# Whoami – Quem sou eu ?

- Estudante da Fatec Bauru – Redes
- DevOps – EZ devs
- Estudante de segurança da informação

# Historia – Onde se iniciou

- Tudo começou no Foreign Broadcast Information Service (FBIS)
- Jornais
- Revistas
- Televisão
- Pioneiro no uso de Open Source Intelligence (OSINT)
- Deram início ao projeto na década de 1930 na Universidade de Princeton

# Historia – Segunda guerra e o FBI

- Sua função era analisar os noticiários por rádio e monitorar publicações oficiais da União das repúblicas Socialistas Soviéticas
- Já em 8 de novembro de 2005 foi anunciado por John Negroponte o Open Source Center (OSC) que é um braço da CIA (depois do 11 de setembro de 2001)
- Coletar , reunir e trabalhar as informações
- Foi ai que deu inicio ao termo OSINT

# Leis – O que eu posso e não posso

- Invasão de dispositivos
- Violar mecanismos de segurança para obter vantagem indevida
- Obter informações
- Adulterar
- Destruir
- Graças às técnicas de buscas usando OSINT podemos começar a procura de informações válidas e falhas em possíveis clientes.

# Motivação

- Problemas com leis
- Problemas com permissão das empresas
- Problemas com logs
- Buscar por determinada vulnerabilidade
- Buscar por arquivos importantes
- Buscar por informações sensíveis
- Monitorar vazamentos

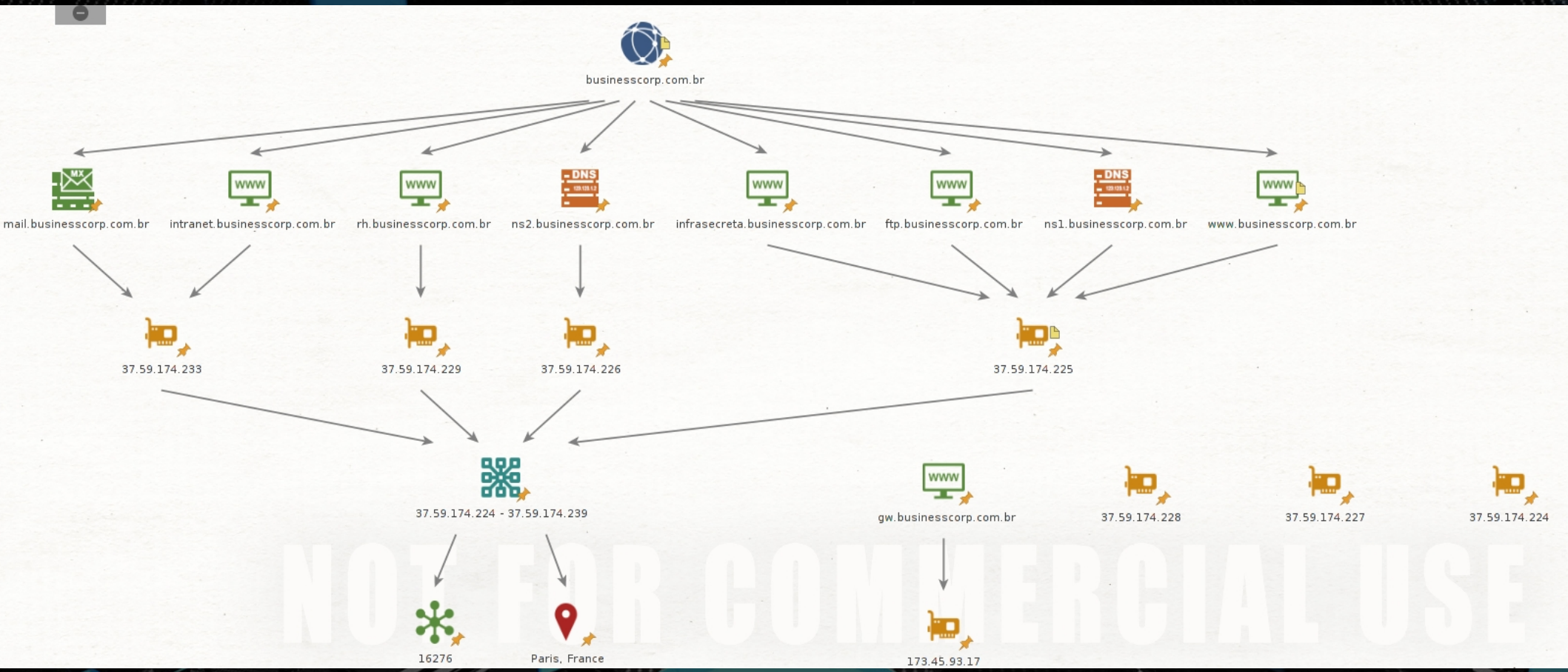
# Motivação

- Problemas com leis
- Problemas com permissão das empresas
- Problemas com logs
- Buscar por determinada vulnerabilidade
- Buscar por arquivos importantes
- Buscar por informações sensíveis
- Monitorar vazamentos

