The poor man’s QUANTUM

@x0rz

Beer rump 2017

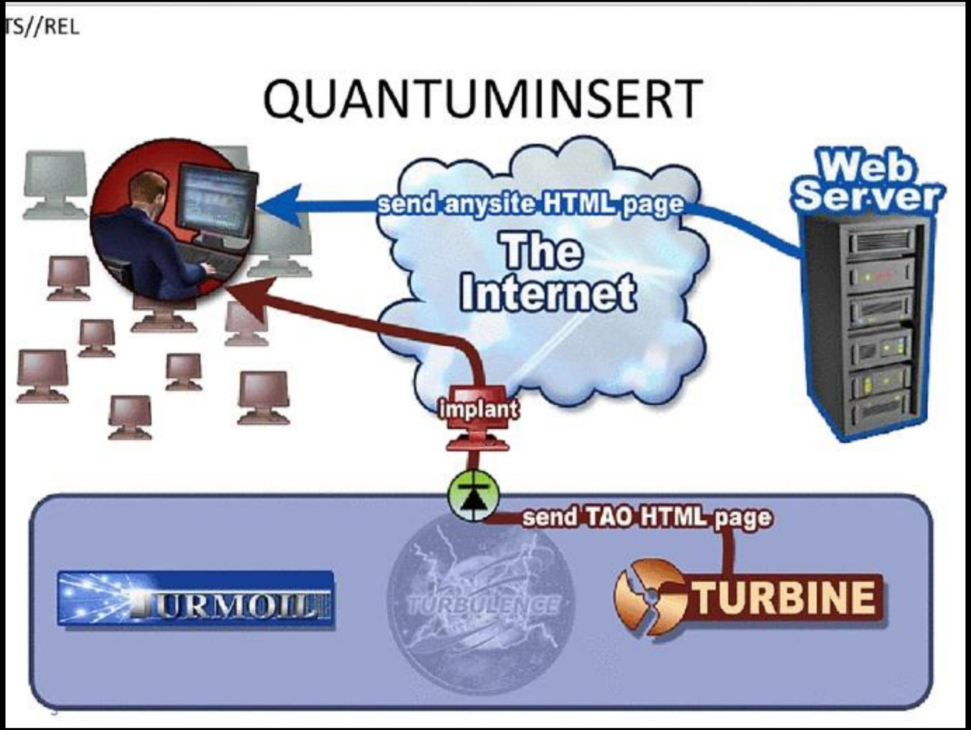
Disclaimer: des parties ont été supprimés pour des raisons de confidentialité

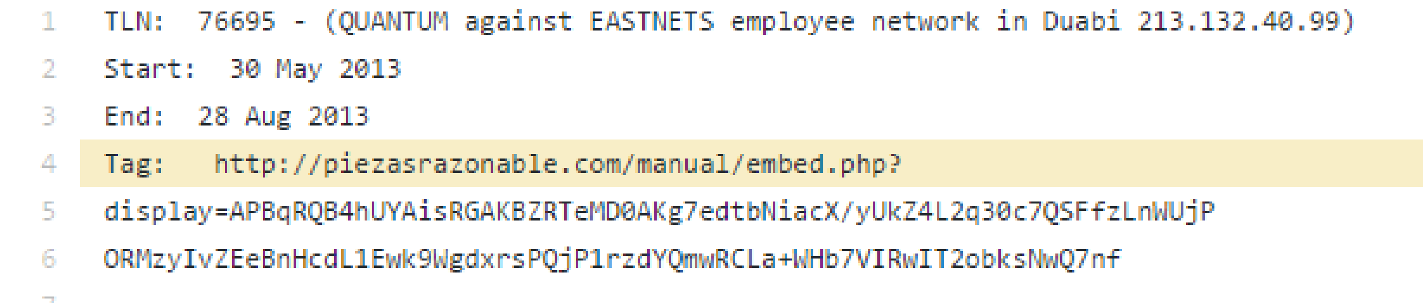
Merci de vous référer au blog

https://blog.0day.rocks/practical-waterholing-through-dns-typosquatting-e252e6a2f99e

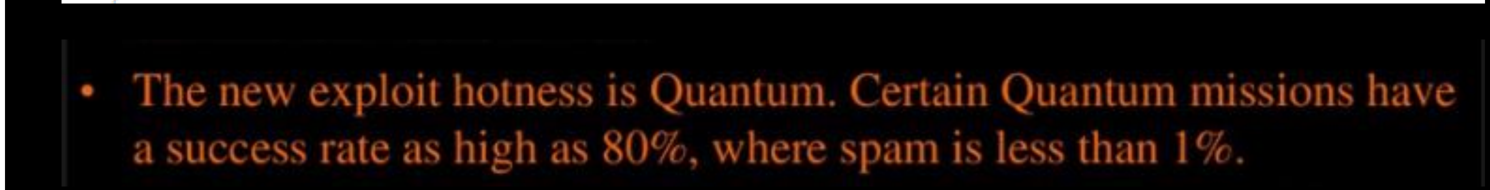
QUANTUM?

Man-on-the-side at Internet scale

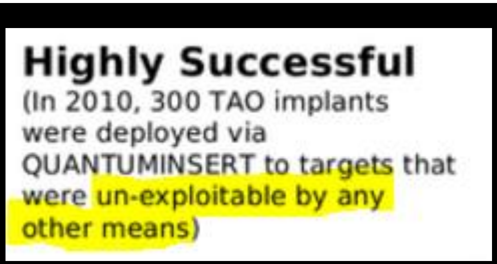




```
TLN:  76695 - (QUANTUM against EASTNETS employee network in Duabi 213.132.40.99)
Start:  30 May 2013
End:  28 Aug 2013
Tag:   http://piezasrazonable.com/manual/embed.php?
display=APBqRQB4hUYAisRGAKBZRTeMD0AKg7edtbNiacX/yUkZ4L2q30c7QSFfzLnWUjP
ORMzyIvZEeBnHcdL1Ewk9WgdxrsPQjP1rzdYQmwRCLa+WHb7VIRwIT2obksNwQ7nf
```



- The new exploit hotness is Quantum. Certain Quantum missions have a success rate as high as 80%, where spam is less than 1%.



Highly Successful
(In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)

Poor man’s QUANTUM

DNS typosquatting

Typcial uesr in atcion

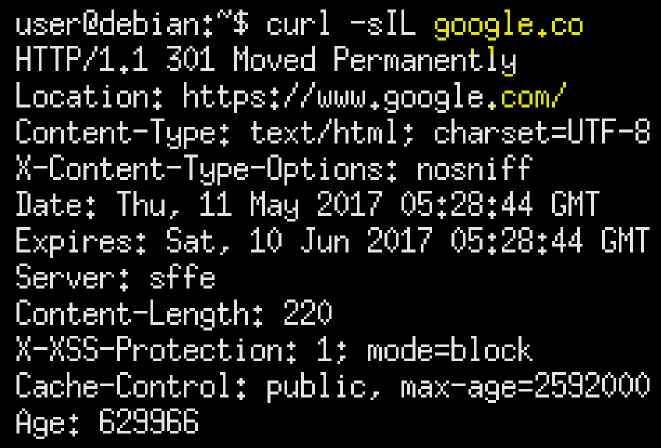
Character omission

.com - .com (Columbia)

.com - .com (Cameroun)

.net - .net (Niger)

