



Instituto Federal do Maranhão  
Grajaú-MA, 20 de Junho de 2022

Prof.: Rodrigo

Integrantes: Paulo André, Danielle Reis, Izau Paulino e Wanderson Galvão

As informações coletadas serão divididas em três etapas:

- 1 - Negócio
- 2 - Infraestrutura

Em informações de negócio devem ser levantadas as seguintes informações:

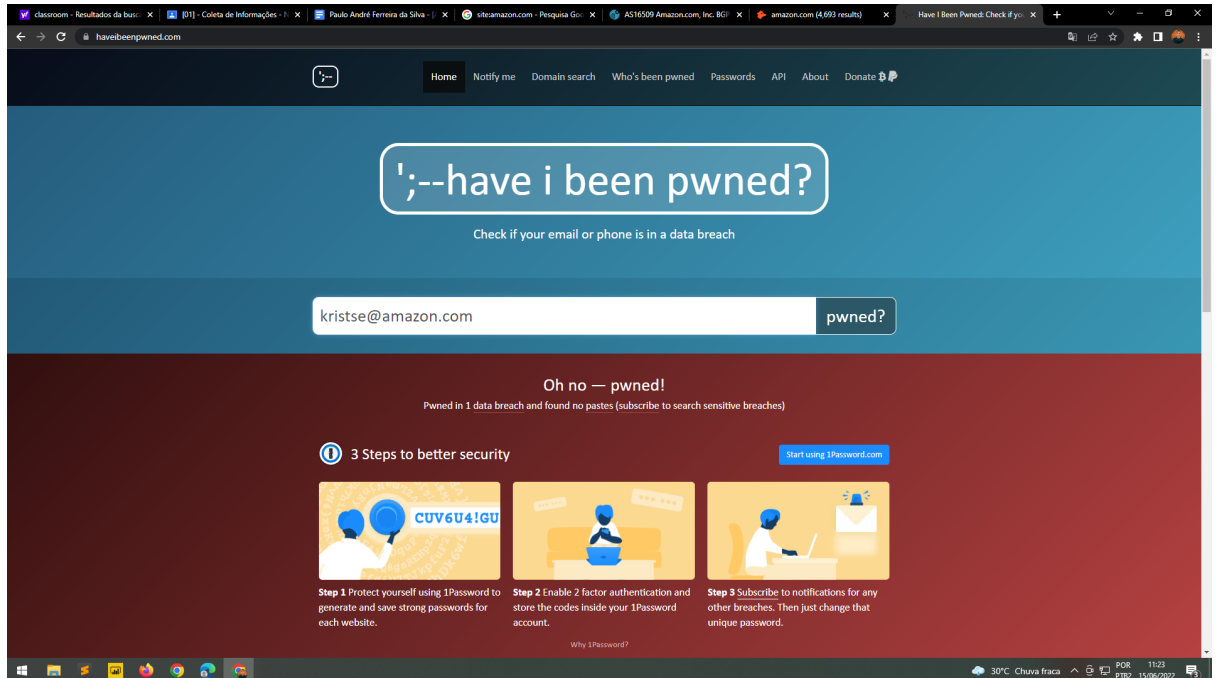
- Lista de E-mails de funcionários.

Verificamos no Website Amazon.com que as seguintes informações levantadas a respeito dos emails abaixo solicitados que dos 10 e-mails pesquisados, 6 emails não haviam vazamentos de dados, portanto os serviços de segurança foram efetivos. Com isso apenas alguns foram menos privilegiados (4 e-mails) contendo acesso de espionagem, ou seja dados foram em partes ou não, ou totalmente vazados :