# OSINT – Buscando informações públicas

- Informações sobre infraestruturas

# Um pouco da meta ....



# Whois - Quem é?

## Realizando consulta com Python3 + API

```
 % python3 whois-ip.py
200

nic-hdl-br:  RES59
person:      Regina Sampaio
e-mail:      fapesp@corp.globo.com
country:     BR
created:     19991110
changed:     20180917

nic-hdl-br:  CSGLO
person:      CSIRT Globo.com
e-mail:      csirt@csirt.globo
country:     BR
created:     20150903
changed:     20160104

nic-hdl-br:  CTG6
person:      Contato Técnico - Globo.com
e-mail:      fapesp@corp.globo.com

inetnum:     186.192.80.0/20
aut-num:     AS28604
abuse-c:     CSGLO
owner:       Globo Comunicação e Participaçoes SA
ownerid:     27.865.757/0024-90
responsible: Regina Sampaio
country:     BR
      c:     RES59
      :      CTG6
      v:     186.192.80.0/20
      r:     ns01.oghost.com.br
      :      20190524 AA
     aa:     20190524
      r:     ns04.oghost.com.br
      :      20190524 AA
     aa:     20190524
      r:     ns03.oghost.com.br
```

# Sharingmyip - Sites que usam mesmo IP

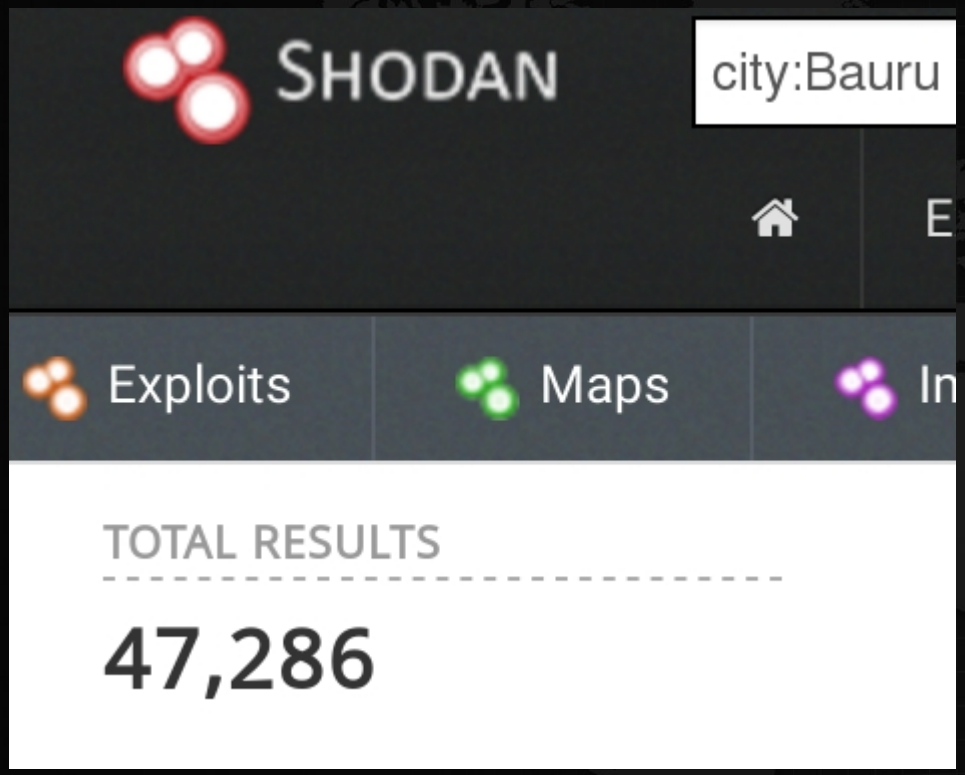
```
== Related DNS entries for www.businesscorp.com.br ==
www.businesscorp.com.br - 37.59.174.225
mail.businesscorp.com.br - 37.59.174.233
ns1.businesscorp.com.br - 37.59.174.225
ns2.businesscorp.com.br - 37.59.174.226
gw.businesscorp.com.br - 173.45.93.17
ftp.businesscorp.com.br - 37.59.174.225
rh.businesscorp.com.br - 37.59.174.229
intranet.businesscorp.com.br - 37.59.174.233
```

