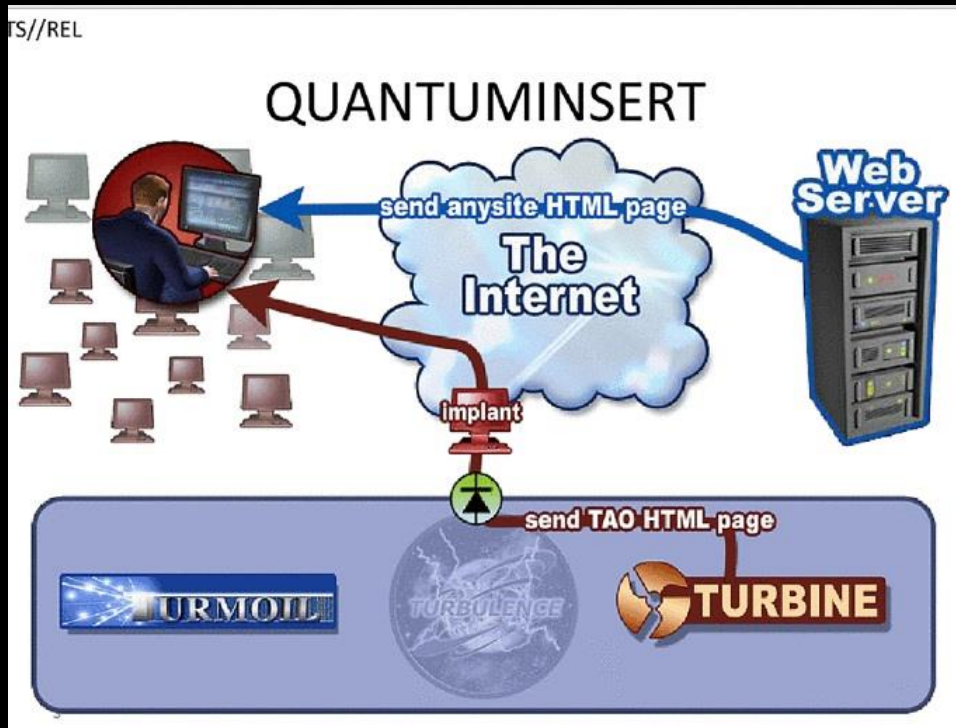


The poor man's QUANTUM

@x0rz

QUANTUM?

Man-on-the-side at Internet scale



- 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

Character omission

.com – .com (Columbia)
.com – .com (Cameroon)
.net – .net (Niger)

...

Other variant: bitsquatting (2011)

<http://dinaburg.org/bitsquatting.html>

Typical user in action



```
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
```

1) Get the most popular domain names

```
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) List all available for sale

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

```
1  # Usage: ./dns_check.py <list_of_domain_names.txt>
2  import dns.resolver
3  import requests
4  import re
5  import json
6  import sys
7
8  resolver = dns.resolver.Resolver()
9  resolver.timeout = 5
10 resolver.lifetime = 5
11
12 def is_available(domain):
13     try:
14         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'}
15         r = requests.get('https://njal.la/list/?search=' + domain, headers=hdr)
16         search = re.search('var results = \[(.*)\];', r.text)
17         if search:
18             domain = json.loads(search.group(1))
19             print(domain)
20             if domain['status'] == 'available':
21                 return True
22     except:
23         pass
24
25     return False
26
27 def main():
28     with open(sys.argv[1], 'r') as dotcom_names:
29         for name in dotcom_names:
30             name = name.strip()
31             try:
32                 resolver.query(name, 'NS')
33                 print("[+] %s is taken" % name)
34             except Exception as e:
35                 print("[+] %s might be available (%s)" % (name, e))
36                 if is_available(name):
37                     print("[!] \033[92m%s is available\033[0m" % name)
38                     with open('available_names.txt', 'a') as f:
39                         f.write("%s\n" % name)
40
41 if __name__ == '__main__':
42     main()
```