…

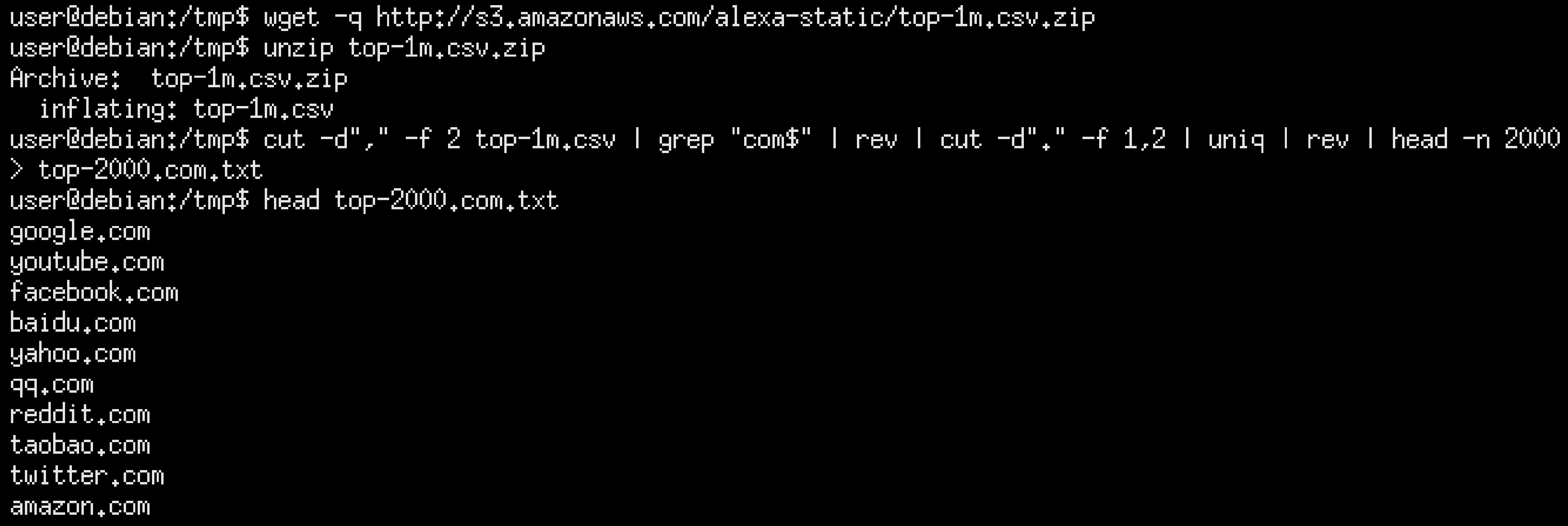


```
user@debian:~$ curl -sIL google.co
HTTP/1.1 301 Moved Permanently
Location: https://www.google.com/
Content-Type: text/html; charset=UTF-8
X-Content-Type-Options: nosniff
Date: Thu, 11 May 2017 05:28:44 GMT
Expires: Sat, 10 Jun 2017 05:28:44 GMT
Server: sffe
Content-Length: 220
X-XSS-Protection: 1; mode=block
Cache-Control: public, max-age=2592000
Age: 629966
```

D’autres vecteurs: le bitsquatting (2011)

http://dinaburg.org/bitsquatting.html

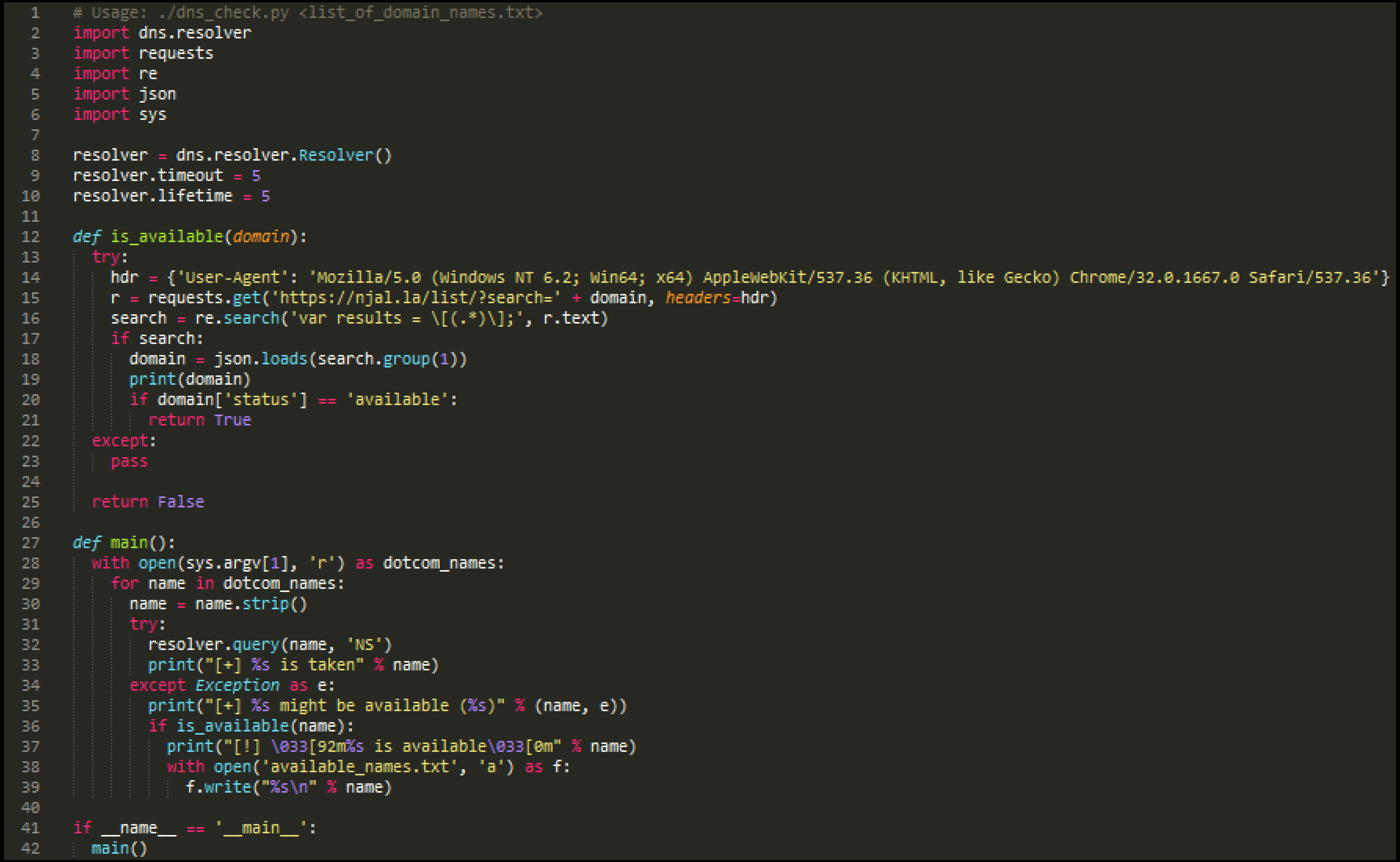
1) Récupérer la liste des domaines les plus populaires