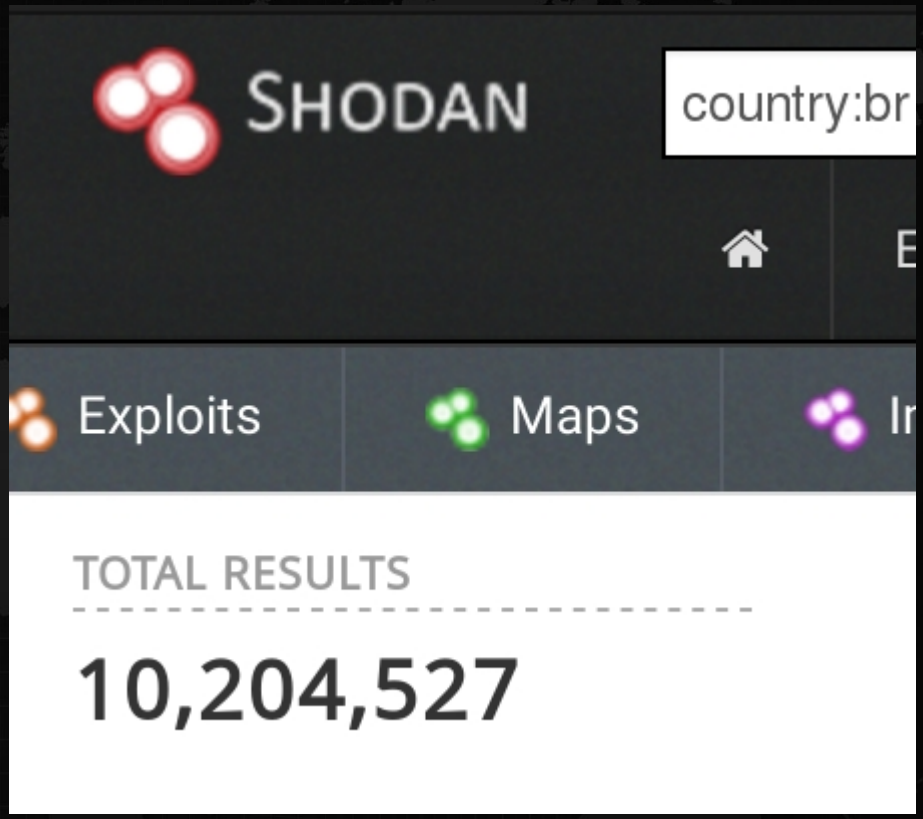
# Sharingmyip - Sites que usam mesmo IP

Coleta de dados com Python3

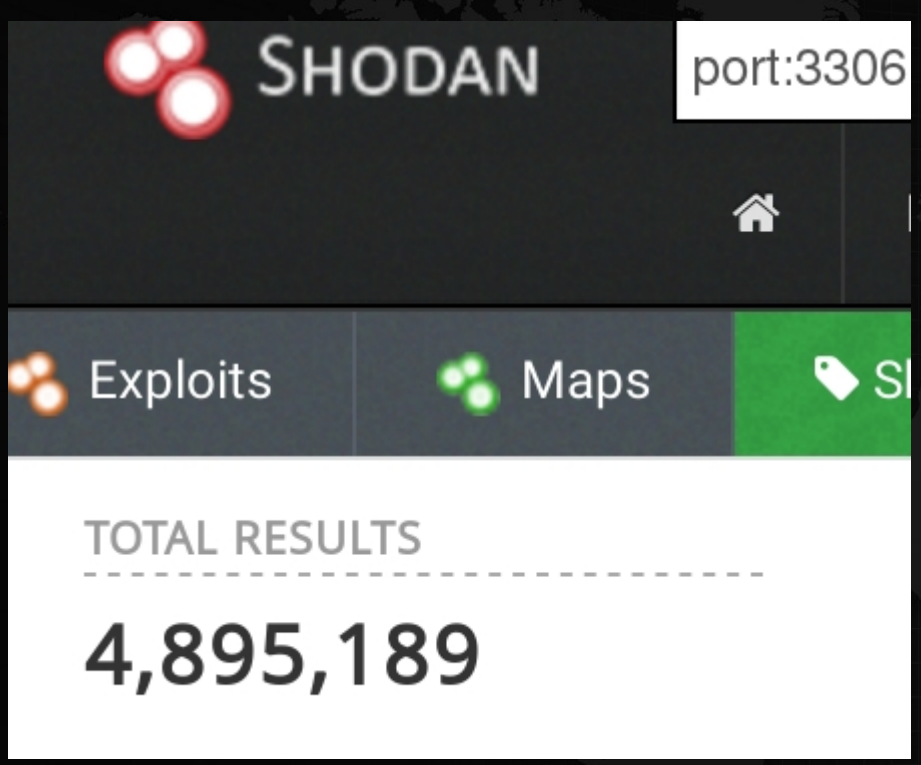
```
 % python3 sharingmyip.py
Site (s) neste endereço 8.8.8.8
www.businesscorp.com.br
ns1.businesscorp.com.br
ftp.businesscorp.com.br
businesscorp.com.br

DNS para  businesscorp.com.br
businesscorp.com.br name server ns2.businesscorp.com.br.
businesscorp.com.br name server ns1.businesscorp.com.br.
businesscorp.com.br mail is handled by 10 mail.businesscorp.com.br.
businesscorp.com.br has address 37.59.174.225
businesscorp.com.br has no AAAA record

Entradas de DNS relacionadas para businesscorp.com.br
www.businesscorp.com.br - 37.59.174.225
mail.businesscorp.com.br - 37.59.174.233
ns1.businesscorp.com.br - 37.59.174.225
ns2.businesscorp.com.br - 37.59.174.226
ftp.businesscorp.com.br - 37.59.174.225
rh.businesscorp.com.br - 37.59.174.229
intranet.businesscorp.com.br - 37.59.174.233
```