```
[+] sharepoint.co is taken
[+] 163.co is taken
[+] foxnews.co is taken
[+] feedly.co is taken
[+] iqqiyi.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-success', 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'label-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

#585 videoyoum7.com

#614 beytoote.com

#642 namnak.com

#735 telewebion.com


#827 sputniknews.com

#871 scribol.com

#906 stockstar.com

#920 askubuntu.com

3) Set up your waterholing server

- Redirect all domains and sub-domains to your server IP address
- Setup a redirect page + JS payload (be evil, or not)
- ...
- Wait for incoming connections 

HTML redirect (meta refresh)



```
<html>
<head>
<title>Loading...</title>
<meta http-equiv="refresh" content="1; url=http://sputniknews.com/" />
<!-- FOXACID SPLOITZ GOES BELOW -->
<script type="text/javascript">
  var _paq = _paq || [];
  _paq.push(['trackPageView']);
  _paq.push(['enableLinkTracking']);
  (function() {
    var u="//185.10.68.99/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></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);
?>
```

JavaScript
code
(ExploitKit
or
Piwik)

PHP logs

IS IT WORKING?!?



2017-05-20 07:19:34;93.20 177;sputniknews.co;;/"Mozilla/5.0 (compatible; MSIE 9.0; windows NT 6.1; WOW64; Trident/5.0)";""

2017-05-20 08:22:55;70.39 94;sputniknews.co;;/"Mozilla/5.0 (compatible; MSIE 9.0; windows NT 6.1; WOW64; Trident/5.0)";""

2017-05-20 09:08:19;5.234 namnak.co;;/"Mozilla/5.0 (Linux; Android 4.2.2; HUAWEI Y320-U10 Build/HUAWEIY320-U10) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36";""

2017-05-20 09:23:23;77.10 94;www.telewebion.co;;/"Mozilla/5.0 (windows NT 6.3; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36";""

2017-05-20 09:51:10;213.2 253;de.sputniknews.co;;/"Mozilla/5.0 (iPhone; CPU iPhone OS 7_1_1 like Mac OS X) AppleWebKit/537.51.2 (KHTML, like Gecko) Version/11.0 Mobile/15B202.5 Safari/604.1";""

2017-05-20 10:42:47;202.4 01;askubuntu.co;;/"Mozilla/5.0 (windows NT 10.0; wow64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36";""

2017-05-20 11:16:16;178.1 210;de.sputniknews.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0";"_pk_id.5.ecd1=dcf6b4ab-494256796."

2017-05-20 11:46:47;64.40 56;namnak.co;;/"Mozilla/5.0 (Linux; Android 6.0; LG-K430 Build/MRA58K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Mobile Safari/537.36";""

2017-05-20 12:53:54;54.92 36;askubuntu.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0";""

2017-05-20 12:54:07;54.82 0;askubuntu.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0";""

2017-05-20 13:13:23;2.50. sputniknews.co;;/"Mozilla/5.0 (windows NT 6.1; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36";""

2017-05-20 13:35:02;54.92 36;www.askubuntu.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0";""

2017-05-20 13:37:28;54.82 0;www.askubuntu.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0";""

2017-05-20 13:59:50;151.2 138;telewebion.co;;/"Mozilla/5.0 (Linux; Android 4.3; en-us; SAMSUNG GT-I9300I Build/JLS36C) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Mobile Safari/537.36";""

2017-05-20 14:57:12;88.19 stockstar.co;;/"Mozilla/5.0 (compatible; MSIE 10.0; windows NT 6.2; WOW64; Trident/6.0; .NET4.0E; .NET4.0C; .NET CLR 3.5.30729; CMNTDFJS)";""

2017-05-20 15:00:12;144.7 51;stockstar.co;;/"Mozilla/5.0 (compatible; MSIE 10.0; windows NT 6.1; WOW64; Trident/6.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)";""

2017-05-20 15:14:40;199.2 42;stockstar.co;http://pizza-tycoon.com/;"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36";""

2017-05-20 16:50:27;98.24 190;sputniknews.co;;/"Mozilla/5.0 (windows NT 5.1; rv:20.0) Gecko/20100101 Firefox/20.0";""