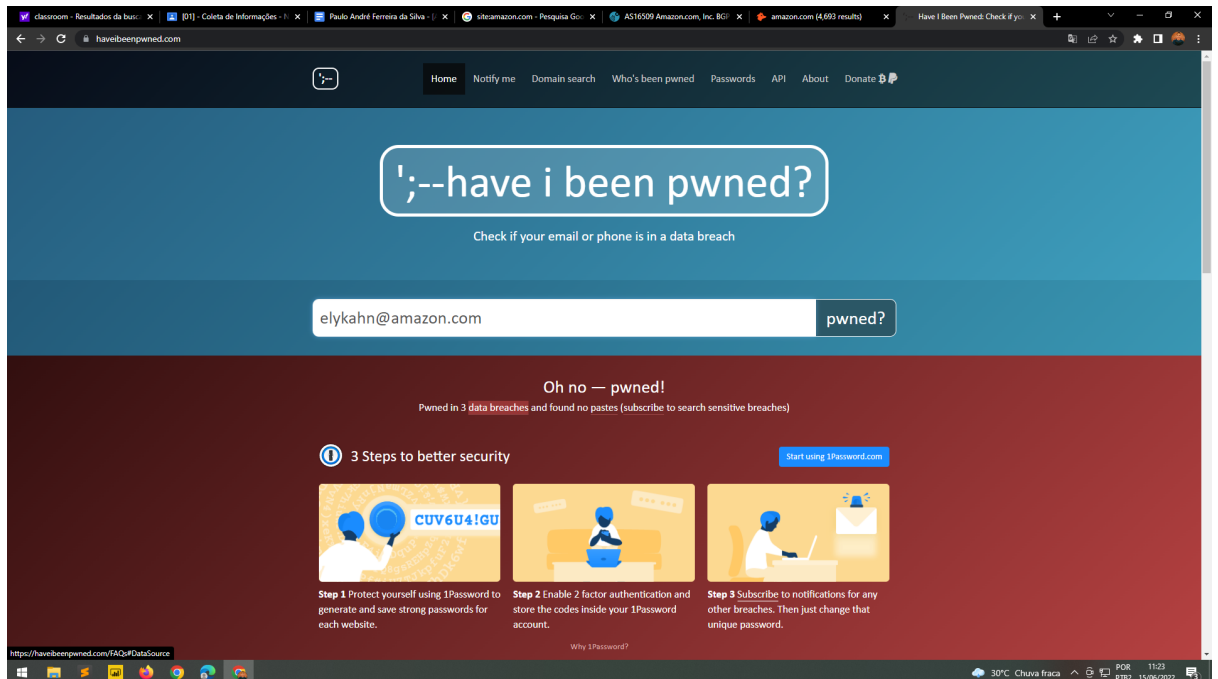
[shashack@amazon.com](mailto:shashack@amazon.com)  
[phildoak@amazon.com](mailto:phildoak@amazon.com)  
[kristse@amazon.com](mailto:kristse@amazon.com)  
[yilmazp@amazon.com](mailto:yilmazp@amazon.com)  
[elykahn@amazon.com](mailto:elykahn@amazon.com)  
[harrigan@amazon.com](mailto:harrigan@amazon.com)  
[karango@amazon.com](mailto:karango@amazon.com)  
[troykirk@amazon.com](mailto:troykirk@amazon.com)  
[ahlgrenp@amazon.com](mailto:ahlgrenp@amazon.com)  
[owulff@amazon.com](mailto:owulff@amazon.com)

- Verificar quais e-mails listados sofreram vazamento de dados

[kristse@amazon.com](mailto:kristse@amazon.com)



[elykahn@amazon.com](mailto:elykahn@amazon.com)



[karango@amazon.com](mailto:karango@amazon.com)

classroom - Resultados da busca x [01] - Coleta de Informações - x Paulo André Ferreira da Silva - x siteamazon.com - Pesquisa Google x AS16509 Amazon.com, Inc. BG x amazon.com (4.693 results) x Have I Been Pwned: Check if you've been pwned x

haveibeenpwned.com

Home Notify me Domain search Who's been pwned Passwords API About Donate

# ';--have i been pwned?

Check if your email or phone is in a data breach

karango@amazon.com **pwned?**

**Oh no — pwned!**  
Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)

**3 Steps to better security** [Start using 1Password.com](#)

**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.

Why 1Password?

30°C Chuva fraca 11:22 15/06/2022

[troykirk@amazon.com](mailto:troykirk@amazon.com)

classroom - Resultados da busca x [01] - Coleta de Informações - x Paulo André Ferreira da Silva - x siteamazon.com - Pesquisa Google x AS16509 Amazon.com, Inc. BG x amazon.com (4.693 results) x Have I Been Pwned: Check if you've been pwned x