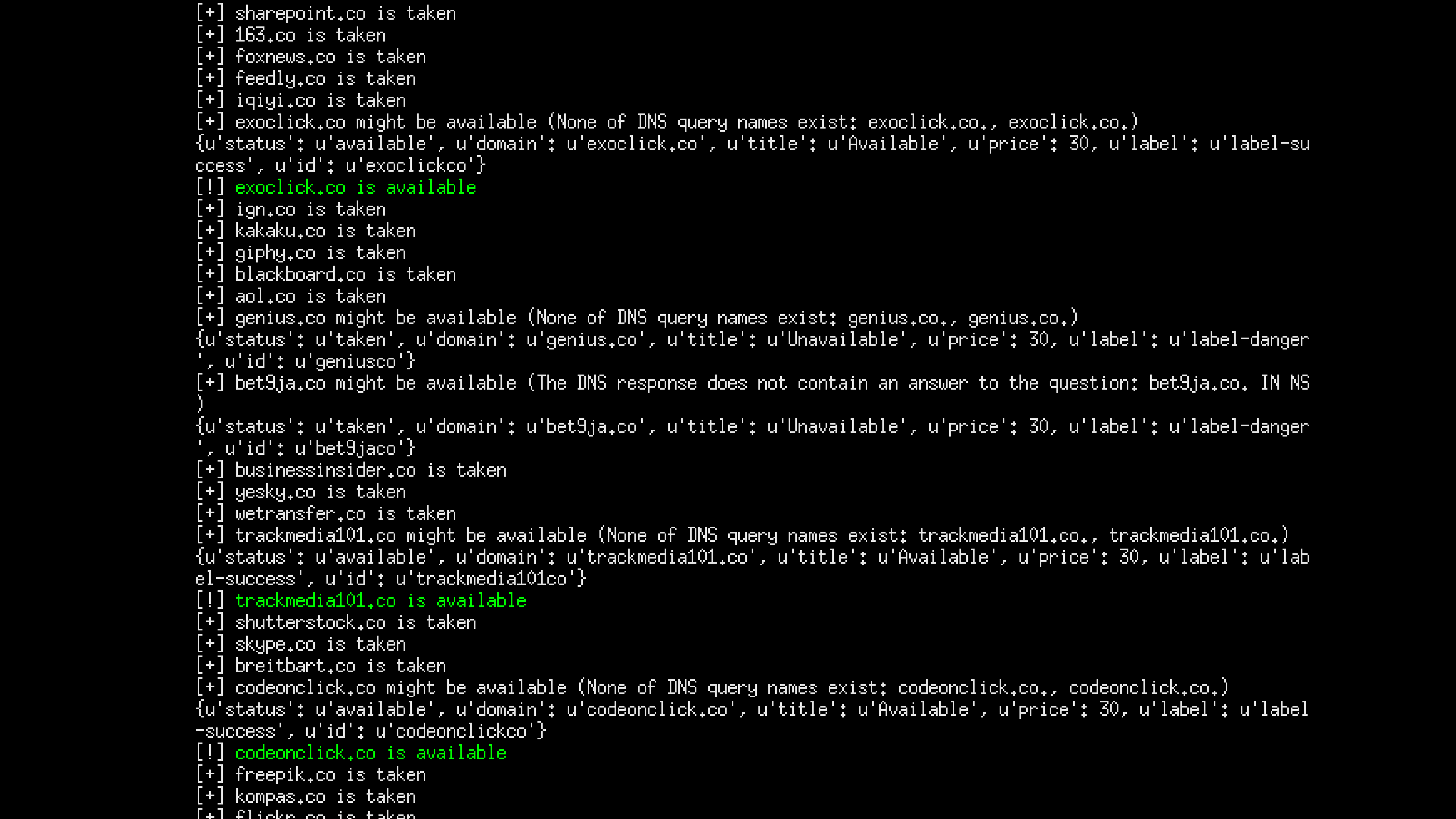
```
user@debian:/tmp$ wget -q http://s3.amazonaws.com/alexa-static/top-1m.csv.zip
user@debian:/tmp$ unzip top-1m.csv.zip
Archive:  top-1m.csv.zip
  inflating: top-1m.csv
user@debian:/tmp$ cut -d"," -f 2 top-1m.csv | grep "com$" | rev | cut -d"." -f 1,2 | uniq | rev | head -n 2000
> top-2000.com.txt
user@debian:/tmp$ head top-2000.com.txt
google.com
youtube.com
facebook.com
baidu.com
yahoo.com
qq.com
reddit.com
taobao.com
twitter.com
amazon.com
```

2) Lister les domaines disponibles

https://gist.github.com/x0rz/80b4b93baa5b33ed25e1823d3494f0a8



```python
# Usage: ./dns_check.py <list_of_domain_names.txt>
import dns.resolver
import requests
import re
import json
import sys

resolver = dns.resolver.Resolver()
resolver.timeout = 5
resolver.lifetime = 5

def is_available(domain):
  try:
    hdr = {'User-Agent': 'Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1667.0 Safari/537.36'}
    r = requests.get('https://njal.la/list/?search=' + domain, headers=hdr)
    search = re.search('var results = \[(.*)\];', r.text)
    if search:
      domain = json.loads(search.group(1))
      print(domain)
      if domain['status'] == 'available':
        return True
  except:
    pass

  return False

def main():
  with open(sys.argv[1], 'r') as dotcom_names:
    for name in dotcom_names:
      name = name.strip()
      try:
        resolver.query(name, 'NS')
        print("[+] %s is taken" % name)
      except Exception as e:
        print("[+] %s might be available (%s)" % (name, e))
        if is_available(name):
          print("[!] \033[92m%s is available\033[0m" % name)
          with open('available_names.txt', 'a') as f:
            f.write("%s\n" % name)

if __name__ == '__main__':
  main()
```



```
[+] sharepoint.co is taken
[+] 163.co is taken
[+] foxnews.co is taken
[+] feedly.co is taken
[+] iqiyi.co is taken
[+] exoclick.co might be available (None of DNS query names exist: exoclick.co., exoclick.co.)
{u'status': u'available', u'domain': u'exoclick.co', u'title': u'Available', u'price': 30, u'label': u'label-su
ccess', u'id': u'exoclickco'}
[!] exoclick.co is available
[+] ign.co is taken
[+] kakaku.co is taken
[+] giphy.co is taken
[+] blackboard.co is taken
[+] aol.co is taken
[+] genius.co might be available (None of DNS query names exist: genius.co., genius.co.)
{u'status': u'taken', u'domain': u'genius.co', u'title': u'Unavailable', u'price': 30, u'label': u'label-danger
', u'id': u'geniusco'}
[+] bet9ja.co might be available (The DNS response does not contain an answer to the question: bet9ja.co. IN NS
)
{u'status': u'taken', u'domain': u'bet9ja.co', u'title': u'Unavailable', u'price': 30, u'label': u'label-danger
', u'id': u'bet9jaco'}
[+] businessinsider.co is taken
[+] yesky.co is taken
[+] wetransfer.co is taken
[+] trackmedia101.co might be available (None of DNS query names exist: trackmedia101.co., trackmedia101.co.)
{u'status': u'available', u'domain': u'trackmedia101.co', u'title': u'Available', u'price': 30, u'label': u'lab
el-success', u'id': u'trackmedia101co'}
[!] trackmedia101.co is available
[+] shutterstock.co is taken
[+] skype.co is taken
[+] breitbart.co is taken
[+] codeonclick.co might be available (None of DNS query names exist: codeonclick.co., codeonclick.co.)
{u'status': u'available', u'domain': u'codeonclick.co', u'title': u'Available', u'price': 30, u'label': u'label
-success', u'id': u'codeonclickco'}
[!] codeonclick.co is available
[+] freepik.co is taken
[+] kompas.co is taken
[+] flickr.co is taken
```

$50 worth of bitcoin later

```
<REDACTED>
```

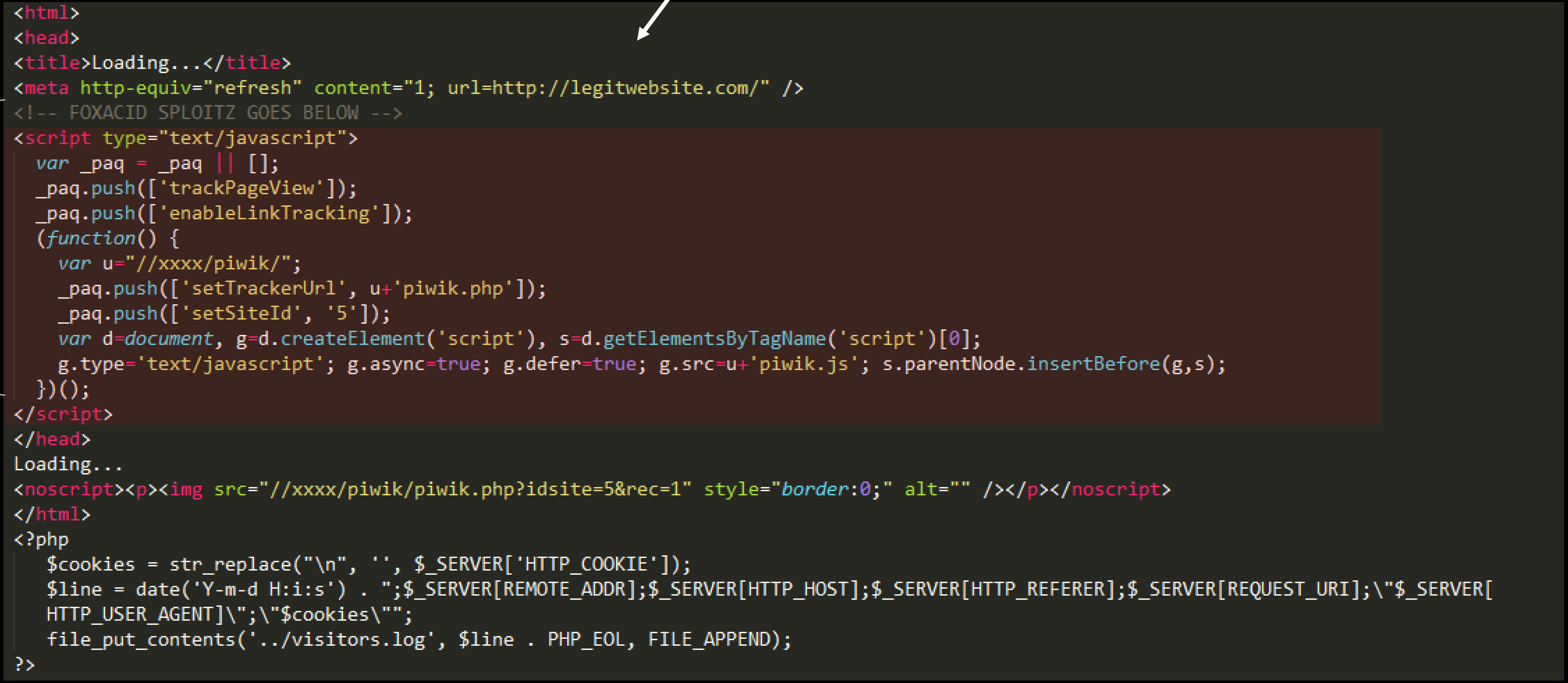
3) Mettre en place son serveur

- Rediriger tous les domaines et sous-domaines vers son IP
- Mettre en place une page de redirection + payload JavaScript
- …
- Attendre le client 😈