2017-05-20 18:06:18;89.16 48;mundo.sputniknews.co;;/"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:53.0) Gecko/20100101 Firefox/53.0";""

2017-05-20 19:07:08;5.215 5;beytoote.co;;/"Mozilla/5.0 (windows NT 6.1; win64; x64; rv:53.0) Gecko/20100101 Firefox/53.0";""

2017-05-20 20:37:16;197.2 25;www.sputniknews.co;;/"Mozilla/5.0 (windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.152 Safari/537.36";""

2017-05-20 21:37:58;83.71 5;tr.sputniknews.co;http://tr.sputniknews.co/;"Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.9.2.8) Gecko/20100721 Firefox/3.0.1";""

2017-05-21 01:36:43;38.10 5;www.stockstar.co;;/"Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2)";""

2017-05-21 02:35:08;211.1 98;kr.sputniknews.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko";""

2017-05-21 08:27:20;173.2 155;sputniknews.co;;/"Mozilla/5.0 (windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36";""

2017-05-21 08:31:25;52.91 5;videoyoum7.co;;/"Go-http-client/1.1";""

2017-05-21 08:49:51;91.25 150;telewebion.co;;/"Mozilla/5.0 (windows NT 6.3; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36";""

2017-05-21 10:16:29;174.1 164;sputniknews.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0";""

2017-05-21 13:32:05;101.8 58;www.stockstar.co;;/"Mozilla/5.0 (windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36";""

2017-05-21 13:58:30;217.7 52;videoyoum7.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36";""

2017-05-21 13:58:30;217.7 52;videoyoum7.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36";""

2017-05-21 14:12:54;46.22 197;askubuntu.co;;/"Mozilla/5.0 (windows NT 6.3; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36";""

2017-05-21 14:18:56;174.1 164;www.sputniknews.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0";""

2017-05-21 14:23:14;137.7 241;sputniknews.co;;/"Mozilla/5.0 (windows NT 6.1; rv:45.0) Gecko/20100101 Firefox/45.0";""

2017-05-21 14:35:19;211.1 98;kr.sputniknews.co;;/"Mozilla/5.0 (windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko";""

2017-05-21 20:42:16;220.1 60;quote.stockstar.co;;/"Mozilla/5.0 (windows; U; MSIE 6.0; windows NT 5.1; SV1; .NET CLR 2.0.50727; BIDUBrowser 8.7)";""

2017-05-21 21:20:44;67.14 95;sputniknews.co;;/"Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:53.0) Gecko/20100101 Firefox/53.0";""

2017-05-21 21:28:21;220.1 109;www.stockstar.co;;/"Mozilla/5.0 (windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36";""

2017-05-21 21:29:46;213.2 5;sputniknews.co;;/"Mozilla/5.0 (compatible; MSIE 9.0; windows NT 6.1; WOW64; Trident/5.0)";""

2017-05-22 04:21:31;8.29. sputniknews.co;;/"Feedly/1.0 (+http://www.feedly.com/fetcher.html; like FeedFetcher-Google)";""

2017-05-22 06:45:07;45.12 4;finance.stockstar.co;;/index.php?m=member&c=index&a=register&siteid=1;"User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET4.0C; ms-office)";""

2017-05-22 07:14:38;218.6 145;bank.stockstar.co;;/"Mozilla/4.0 (compatible; MSIE 7.0; windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET4.0C; ms-office)";""