haveibeenpwned.com

Home Notify me Domain search Who's been pwned Passwords API About Donate

# ';--have i been pwned?

Check if your email or phone is in a data breach

troykirk@amazon.com **pwned?**

**Oh no — pwned!**  
Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

**3 Steps to better security** [Start using 1Password.com](#)

**Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.

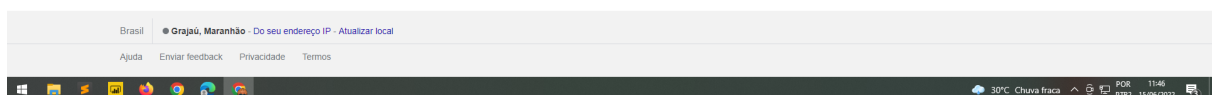
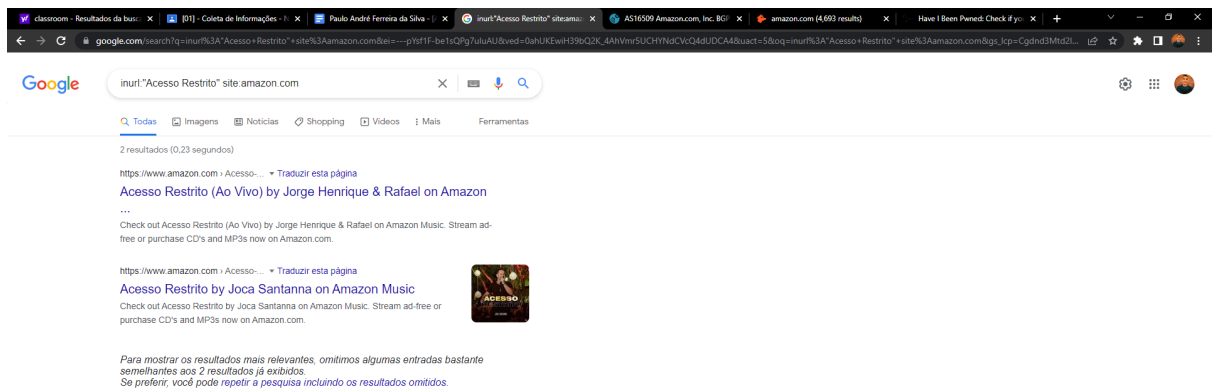
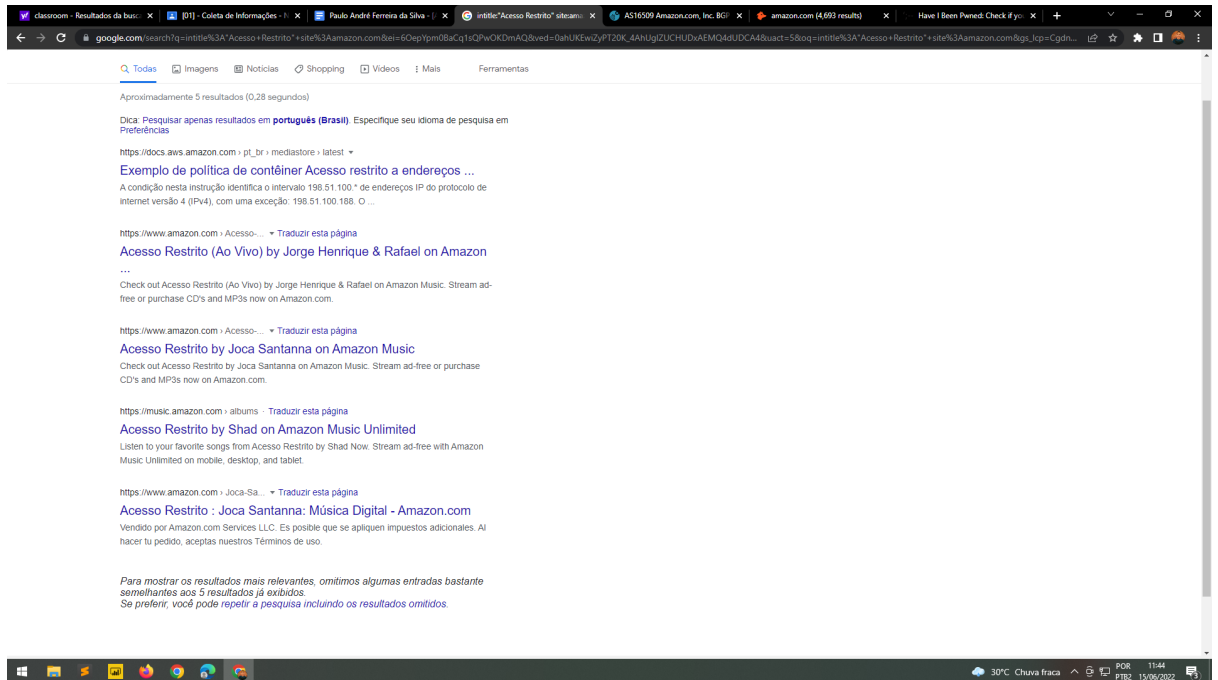
**Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.