Redirection HTML (meta refresh)

Code JavaScript (ExploitKit ou Piwik)

Log PHP

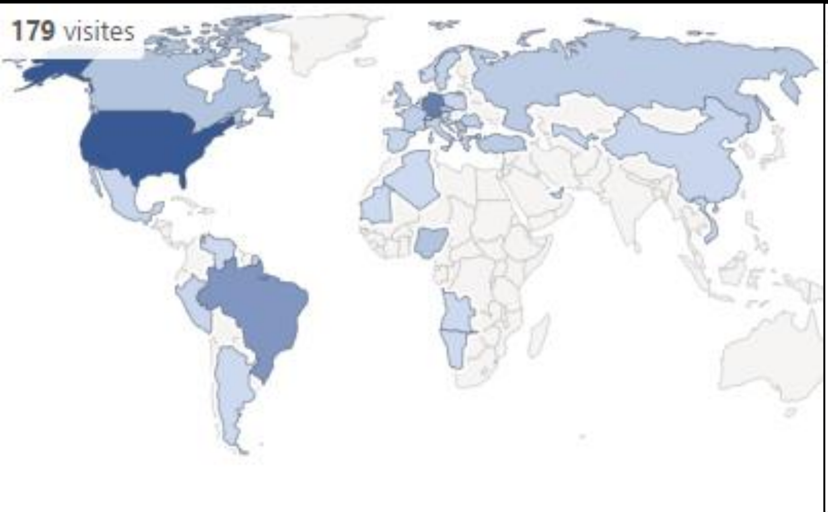


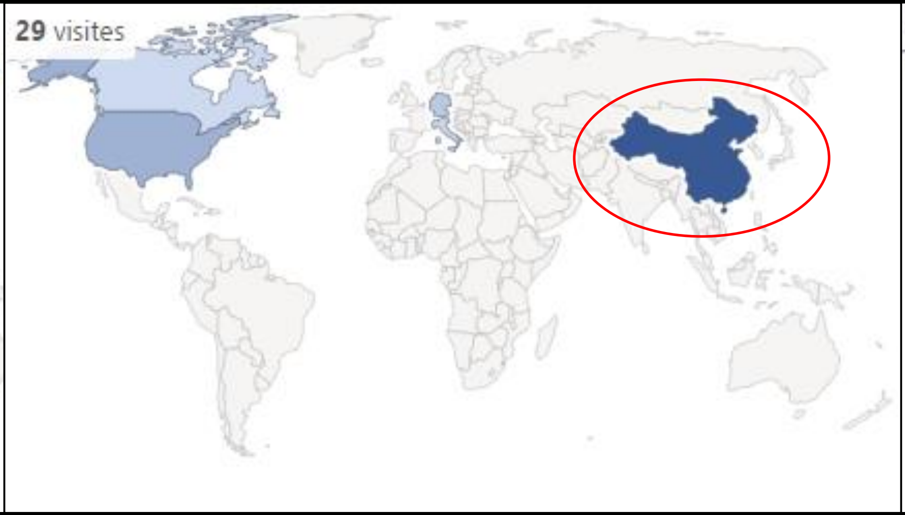
```
<html>
<head>
<title>Loading...</title>
<meta http-equiv="refresh" content="1; url=http://legitwebsite.com/" />
<!-- FOXACID SPLOITZ GOES BELOW -->
<script type="text/javascript">
  var _paq = _paq || [];
  _paq.push(['trackPageView']);
  _paq.push(['enableLinkTracking']);
  (function() {
    var u="//xxxx/piwik/";
    _paq.push(['setTrackerUrl', u+'piwik.php']);
    _paq.push(['setSiteId', '5']);
    var d=document, g=d.createElement('script'), s=d.getElementsByTagName('script')[0];
    g.type='text/javascript'; g.async=true; g.defer=true; g.src=u+'piwik.js'; s.parentNode.insertBefore(g,s);
  })();
</script>
</head>
Loading...
<noscript><p><img src="//xxxx/piwik/piwik.php?idsite=5&rec=1" style="border:0;" alt="" /></p></noscript>
</html>
<?php
   $cookies = str_replace("\n", '', $_SERVER['HTTP_COOKIE']);
   $line = date('Y-m-d H:i:s') . ";$_SERVER[REMOTE_ADDR];$_SERVER[HTTP_HOST];$_SERVER[HTTP_REFERER];$_SERVER[REQUEST_URI];\"$_SERVER[
   HTTP_USER_AGENT]\";\"$cookies\"";
   file_put_contents('../visitors.log', $line . PHP_EOL, FILE_APPEND);
?>
```

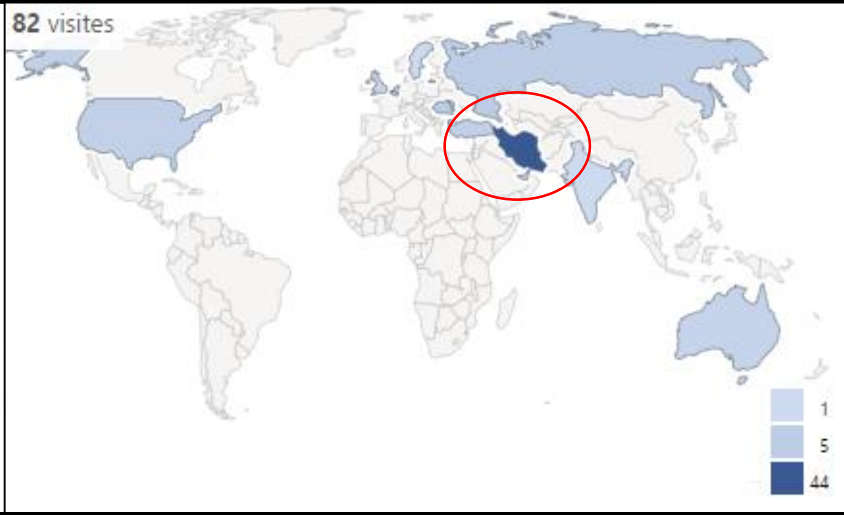
Est-ce que ça marche? 🙏

Statistiques

- 5430 entrées dans le fichier de log sur 40 jours
  - 1764 en enlevant les bots/crawlers
    - **916** IP uniques (~23/jour)
  - Seulement 392 visiteurs uniques chargeant le code JS Piwik
    - Ad blockers?
  - 80 pays