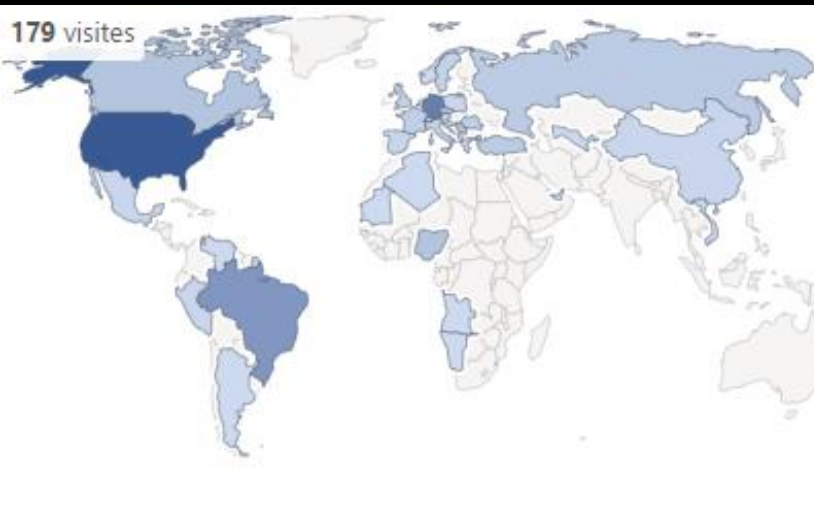
2017-05-22 07:15:00;218.6 145;bank.stockstar.co;;/"Mozilla/5.0 (windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36";""

2017-05-22 07:15:39;106.1 119;bank.stockstar.co;http://bank.stockstar.co/;"Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 2.0.50727)";""

2017-05-22 07:15:51;220.1 194;bank.stockstar.co;;/"Mozilla/5.0 (Linux; U; Android 5.0.2; zh-CN; Redmi Note 3 Build/LRX22G) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Mobile Safari/537.36";""

Statistics

- **5430** log entries over **40 days**
 - **1764** (~40/day) without bots/crawlers
 - Only 392 unique visitors that load my Piwik JS code
 - Ad blockers?
 - 80 countries



sputniknews.co



stockstar.co



telewebion.co

Statistics

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

The screenshot displays a list of visitor logs from a web analytics tool. Each log entry includes a date and time, a country flag, a browser icon, an operating system icon, an IP address, and the text 'Entrées directes'. Below each entry is an 'Actions' section with folder icons. The third entry from the top is highlighted with a red circle around the 'Plugins' field, which lists 'Maxthon 5.0, Plugins: pc, flash, java, realplayer, windowsmedia'. A red handwritten note 'Lol Java + Flash' with a shocked face emoji is placed next to this entry. The interface also shows a sidebar on the right with a search bar and a 'Récap' (Summary) section.

Mercredi 21 Juin - 16:21:49
🇮🇹 📱 iOS IP: 151.95.
Entrées directes
Actions: 📁

Mercredi 21 Juin - 14:08:24 (2 min 10s)
🇧🇷 🌐 🖥️ IP: 177.79.
Entrées directes
Actions: 📁 📁

Mercredi 21 Juin - 09:20:37
🇨🇦 🌐 🖥️ IP: 99.240.
Entrées directes
Maxthon 5.0, Plugins: pc, flash, java, realplayer, windowsmedia
Actions: 📁

Mardi 20 Juin - 09:16:38
🇩🇰 📱 iOS IP: 89.162.
Entrées directes
Actions: 📁

Mardi 20 Juin - 08:18:14
🇺🇸 🌐 🖥️ IP: 70.209.
Entrées directes
Actions: 📁

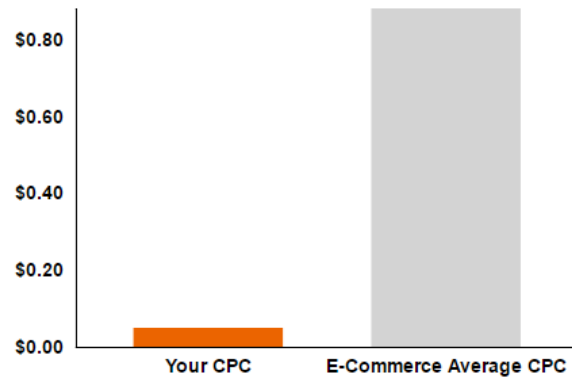
Mardi 20 Juin - 04:11:46
🇺🇸 🌐 🖥️ IP: 99.125.
Entrées directes

