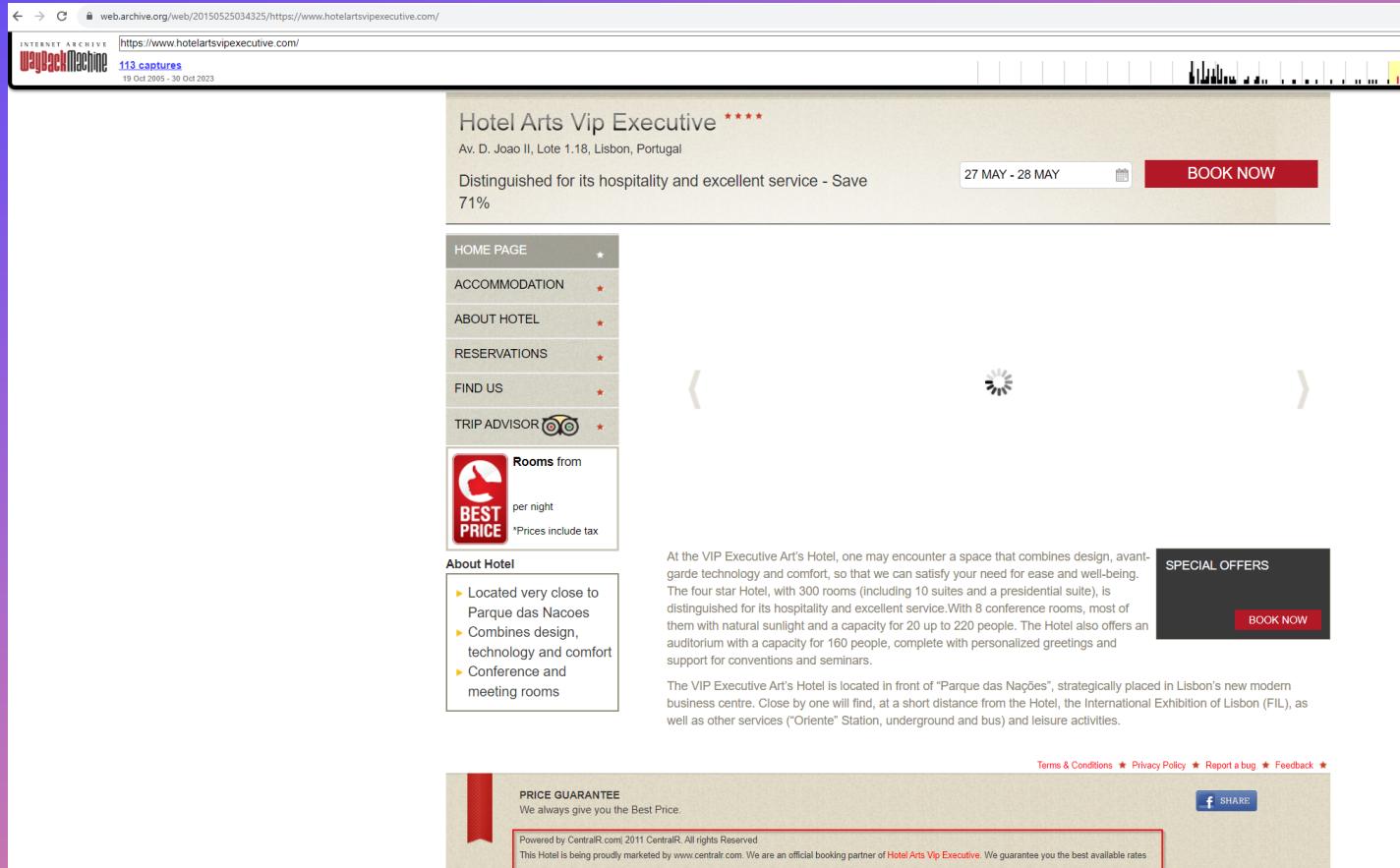
<https://archive.org/web/>

WAYBACK MACHINE



https://web.archive.org/web/20150701000000*/https://www.hotelartsvipexecutive.com/

WAYBACK MACHINE



<https://web.archive.org/web/20150525034325/https://www.hotelartsvipexecutive.com/>