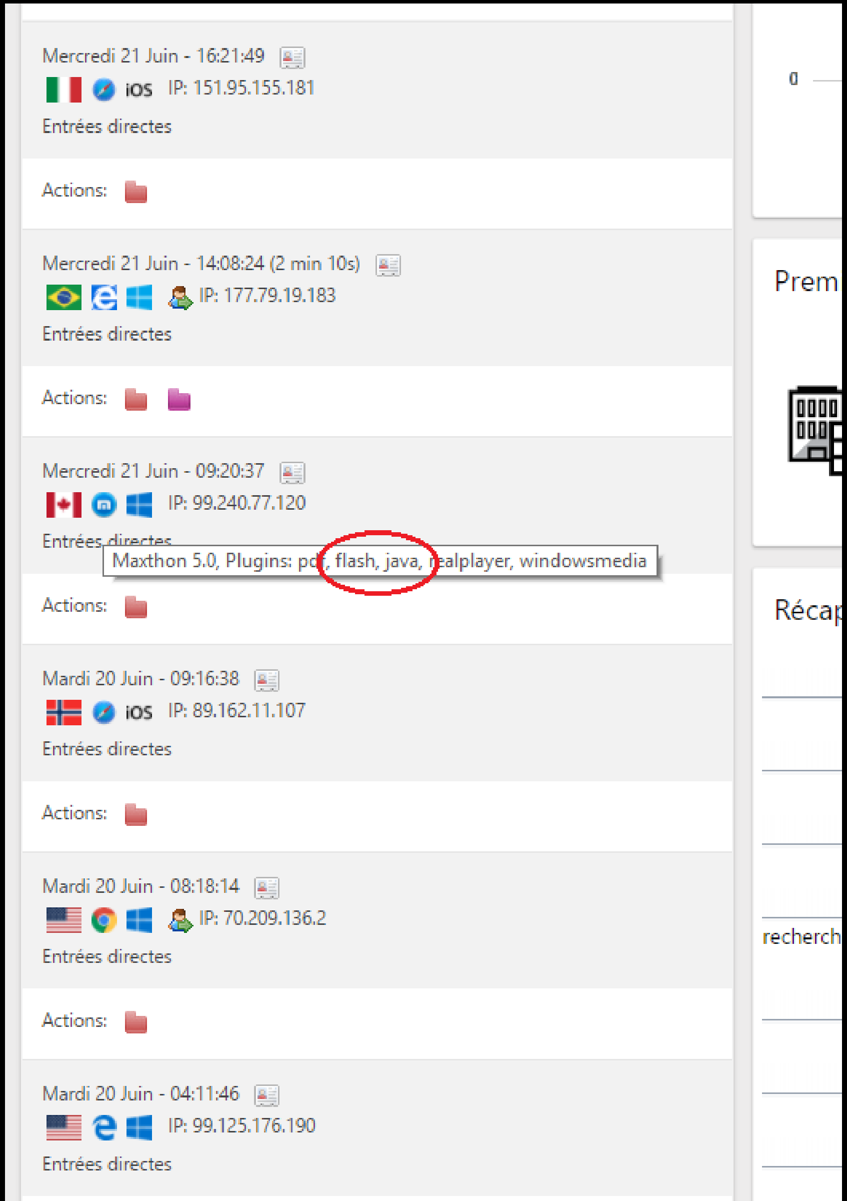






Statistiques

```
2415 CN
1292 US
 823 IR
 198 RU
 114 DE
  67 KR
  63 FR
  52 CA
  37 GB
  34 BR
  33 NL
  26 ??
  25 RO
  22 JP
  19 SE
  16 EG
  14 TR
  14 CH
  13 PL
  11 IE
```



Mercredi 21 Juin - 16:21:49
iOS IP: 151.95.155.181
Entrées directes

Actions:

Mercredi 21 Juin - 14:08:24 (2 min 10s)
IP: 177.79.19.183
Entrées directes

Actions:

Mercredi 21 Juin - 09:20:37
IP: 99.240.77.120
Entrées directes

Maxthon 5.0, Plugins: pdf, flash, java, realplayer, windowsmedia

Actions:

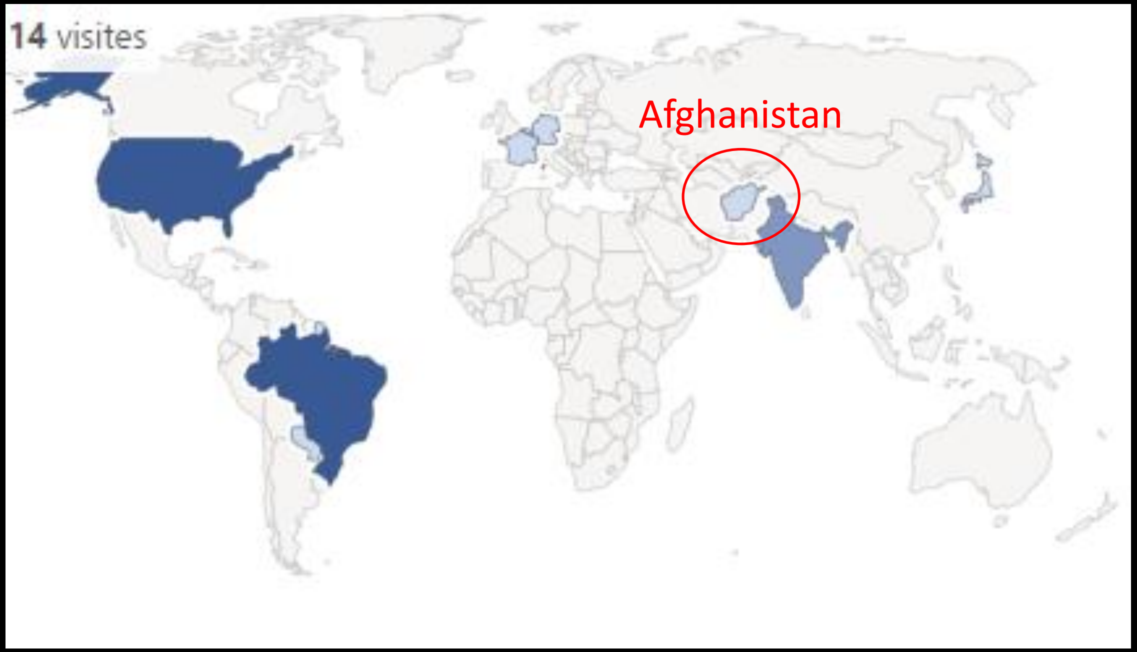
Mardi 20 Juin - 09:16:38
iOS IP: 89.162.11.107
Entrées directes

Actions:

Mardi 20 Juin - 08:18:14
IP: 70.209.136.2
Entrées directes

Actions:

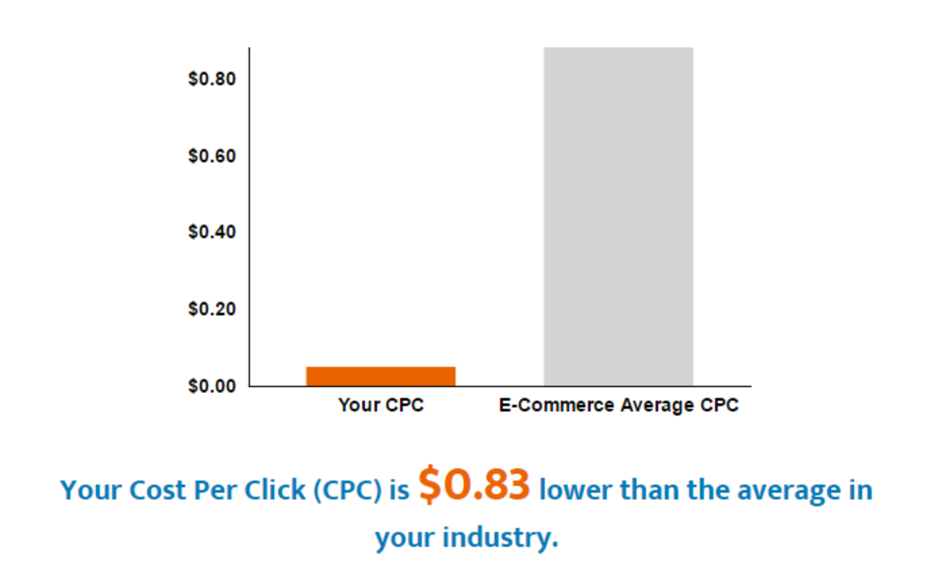
Mardi 20 Juin - 04:11:46
IP: 99.125.176.190
Entrées directes



```
AF;2017-05-31 13:00:22;[REDACTED];[REDACTED];;/;"Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36";
```