0
Prem
Récap
recherch

Rol



\$0,05 click/pwn



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



WhatsApp leak

```

2017-05-11 16:35:14;151.7
2017-05-11 16:44:23;91.2
2017-05-11 16:48:18;93.1
2017-05-11 18:24:55;5.22
2017-05-11 18:35:29;46.1
2017-05-11 18:47:41;37.6
2017-05-11 20:35:04;151.7
2017-05-11 21:44:12;5.22
2017-05-12 03:57:15;5.11
2017-05-12 05:32:41;5.12
2017-05-12 05:38:56;5.21
2017-05-12 06:03:26;2.18
2017-05-12 06:43:32;5.12
2017-05-12 07:00:32;5.11
2017-05-12 08:44:51;197.1
2017-05-12 10:00:30;95.6
2017-05-12 11:07:49;2.18
2017-05-12 14:03:18;160.1
2017-05-12 14:38:18;178.1
2017-05-12 14:42:23;5.21
2017-05-12 18:37:53;83.1
2017-05-12 19:35:31;181.1
2017-05-13 10:45:52;93.1
2017-05-13 12:27:32;5.12
2017-05-13 14:54:11;5.12
2017-05-13 16:56:32;5.21
2017-05-13 21:50:43;151.7
2017-05-14 01:38:40;5.12
2017-05-14 02:28:54;5.11
2017-05-14 05:34:41;5.11
2017-05-14 10:13:15;151.7
2017-05-14 11:01:25;5.21
2017-05-14 11:24:59;5.21
2017-05-14 11:42:02;94.1
2017-05-14 11:44:12;5.12
2017-05-14 12:03:14;188.7
2017-05-14 12:39:50;89.3
2017-05-14 13:39:19;5.12
2017-05-14 13:55:20;212.7
2017-05-14 15:58:55;188.7
2017-05-14 16:31:08;193.7
2017-05-14 17:43:00;5.21
2017-05-14 18:55:32;5.12
2017-05-14 20:17:32;178.1
2017-05-14 22:05:59;217.6
2017-05-14 22:25:17;5.12
2017-05-15 02:40:07;158.1
2017-05-15 03:07:47;5.21
2017-05-15 05:09:21;5.12
2017-05-15 06:45:17;5.21
2017-05-15 07:54:35;89.3
2017-05-15 08:24:32;46.2
2017-05-15 08:31:48;5.11
2017-05-15 09:06:53;5.21
2017-05-15 09:59:28;5.12
19;www.beytoote.co;/"whatsApp/2.17.14 A";""
01;www.telewebion.co;/"whatsApp/2.16.396 A";""
17;www.beytoote.co;/"whatsApp/2.17.146 A";""
www.beytoote.co;/"whatsApp/2.17.79 A";""
www.beytoote.co;/"whatsApp/2.17.14 A";""
www.beytoote.co;/"whatsApp/2.17.146 A";""
L27;www.beytoote.co;/"whatsApp/2.17.146 A";""
www.beytoote.co;/"whatsApp/2.17.174 A";""
3;www.beytoote.co;/"whatsApp/2.17.24 A";""
www.beytoote.co;/"whatsApp/2.16.396 A";""
www.telewebion.co;/"whatsApp/2.17.107 A";""
www.beytoote.co;/"whatsApp/2.17.24 A";""
namnak.co;/"whatsApp/2.17.146 A";""
www.beytoote.co;/"whatsApp/2.16.396 A";""
L02;files.namnak.co;/"whatsApp/2.16.396 A";""
L;www.beytoote.co;/"whatsApp/2.16.396 A";""
www.telewebion.co;/"whatsApp/2.17.107 A";""
217;www.beytoote.co;/"whatsApp/2.17.107 A";""
L7;www.beytoote.co;/"whatsApp/2.17.107 A";""
9;files.namnak.co;/"whatsApp/2.16.392 A";""
3;www.telewebion.co;/"whatsApp/2.16.396 A";""
9;www.mundo.sputniknews.co;/"whatsApp/2.17.146 A";""
5;namnak.co;/"whatsApp/2.17.174 A";""
5;files.namnak.co;/"whatsApp/2.17.107 A";""
www.telewebion.co;/"whatsApp/2.17.79 A";""
namnak.co;/"whatsApp/2.17.146 A";""
9;namnak.co;/"whatsApp/2.17.79 A";""
9;www.beytoote.co;/"whatsApp/2.17.127 A";""
5;namnak.co;/"whatsApp/2.17.107 A";""
www.telewebion.co;/"whatsApp/2.17.79 A";""
11;www.telewebion.co;/"whatsApp/2.17.24 A";""
www.beytoote.co;/"whatsApp/2.17.107 A";""
www.telewebion.co;/"whatsApp/2.17.146 A";""
37;www.telewebion.co;/"whatsApp/2.17.24 A";""
17;www.beytoote.co;/"whatsApp/2.17.146 A";""
www.telewebion.co;/"whatsApp/2.17.24 A";""
www.telewebion.co;/"whatsApp/2.17.146 A";""
www.beytoote.co;/"whatsApp/2.17.146 A";""
5;www.telewebion.co;/"whatsApp/2.17.190 A";""
242;www.telewebion.co;/"whatsApp/2.17.146 A";""
L65;www.telewebion.co;/"whatsApp/2.17.146 A";""
7;www.beytoote.co;/"whatsApp/2.17.107 A";""
L;www.beytoote.co;/"whatsApp/2.17.107 A";""
L34;www.telewebion.co;/"whatsApp/2.17.79 A";""
26;namnak.co;/"whatsApp/2.17.146 A";""
1;www.beytoote.co;/"whatsApp/2.17.146 A";""
37;files.namnak.co;/"whatsApp/2.17.79 A";""
9;www.telewebion.co;/"whatsApp/2.17.190 A";""
namnak.co;/"whatsApp/2.16.396 A";""
namnak.co;/"whatsApp/2.17.144 A";""
5;www.beytoote.co;/"whatsApp/2.17.79 A";""
3;www.telewebion.co;/"whatsApp/2.16.396 A";""
files.namnak.co;/"whatsApp/2.17.24 A";""
www.beytoote.co;/"whatsApp/2.17.191 A";""
www.beytoote.co;/"whatsApp/2.17.107 A";""