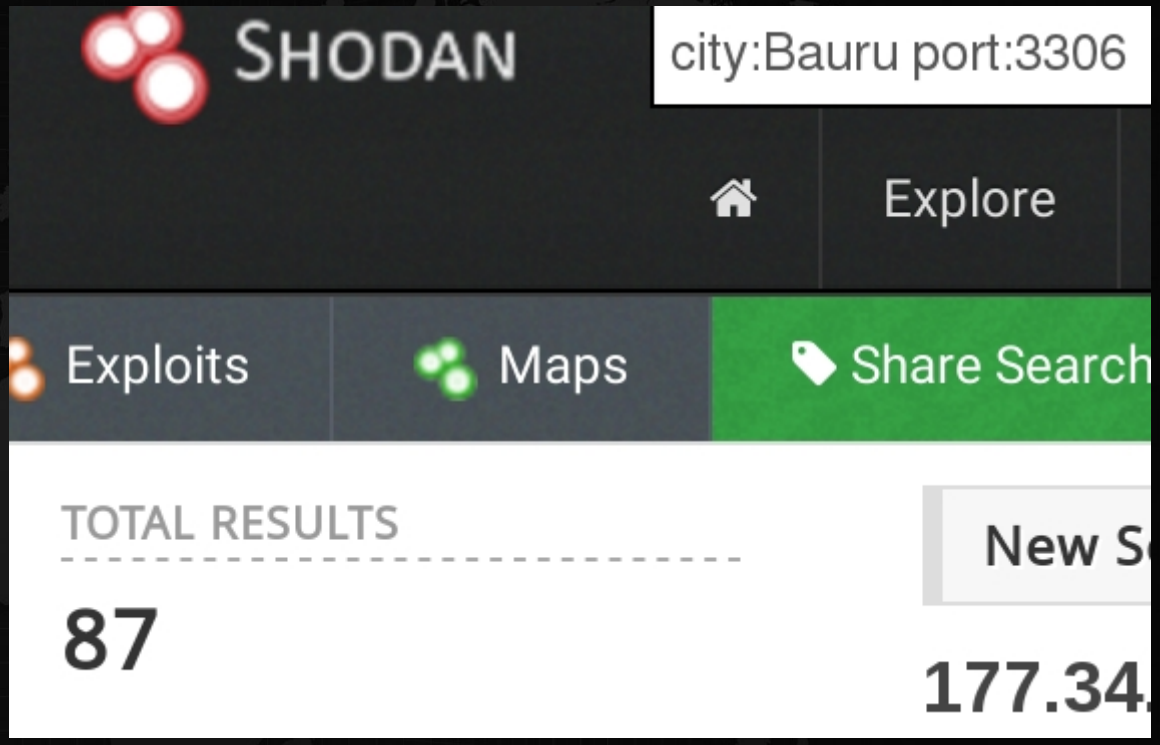
# Shodan – Operadores



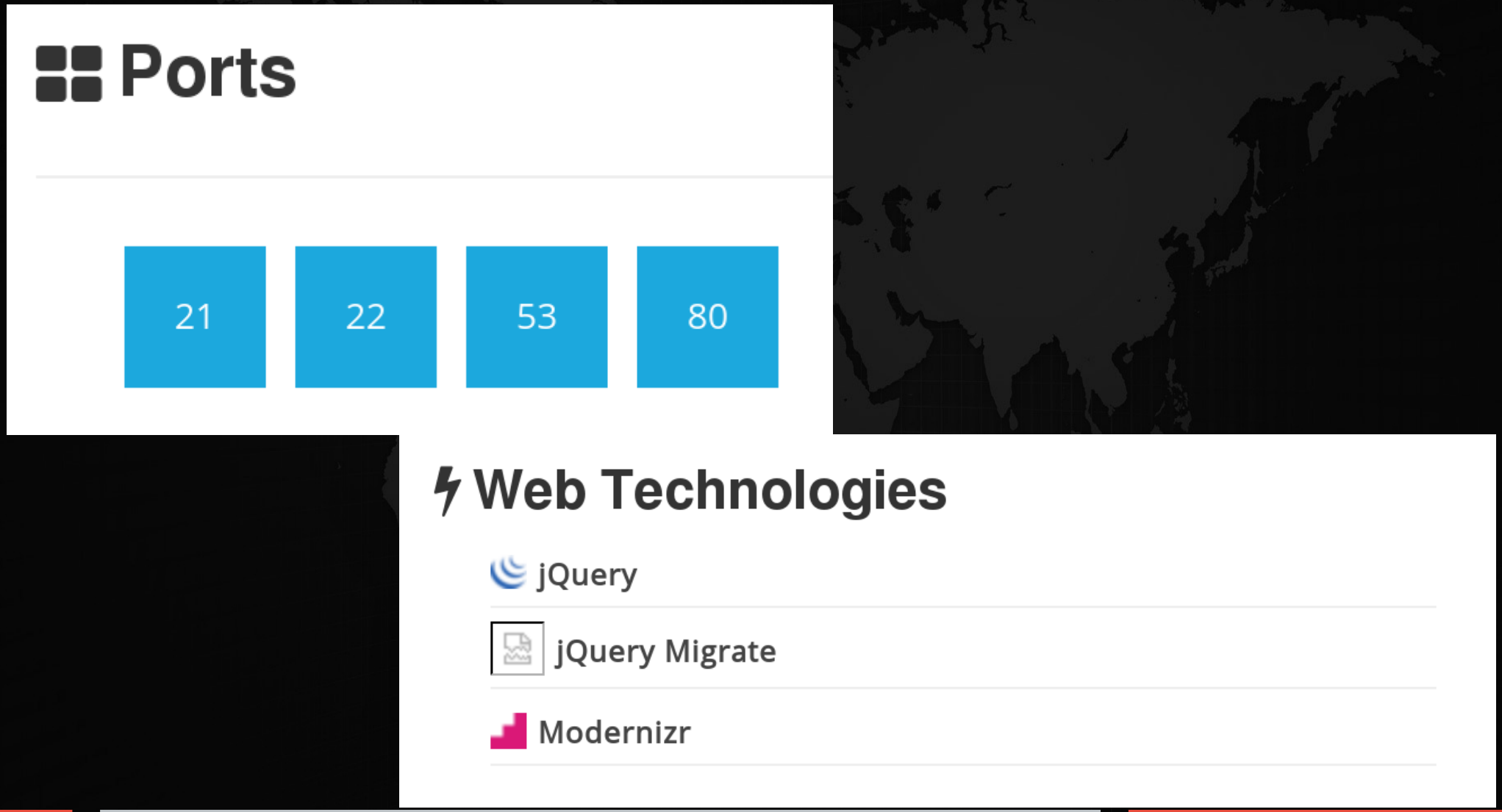



# Shodan – Operadores



# Shodan – Operadores



# Shodan – Operadores

## ⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

| | |
|---|---|
| **CVE-2012-4558** | Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string. |
| **CVE-2013-1896** | mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI. |