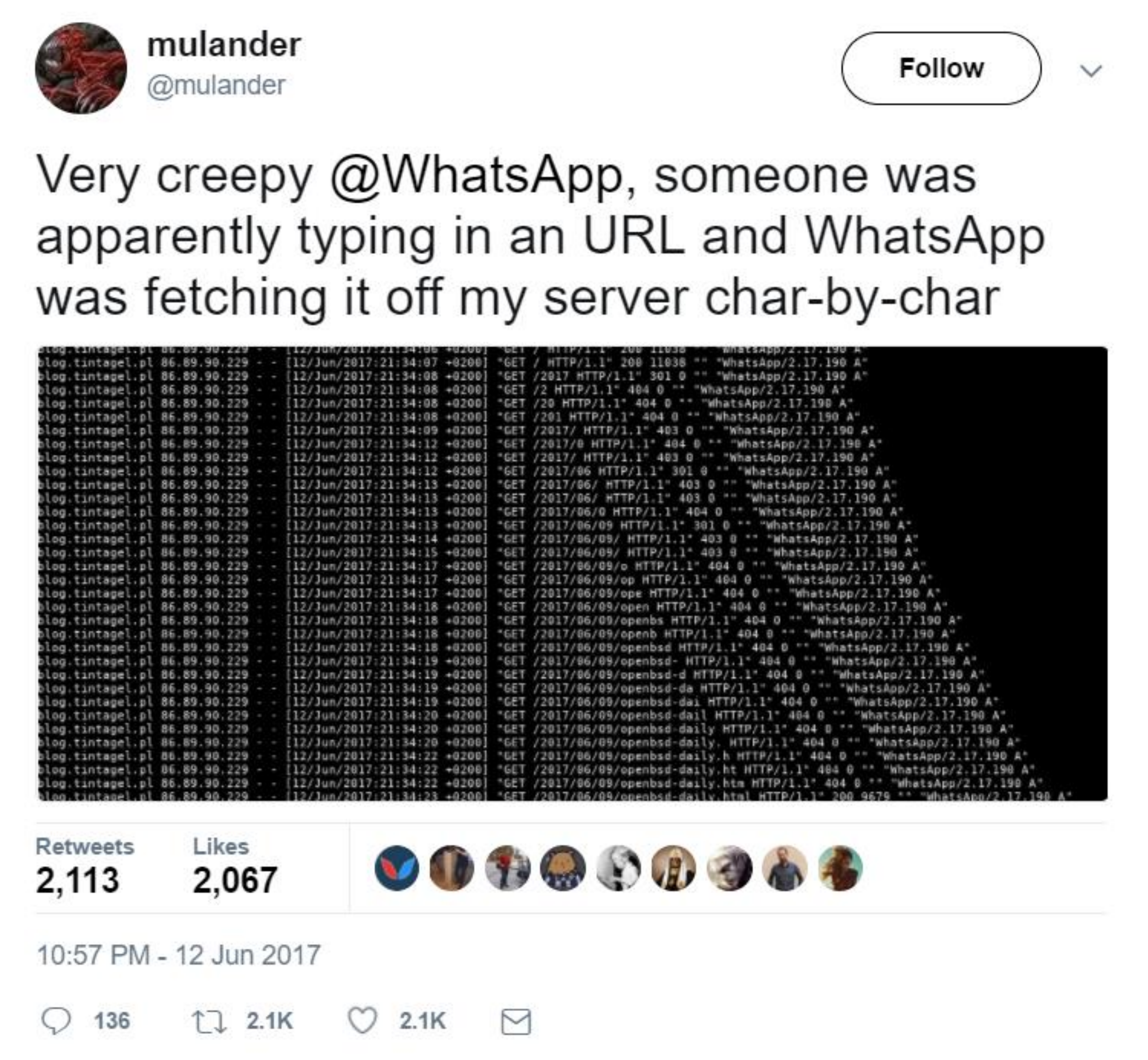
RoI

$0,05 par click/pwn



Your Cost Per Click (CPC) is $0.83 lower than the average in your industry.

WhatsApp leak



mulander
@mulander

Very creepy @WhatsApp, someone was apparently typing in an URL and WhatsApp was fetching it off my server char-by-char

```
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:06 +0200] "GET / HTTP/1.1" 200 11038 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:07 +0200] "GET / HTTP/1.1" 200 11038 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:08 +0200] "GET /2017 HTTP/1.1" 301 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:08 +0200] "GET /2 HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:08 +0200] "GET /20 HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:08 +0200] "GET /201 HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:09 +0200] "GET /2017/ HTTP/1.1" 403 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:12 +0200] "GET /2017/0 HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:12 +0200] "GET /2017/ HTTP/1.1" 403 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:12 +0200] "GET /2017/06 HTTP/1.1" 301 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:13 +0200] "GET /2017/06/ HTTP/1.1" 403 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:13 +0200] "GET /2017/06/ HTTP/1.1" 403 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:13 +0200] "GET /2017/06/0 HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:13 +0200] "GET /2017/06/09 HTTP/1.1" 301 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:14 +0200] "GET /2017/06/09/ HTTP/1.1" 403 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:15 +0200] "GET /2017/06/09/ HTTP/1.1" 403 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:17 +0200] "GET /2017/06/09/o HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:17 +0200] "GET /2017/06/09/op HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:17 +0200] "GET /2017/06/09/ope HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:18 +0200] "GET /2017/06/09/open HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:18 +0200] "GET /2017/06/09/openbs HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:18 +0200] "GET /2017/06/09/openb HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:18 +0200] "GET /2017/06/09/openbsd HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:19 +0200] "GET /2017/06/09/openbsd- HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:19 +0200] "GET /2017/06/09/openbsd-d HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:19 +0200] "GET /2017/06/09/openbsd-da HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:19 +0200] "GET /2017/06/09/openbsd-dai HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:20 +0200] "GET /2017/06/09/openbsd-dail HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:20 +0200] "GET /2017/06/09/openbsd-daily HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:20 +0200] "GET /2017/06/09/openbsd-daily. HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:22 +0200] "GET /2017/06/09/openbsd-daily.h HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:22 +0200] "GET /2017/06/09/openbsd-daily.ht HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:22 +0200] "GET /2017/06/09/openbsd-daily.htm HTTP/1.1" 404 0 "" "WhatsApp/2.17.190 A"
blog.tintagel.pl 86.89.90.229 - - [12/Jun/2017:21:34:23 +0200] "GET /2017/06/09/openbsd-daily.html HTTP/1.1" 200 9679 "" "WhatsApp/2.17.190 A"
```