**Step 3** Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

30°C Chuva fraca 11:24 15/06/2022

- Verificar se é retornado algumas informações no domínio via Google Hacking.



- Utilizar a ferramenta TheHarvester via Kali Linux para coleta de informações.

```
root@kali:~# whois amazon.com
connect: A rede está fora de alcance
root@kali:~# host amazon.com
amazon.com has address 176.32.103.205
amazon.com has address 205.251.242.103
amazon.com has address 54.239.28.85
amazon.com mail is handled by 5 amazon-smtp.amazon.com.
root@kali:~# theHarvester -d amazon.com
bash: theHarvester: comando não encontrado
root@kali:~# theHarvester -d amazon.com -l 100 -b google -f resultado.html
bash: theHarvester: comando não encontrado
root@kali:~# theharvester -d amazon.com -l 100 -b google -f resultado.html

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

*****
* theHarvester Ver. 3.0.6
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

found supported engines
[-] Starting harvesting process for domain: amazon.com

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...

Harvesting results
No IP addresses found

[+] Emails found:
-----
No emails found

[+] Hosts found in search engines:
-----

Total hosts: 3
```

```
Aplicativos Localiz Terminal qua 11:03
root@kali:~#

Arquivo Editar Ver Pesquisar Terminal Ajuda
amazon.com has address 54.239.28.85
amazon.com mail is handled by 5 amazon-smtp.amazon.com.
root@kali:~# theHarvester -d amazon.com
bash: theHarvester: comando não encontrado
root@kali:~# theHarvester -d amazon.com -l 100 -b google -f resultado.html
bash: theHarvester: comando não encontrado
root@kali:~# theharvester -d amazon.com -l 100 -b google -f resultado.html

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

*****
* theHarvester Ver. 3.0.6
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

found supported engines
[-] Starting harvesting process for domain: amazon.com

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...

Harvesting results
No IP addresses found

[+] Emails found:
-----
No emails found

[+] Hosts found in search engines:
-----

Total hosts: 3

[-] Resolving hostnames IPs...
login.amazon.com:52.94.235.93
music.amazon.com:54.239.28.85
www.amazon.com:13.227.109.239
NEW REPORTING BEGINS:
NEW REPORTING FINISHED!
[+] Saving files...
Files saved!
root@kali:~#
```

- Ano em que o domínio do site começou a ser utilizado; Qual ano, o domínio teve mais acesso; Qual mês costuma ter mais acessos no site, etc.

A Amazon utiliza o domínio [amazon.com](https://amazon.com) desde 12 de dezembro de 1998, este utiliza o modelo e-commerce e diante do cenário atual é uma das maiores no ramo tecnológico, sendo o maior site de vendas do mundo. O grande varejista obteve seu maior pico em acessos no ano de 2021 e possui uma maior crescente em alcance no dia 8 de março.

Em informações de infraestrutura devem ser levantadas as seguintes informações:

- Localização do servidor web.

Estados Unidos, servidor AS16509, por nome de Amazon.com, Inc. com endereço Ipv4: 42,487,552; number of peers: 10; Numbers of prefixes: 8,808.

- Encontrar subdomínios no site (Utilizando o script criado em sala de aula).

```
root@kali:~# gedit lista.txt
root@kali:~# ./subtakeover.sh amazon.com
root@kali:~# cat lista.txt
firewall
monitoramento
intranet
ns1
ns01
mail
webmail
rh
sistema
homologacao
admin
api
logs
devs
documentos
server
rastreamento
vendas
produtos
clientes
```

Sobre os domínios pesquisado, não obtivemos os resultados esperados, sobre os domínios do website [amazon.com](https://amazon.com).

- Verificar lista de endereço IP ou ASN dos servidores.

Browser window showing BGPview.io report for AS16509 Amazon.com, Inc. (AMAZON-02).