# Shodan – Via linha de comando CLI

```
root@57b6bb7d46be:/# shodan host 37.59.174.225
37.59.174.225
Hostnames:                ip225.ip-37-59-174.eu
Country:                  France
Operating System:         Linux 3.x
Organization:             OVH SAS
Updated:                  2019-05-21T09:43:48.284755
Number of open ports:     4
Vulnerabilities:          CVE-2012-4558  CVE-2013-1896   CVE-2012-3499   CVE-20
-0231   CVE-2017-7679   CVE-2013-2249   CVE-2016-4975   CVE-2013-5704   CVE-20
-7668   CVE-2013-6438   CVE-2012-2687   CVE-2017-3167   CVE-2017-3169   CVE-20
-0098   CVE-2013-1862   CVE-2016-8612

Ports:
     21/tcp ProFTPD (1.3.4a)
     22/tcp OpenSSH (6.0p1 Debian 4+deb7u2)
     53/udp
     80/tcp Apache httpd (2.2.22)
```

# Censys -

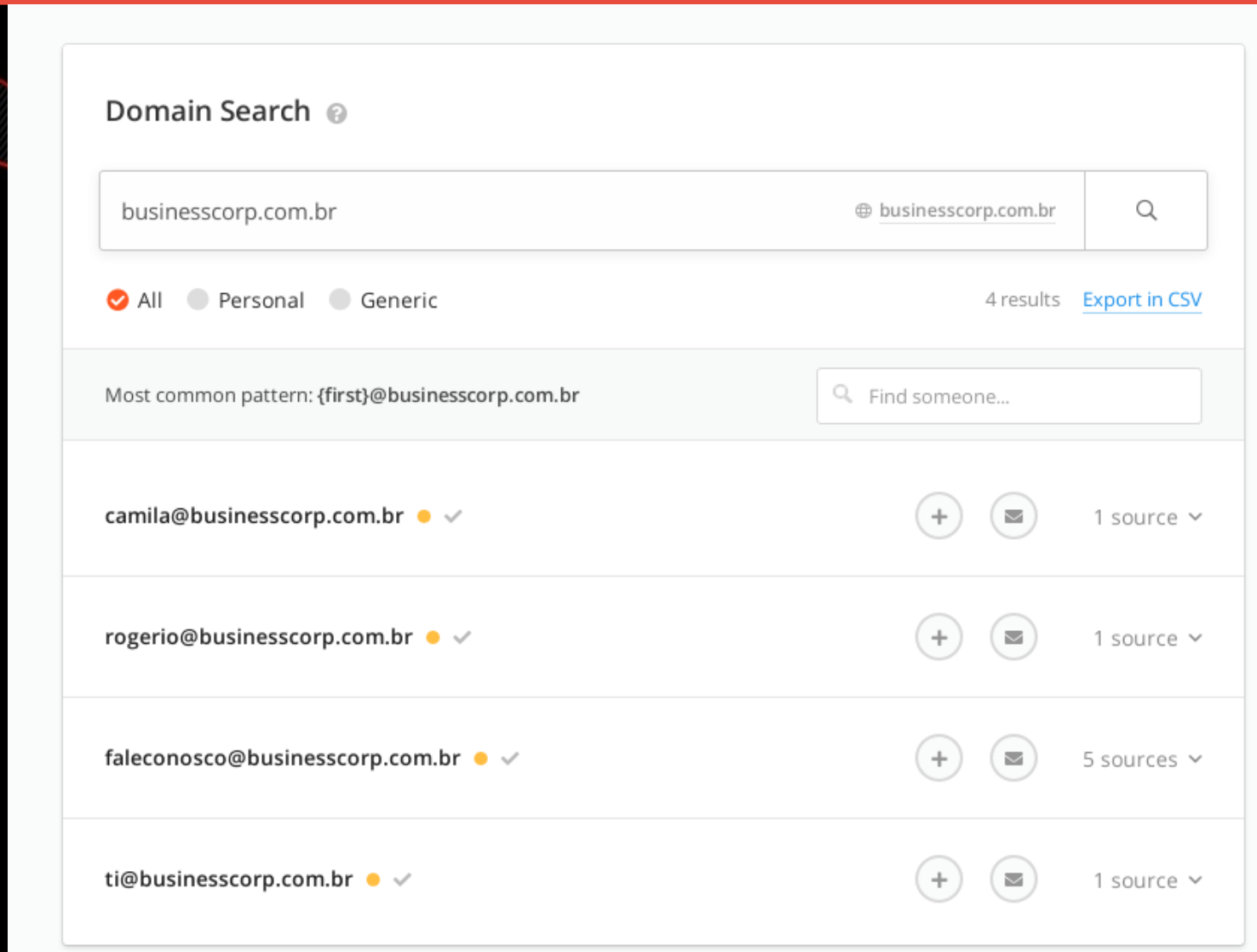
- Censys criado em 2015 na universidade de Michigan
- Busca de dispositivos , redes e infraestruturas
- 45 das Fortune 500 usa dados do Censys
- Latitude/Longitude ,País , Rota , Portas abertas e protocolos
- Podemos ver o tipo de servidor usado
- Status do teste
- Titulo do IP usado
- Nome da rede de sites e IPS.