Retweets 2,113
Likes 2,067

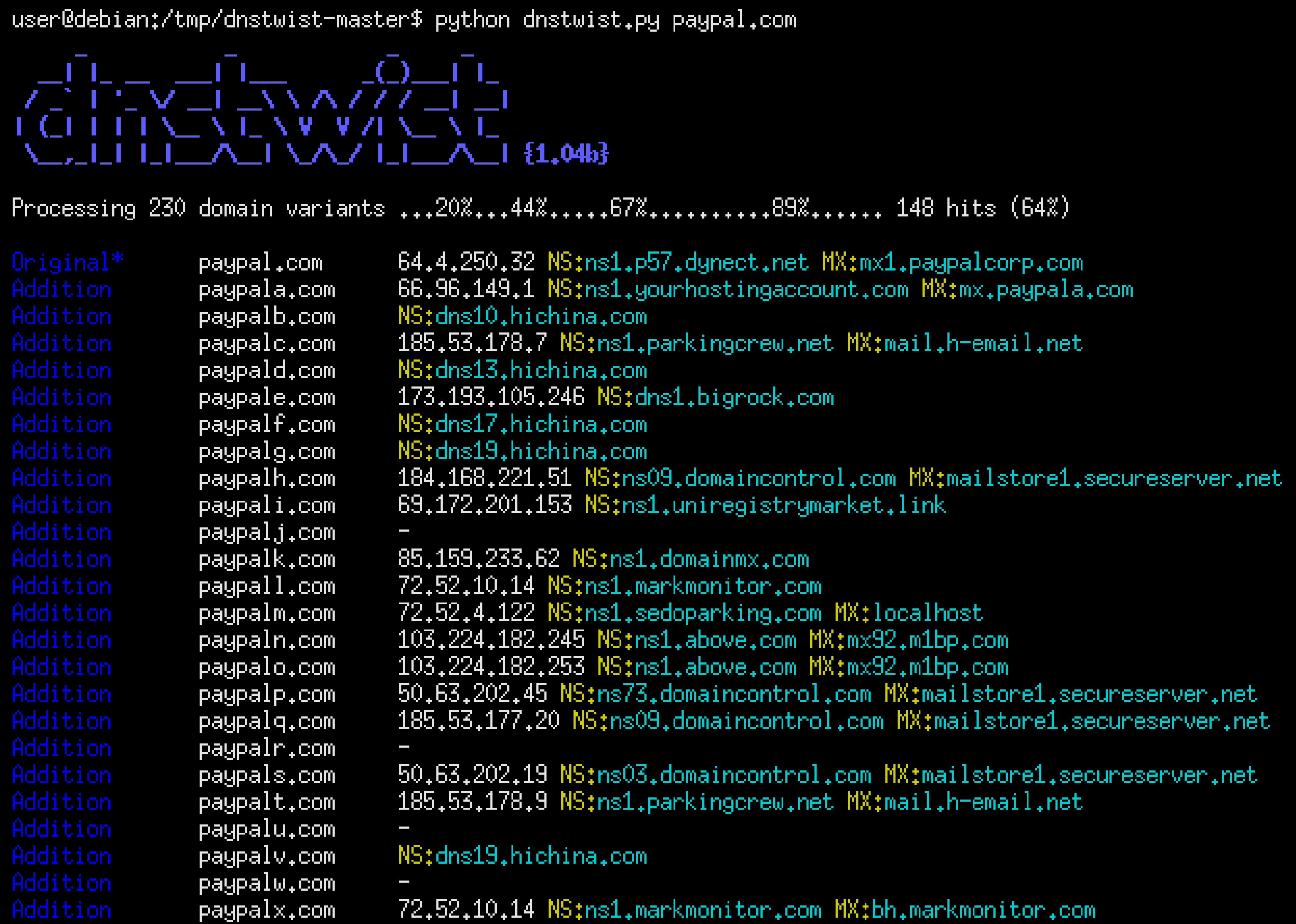
10:57 PM - 12 Jun 2017

136 2.1K 2.1K

In the wild? 😏

Permutation sur domaines avec *dnstwist*

Domain name permutation engine for detecting typo squatting, phishing and corporate espionage

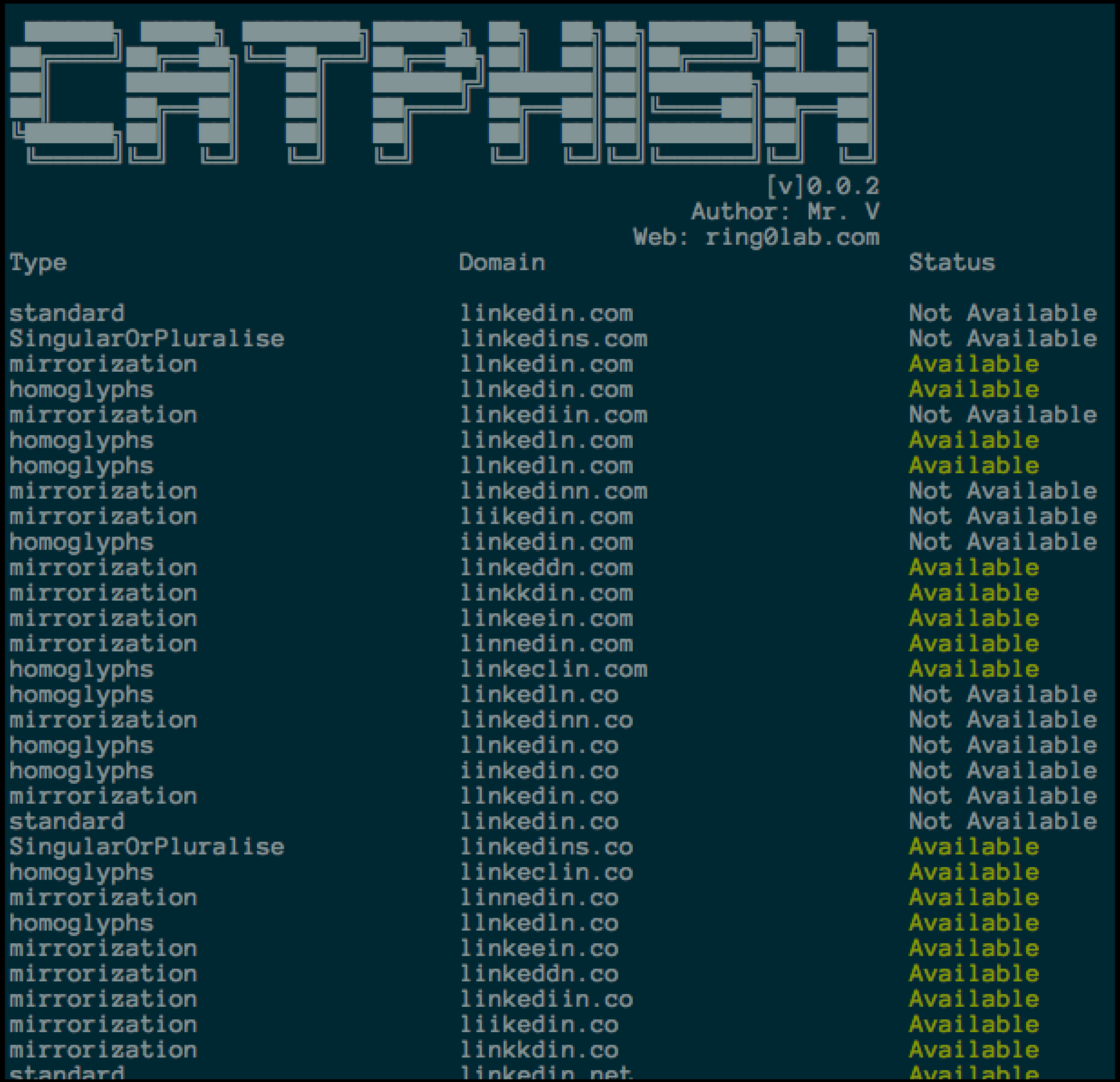


```
user@debian:/tmp/dnstwist-master$ python dnstwist.py paypal.com
     _           _            _     _
  __| |_ __  ___| |___      _(_)___| |_
 / _` | '_ \/ __| __\ \ /\ / / / __| __|
| (_| | | | \__ \ |_ \ V  V /| \__ \ |_
 \__,_|_| |_|___/\__| \_/\_/ |_|___/\__| {1.04b}

Processing 230 domain variants ...20%...44%.....67%..........89%...... 148 hits (64%)

Original*     paypal.com      64.4.250.32 NS:ns1.p57.dynect.net MX:mx1.paypalcorp.com
Addition      paypala.com     66.96.149.1 NS:ns1.yourhostingaccount.com MX:mx.paypala.com
Addition      paypalb.com     NS:dns10.hichina.com
Addition      paypalc.com     185.53.178.7 NS:ns1.parkingcrew.net MX:mail.h-email.net
Addition      paypald.com     NS:dns13.hichina.com
Addition      paypale.com     173.193.105.246 NS:dns1.bigrock.com
Addition      paypalf.com     NS:dns17.hichina.com
Addition      paypalg.com     NS:dns19.hichina.com
Addition      paypalh.com     184.168.221.51 NS:ns09.domaincontrol.com MX:mailstore1.secureserver.net
Addition      paypali.com     69.172.201.153 NS:ns1.uniregistrymarket.link
Addition      paypalj.com     -
Addition      paypalk.com     85.159.233.62 NS:ns1.domainmx.com
Addition      paypall.com     72.52.10.14 NS:ns1.markmonitor.com
Addition      paypalm.com     72.52.4.122 NS:ns1.sedoparking.com MX:localhost
Addition      paypaln.com     103.224.182.245 NS:ns1.above.com MX:mx92.m1bp.com
Addition      paypalo.com     103.224.182.253 NS:ns1.above.com MX:mx92.m1bp.com
Addition      paypalp.com     50.63.202.45 NS:ns73.domaincontrol.com MX:mailstore1.secureserver.net
Addition      paypalq.com     185.53.177.20 NS:ns09.domaincontrol.com MX:mailstore1.secureserver.net
Addition      paypalr.com     -
Addition      paypals.com     50.63.202.19 NS:ns03.domaincontrol.com MX:mailstore1.secureserver.net
Addition      paypalt.com     185.53.178.9 NS:ns1.parkingcrew.net MX:mail.h-email.net
Addition      paypalu.com     -
Addition      paypalv.com     NS:dns19.hichina.com
Addition      paypalw.com     -
Addition      paypalx.com     72.52.10.14 NS:ns1.markmonitor.com MX:bh.markmonitor.com
```

[REDACTED]

