

Turbolist3r: Enumeración de Subdominios

Turbolist3r

Turbolist3r en GitHub

Basado en Sublist3r por Ahmed Aboul-Ela - @aboul3la

Bifurcado por Carl Pearson - GitHub

```
python turbolist3r.py -d google.com
```

Sublist3r

Probado. <https://github.com/aboul3la/Sublist3r>

```
% python sublist3r.py -d google.com
```

```
**Configuración de Proxy Detectada:**
```

```
- HTTP_PROXY: http://127.0.0.1:7890
```

```
- HTTPS_PROXY: http://127.0.0.1:7890
```

```

  ----      -      - -      -      ----
/  ___| _   _| |__| ( )___| | |___ /  _
\___ \ | | | | ' \ | | /  __| __| | \ | '___|
   __) | | | | |) | | \__ \ | ___) | |
|____/ \__,_|_|_./|_|_|___/\__|_____|_|

```

Este es un diseño ASCII que representa un título o encabezado. No requiere traducción, ya que es un arte visual basado en caracteres.

```
# Codificado por Ahmed Aboul-Ela - @aboul3la
```

```
[-] Enumerando subdominios ahora para google.com
```

```
[-] Buscando ahora en Baidu..
```

```
[-] Buscando ahora en Yahoo..
```

```
[-] Buscando ahora en Google..
```

```
[-] Buscando ahora en Bing..
```

```
[-] Buscando ahora en Ask..
```

```
[-] Buscando ahora en Netcraft..
```

[-] Buscando ahora en DNSdumpster..

[-] Buscando ahora en Virustotal..

[-] Buscando ahora en ThreatCrowd..

[-] Buscando ahora en Certificados SSL..

[-] Buscando ahora en PassiveDNS..

Proceso DNSdumpster-8:

Traceback (most recent call last):

File "/Users/lzwjava/anaconda3/lib/python3.10/multiprocessing/process.py", line 314, in _bootstrap

self.run()

File "/Users/lzwjava/projects/Sublist3r/sublist3r.py", line 268, in run

domain_list = self.enumerate()

File "/Users/lzwjava/projects/Sublist3r/sublist3r.py", line 647, in enumerate

token = self.get_csrf_token(resp)

File "/Users/lzwjava/projects/Sublist3r/sublist3r.py", line 641, in get_csrf_token

token = csrf_regex.findall(resp)[0]

IndexError: list index out of range

[!] Error: Virustotal probablemente ahora está bloqueando nuestras solicitudes

[-] Total de subdominios únicos encontrados: 97

www.google.com

accounts.google.com

freezone.accounts.google.com

adwords.google.com

qa.adz.google.com

answers.google.com

apps-secure-data-connector.google.com

audioads.google.com

checkout.google.com

mtv-da-1.ad.corp.google.com

ads-compare.eem.corp.google.com

da.ext.corp.google.com

m.guts.corp.google.com

m.gutsdev.corp.google.com

login.corp.google.com

mtv-da.corp.google.com

mygeist.corp.google.com

mygeist2010.corp.google.com
proxyconfig.corp.google.com
reseed.corp.google.com
twdsalesgsa.twd.corp.google.com
uberproxy.corp.google.com
uberproxy-nocert.corp.google.com
uberproxy-san.corp.google.com
ext.google.com
cag.ext.google.com
cod.ext.google.com
da.ext.google.com
eggroll.ext.google.com
fra-da.ext.google.com
glass.ext.google.com
glass-eur.ext.google.com
glass-mtv.ext.google.com
glass-twd.ext.google.com
hot-da.ext.google.com
hyd-da.ext.google.com
ice.ext.google.com
meeting.ext.google.com
mtv-da.ext.google.com
soaproxyprod01.ext.google.com
soaproxytest01.ext.google.com
spdy-proxy.ext.google.com
spdy-proxy-debug.ext.google.com
twd-da.ext.google.com
flexpack.google.com
www.flexpack.google.com
accounts.flexpack.google.com
gaiastaging.flexpack.google.com
mail.flexpack.google.com
plus.flexpack.google.com
search.flexpack.google.com
freezone.google.com
www.freezone.google.com

accounts.freezone.google.com
gaiastaging.freezone.google.com
mail.freezone.google.com
news.freezone.google.com
plus.freezone.google.com
search.freezone.google.com
gmail.google.com
hosted-id.google.com
jmt0.google.com
aspmx.l.google.com
alt1.aspmx.l.google.com
alt2.aspmx.l.google.com
alt3.aspmx.l.google.com
alt4.aspmx.l.google.com
gmail-smtp-in.l.google.com
alt1.gmail-smtp-in.l.google.com
alt2.gmail-smtp-in.l.google.com
alt3.gmail-smtp-in.l.google.com
alt4.gmail-smtp-in.l.google.com
gmr-smtp-in.l.google.com
alt1.gmr-smtp-in.l.google.com
alt2.gmr-smtp-in.l.google.com
alt3.gmr-smtp-in.l.google.com
alt4.gmr-smtp-in.l.google.com
vp.video.l.google.com
m.google.com
freezone.m.google.com
mail.google.com
freezone.mail.google.com
misc.google.com
misc-sni.google.com
mtalk.google.com
mx.google.com
ics.prod.google.com
sandbox.google.com
cert-test.sandbox.google.com

ecc-test.sandbox.google.com

services.google.com

talk.google.com

upload.google.com

dg.video.google.com

upload.video.google.com

wifi.google.com

onex.wifi.google.com

““