# Censys -


**Geographic Location**

| | |
|---|---|
| **Country** | France (FR) |
| **Lat/Long** | 48.8582, 2.3387 |
| **Timezone** | Europe/Paris |

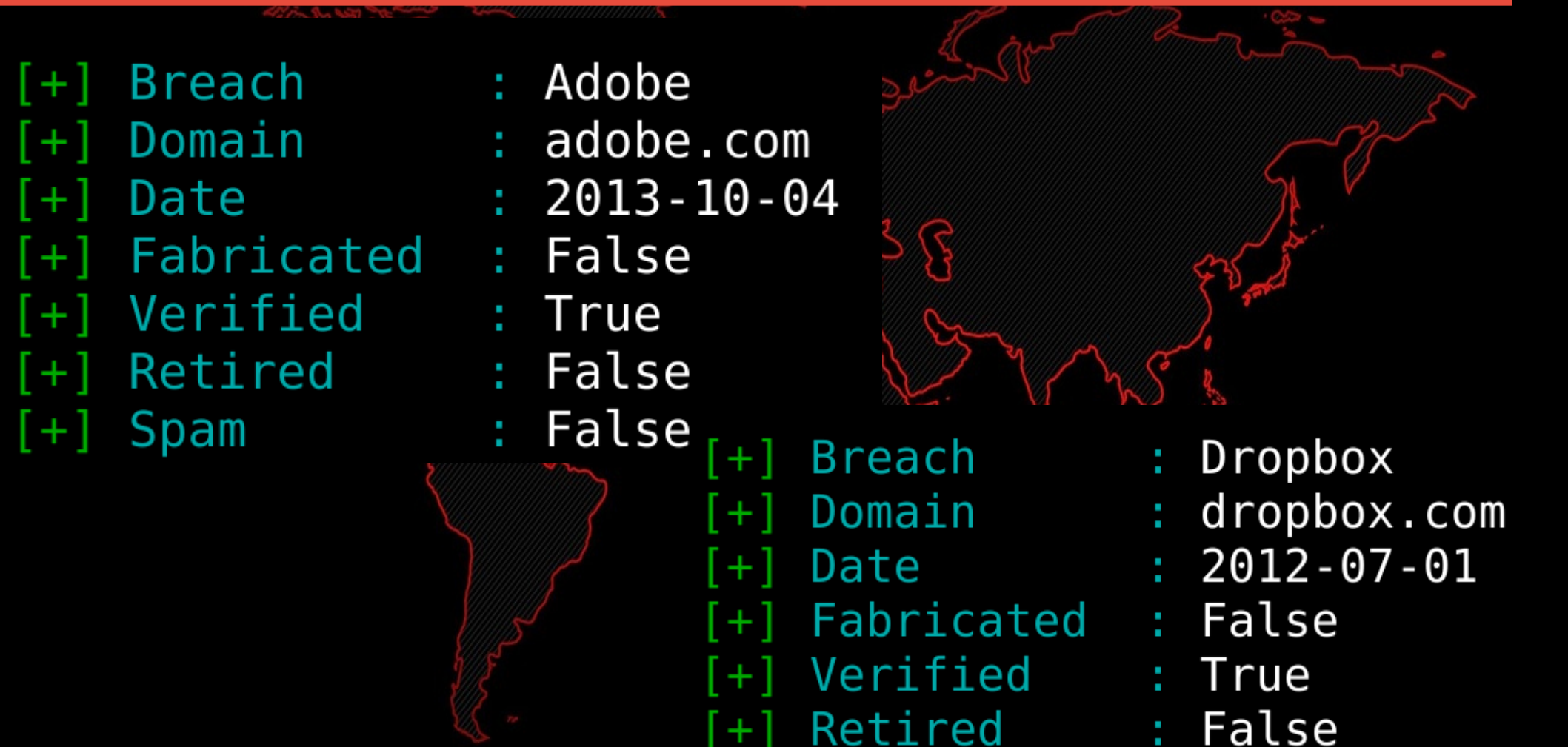
# Hunter.io


Domain Search
businesscorp.com.br
businesscorp.com.br
All
Personal
Generic
4 results
Export in CSV
Most common pattern: {first}@businesscorp.com.br
Find someone...
camila@businesscorp.com.br
1 source
rogerio@businesscorp.com.br
1 source
faleconosco@businesscorp.com.br
5 sources
ti@businesscorp.com.br
1 source