AS16509 Amazon.com, Inc. (AMAZON-02)

IPv4 Addresses: 42,490,624    Number of Peers: 104    Number of Prefixes: 8,826    ASN Allocated: 4<sup>th</sup> May 2000

**AS16509 Summary**

REGIONAL REGISTRY: ARIN  
ALLOCATION STATUS: Assigned  
ALLOCATION DATE: 4<sup>th</sup> May 2000  
ALLOCATED COUNTRY: US

TRAFFIC RATIO: Balanced  
INTERNET EXCHANGES: 257  
WEBSITE: <http://www.amazon.com>

**AS16509 Network**

IPv4 PREFIXES: 6,639    IPv6 PREFIXES: 2,187  
IPv4 PEERS: 62    IPv6 PEERS: 42  
IPv4 UPSTREAMS: 21    IPv6 UPSTREAMS: 18

**Contacts**

EMAIL CONTACTS: [aws-routing-poc@amazon.com](mailto:aws-routing-poc@amazon.com), [amazon-noc-contact@amazon.com](mailto:amazon-noc-contact@amazon.com), [abuse@amazonaws.com](mailto:abuse@amazonaws.com), [aws-rpki-routing-poc@amazon.com](mailto:aws-rpki-routing-poc@amazon.com), [ipmanagement@amazon.com](mailto:ipmanagement@amazon.com)


ABUSE CONTACTS: [abuse@amazonaws.com](mailto:abuse@amazonaws.com)

ADDRESS: 1918 8th Ave, SEATTLE, WA, 98101-1244, US


POWERED BY SecurityTrails

205.251.242.103

Announcing ASNs

Country	ASN	Name	Description
	AS16509	AMAZON-02	Amazon.com, Inc.

**205.251.240.0/22 Summary**

PREFIX: 205.251.240.0/22  
NAME: AMAZON-05  
DESCRIPTION: Amazon.com, Inc.  
COUNTRY:   
IP ADDRESSES: 1,024

REGIONAL REGISTRY: ARIN  
ALLOCATION STATUS: Allocated  
ALLOCATION DATE: 27<sup>th</sup> August 2010  
PARENT PREFIX: 205.251.192.0/18

**Contacts**

EMAIL CONTACTS: [abuse@amazonaws.com](mailto:abuse@amazonaws.com), [aws-routing-poc@amazon.com](mailto:aws-routing-poc@amazon.com), [aws-rpki-routing-poc@amazon.com](mailto:aws-rpki-routing-poc@amazon.com), [amzn-noc-contact@amazon.com](mailto:amzn-noc-contact@amazon.com), [ipmanagement@amazon.com](mailto:ipmanagement@amazon.com)

ABUSE CONTACTS: [abuse@amazonaws.com](mailto:abuse@amazonaws.com)

ADDRESS: 1918 8th Ave, SEATTLE, WA, 98101-1244, US

54.239.28.85

## Announcing ASNs

Country	ASN	Name	Description
	AS16509	AMAZON-02	Amazon.com, Inc.

## 54.239.16.0/20 Summary

PREFIX: 54.239.16.0/20

NAME: AMAZON-2011L

DESCRIPTION: Amazon Technologies Inc.

COUNTRY: 

IP ADDRESSES: 4,096

REGIONAL REGISTRY: ARIN

ALLOCATION STATUS: Allocated

ALLOCATION DATE: 1<sup>st</sup> March 2012

PARENT PREFIX: 54.224.0.0/11

## Contacts

### EMAIL CONTACTS:

aws-dogfish-routing-poc@amazon.com

amzn-noc-contact@amazon.com

aws-routing-poc@amazon.com

abuse@amazonaws.com

### ABUSE CONTACTS:

abuse@amazonaws.com

### ADDRESS:

410 Terry Ave N.,

Seattle,

WA,

98109,

US

176.32.103.205

## Announcing ASNs

Country	ASN	Name	Description
	AS16509	AMAZON-02	Amazon.com, Inc.

## 176.32.96.0/21 Summary

PREFIX: 176.32.96.0/21

NAME: Unkown

DESCRIPTION:

COUNTRY: 

IP ADDRESSES: 2,048

REGIONAL REGISTRY: RIPE

ALLOCATION STATUS: Allocated

ALLOCATION DATE: 23<sup>rd</sup> May 2011

PARENT PREFIX: 176.32.64.0/18

## Contacts

### EMAIL CONTACTS:

None

### ABUSE CONTACTS:

None

### ADDRESS:

Unknown