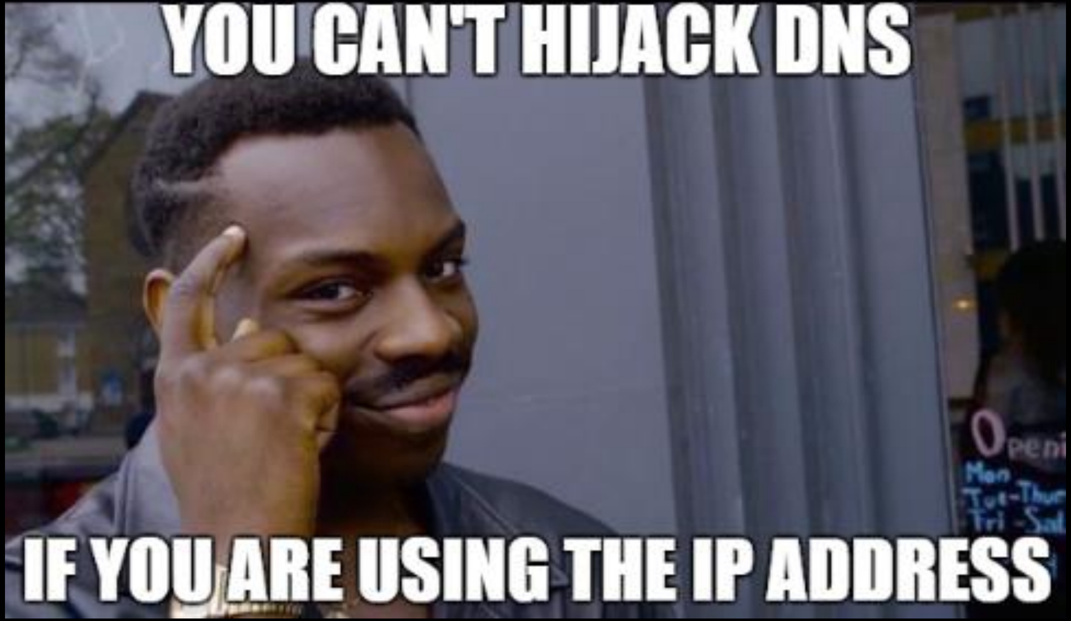
TLP GREEN data available upon request

Contact: x0rz@cypher.pw (PGP https://0day.rocks/public.pgp.asc)

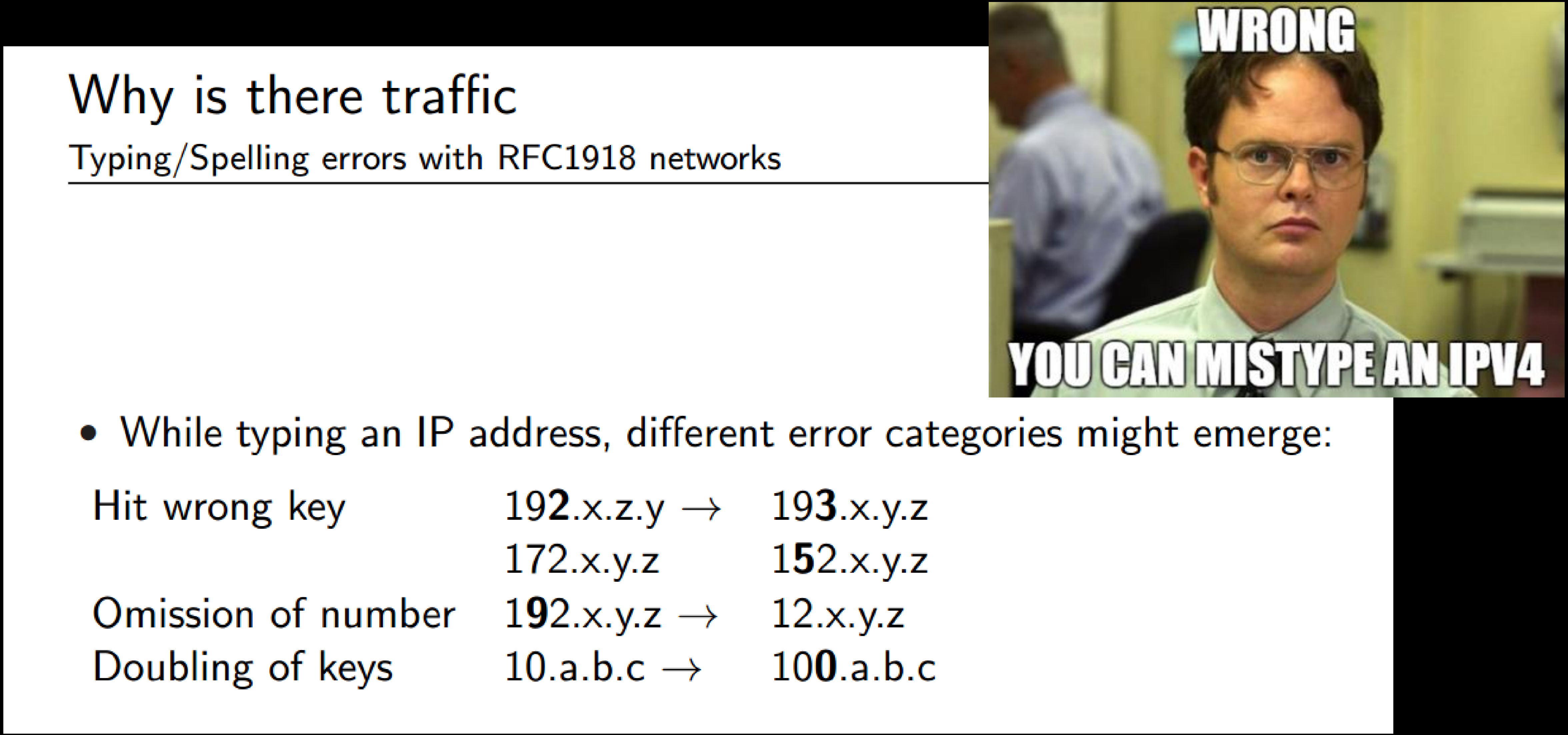


```
                                                    [v]0.0.2
                                               Author: Mr. V
                                           Web: ring0lab.com
Type                           Domain                         Status

standard                       linkedin.com                   Not Available
SingularOrPluralise            linkedins.com                  Not Available
mirrorization                  llnkedin.com                   Available
homoglyphs                     llnkedin.com                   Available
mirrorization                  linkediin.com                  Not Available
homoglyphs                     linkedln.com                   Available
homoglyphs                     llnkedln.com                   Available
mirrorization                  linkedinn.com                  Not Available
mirrorization                  liikedin.com                   Not Available
homoglyphs                     iinkedin.com                   Not Available
mirrorization                  linkeddn.com                   Available
mirrorization                  linkkdin.com                   Available
mirrorization                  linkeein.com                   Available
mirrorization                  linnedin.com                   Available
homoglyphs                     linkeclin.com                  Available
homoglyphs                     linkedln.co                    Not Available
mirrorization                  linkedinn.co                   Not Available
homoglyphs                     llnkedin.co                    Not Available
homoglyphs                     iinkedin.co                    Not Available
mirrorization                  llnkedin.co                    Not Available
standard                       linkedin.co                    Not Available
SingularOrPluralise            linkedins.co                   Available
homoglyphs                     linkeclin.co                   Available
mirrorization                  linnedin.co                    Available
homoglyphs                     llnkedln.co                    Available
mirrorization                  linkeein.co                    Available
mirrorization                  linkeddn.co                    Available
mirrorization                  linkediin.co                   Available
mirrorization                  liikedin.co                    Available
mirrorization                  linkkdin.co                    Available
standard                       linkedin.net                   Available
```

https://github.com/ring0lab/catphish



YOU CAN'T HIJACK DNS
IF YOU ARE USING THE IP ADDRESS
Open
Mon
Tue-Thur
Fri -Sat



WRONG
YOU CAN MISTYPE AN IPV4

Why is there traffic

Typing/Spelling errors with RFC1918 networks

- While typing an IP address, different error categories might emerge:

Hit wrong key	19**2**.x.z.y →	19**3**.x.y.z
	172.x.y.z	1**5**2.x.y.z
Omission of number	1**9**2.x.y.z →	12.x.y.z
Doubling of keys	10.a.b.c →	10**0**.a.b.c

Blackhole Networks: an Underestimated Source for Information Leaks, Alexandre Dulaunoy CIRCL - FIRST2017
https://www.circl.lu/assets/files/circl-blackhole-first2017.pdf