# PwnedOrNot

```
[+] Checking Breach status for nadine.blaser@vale.com [ pwned ]
```

# PwnedOrNot



```
[+] Breach      : Adobe
[+] Domain      : adobe.com
[+] Date        : 2013-10-04
[+] Fabricated  : False
[+] Verified    : True
[+] Retired     : False
[+] Spam        : False
[+] Breach      : Dropbox
[+] Domain      : dropbox.com
[+] Date        : 2012-07-01
[+] Fabricated  : False
[+] Verified    : True
[+] Retired     : False
[+] Spam        : False
```

# Twitter-intelligence

```
python3 tracking.py --query "leak password"

python3 tracking.py --query "leak passwords"
```

```
python3 tracking.py --query "leak pass"
```

# Twitter-intelligence

```
python3 tracking.py --query "leak senha" 2019-05-20 2019-05-22

@MesninoOwna: #hacked #DB_leak #C00n3tTeam #OPbr #Vazamento_de_dados_lula_website URL DE USERS
: https://lula.com.br/wp-json/wp/v2/users/ … … URL USERS ADMINISTRADOR : https://lula.com.br/wp
-json/oembed/1.0/embed?url=https://lula.com.br/&format=json … … URL LOGIN : https://lula.com.br
/wp-login.php?redirect_to=https%3A%2F%2Flula.com.br%2Fwp-admin%2F&reauth=1 … … -----We Are C00n
3t Team ! ------ #OpAssange @LabDefCon @g1tecnologia

@PC00n3t: #hacked #DB_leak #C00n3tTeam #OPbr #Vazamento_de_dados_lula_website URL DE USERS : ht
tps://lula.com.br/wp-json/wp/v2/users/ … URL USERS ADMINISTRADOR : https://lula.com.br/wp-json/
oembed/1.0/embed?url=https://lula.com.br/&format=json … URL LOGIN : https://lula.com.br/wp-logi
n.php?redirect_to=https%3A%2F%2Flula.com.br%2Fwp-admin%2F&reauth=1 … -----We Are C00n3t Team !
#OpAssange @LabDefCon @g1tecnologiapic.twitter.com/uzcfRcBokB

@PC00n3t: #hacked #leaks #Vazamento @LabDefCon @g1tecnologia #OpLulaLindo Camera Aurora [SC] LI
NK : https://pastebin.com/c0tXeyxb by : Pep1no && Web Kiddie ------We Are C00n3t------- #FreeAs
sange #OpAssange #OpBr @Tec_Mundopic.twitter.com/NDv66nx6zn

@PC00n3t: #Vazamento #leaks #C00n3tTeam #OpLulaLindo @LabDefCon Se não me der uma namorada, vou
 continuar vazando, rsrs. Vazamento DETRAN Link : https://pastebin.com/erRjtcES by : Pep1no &&
Web Kiddie ----We Are C00n3t Team----- #OpAssange #FreeAssange @g1tecnologiapic.twitter.com/Llz
sqekCmH
```

# LGPD e o futuro

- A Lei Geral de Proteção de Dados Pessoais
- É a legislação brasileira que regula as atividades de tratamento de dados pessoais
- Altera os artigos 7º e 16 do Marco Civil da Internet

# O uso de informações publicas

- Podemos usar toda informação publica
- Legalmente falando podemos usar
- Não quebramos nenhum sistema de segurança
- Temos diversas fontes de informações

# Conclusão

- OSINT pode nos ajudar durante o reconhecimento
- Podemos buscar informações sobre vazamentos
- Podemos buscar informações sobre uma empresa
- Ajuda na espionagem e contra espionagem
- Auxilia na inteligencia comercial e competitiva

# Obrigado

- https://github.com/abase-br/osint ← Material
- https://github.com/abase-br/ ← Outros materiais
- Greenmind.sec@gmail.com ← Meu contato

“A solução dos seus problemas não é dinheiro, politicos ou o governo. . . É conhecimento compartilhado!” - Ton Gadioli