+

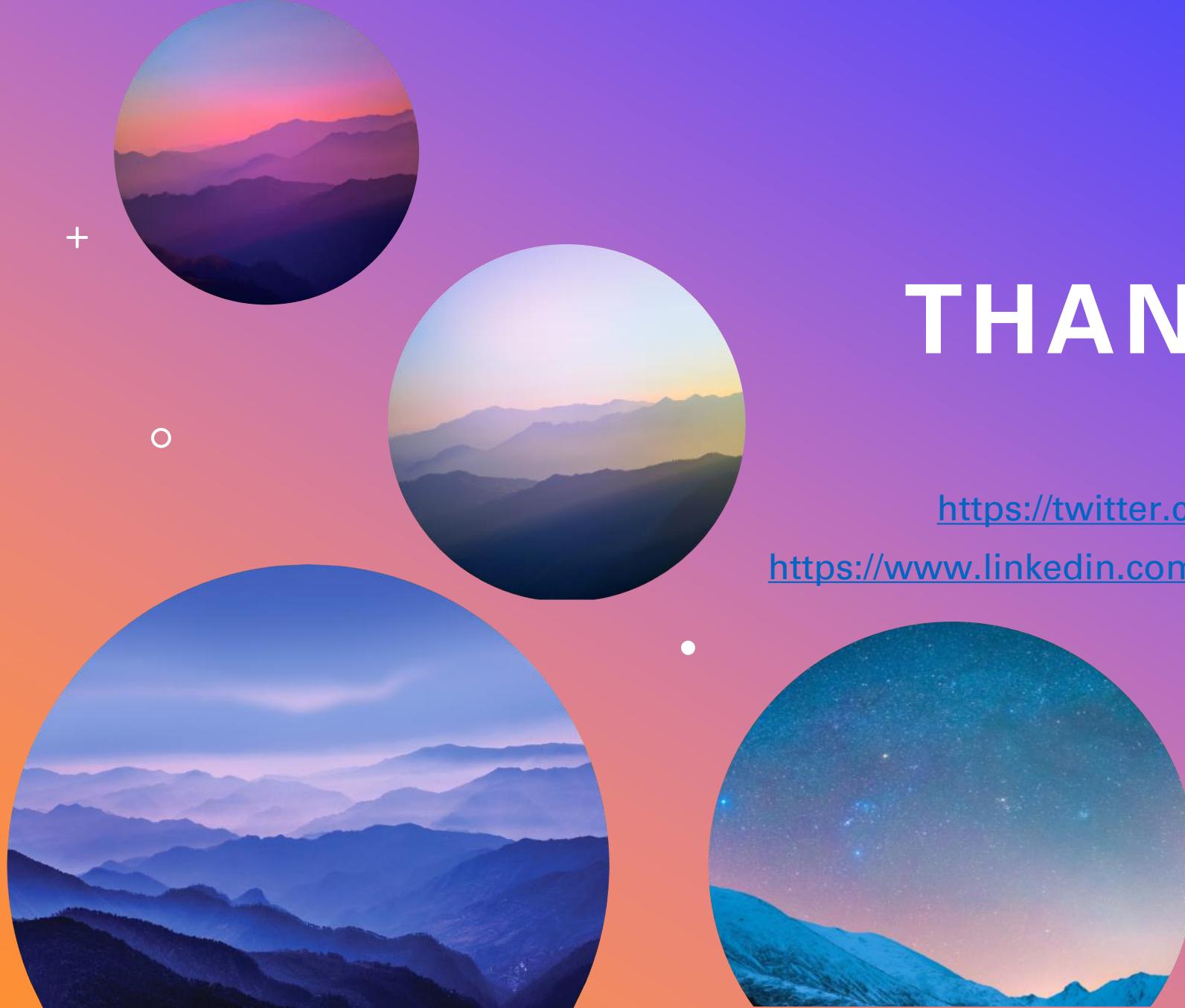
●

○

+

○

●



THANK YOU

Miguel Santareno

<https://twitter.com/MiguelSantareno>

<https://www.linkedin.com/in/miguelsantareno/>