```



mulander

@mulander

Follow

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

[illegible]

Retweets

2,113

Likes

2.067



10:57 PM - 12 Jun 2017



136



2.1K



2.1K



In the wild? 🤔

Detection using *dnstwist*

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

```
user@debian:/tmp/dnstwist-master$ python dnstwist.py paypal.com
```

```
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	paypal.a.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	paypal.i.com	69.172.201.153 NS:ns1.uniregistrymarket.link
Addition	paypalj.com	-
Addition	paypal.k.com	85.159.233.62 NS:ns1.domainmx.com
Addition	paypall.com	72.52.10.14 NS:ns1.markmonitor.com
Addition	paypal.m.com	72.52.4.122 NS:ns1.sedoparking.com MX:localhost
Addition	paypal.n.com	103.224.182.245 NS:ns1.above.com MX:mx92.m1bp.com
Addition	paypal.o.com	103.224.182.253 NS:ns1.above.com MX:mx92.m1bp.com
Addition	paypal.p.com	50.63.202.45 NS:ns73.domaincontrol.com MX:mailstore1.secureserver.net
Addition	paypal.q.com	185.53.177.20 NS:ns09.domaincontrol.com MX:mailstore1.secureserver.net
Addition	paypalr.com	-
Addition	paypal.s.com	50.63.202.19 NS:ns03.domaincontrol.com MX:mailstore1.secureserver.net
Addition	paypal.t.com	185.53.178.9 NS:ns1.parkingcrew.net MX:mail.h-email.net
Addition	paypal.u.com	-
Addition	paypal.v.com	NS:dns19.hichina.com
Addition	paypal.w.com	-
Addition	paypal.x.com	72.52.10.14 NS:ns1.markmonitor.com MX:bh.markmonitor.com

Omission	wpengine.com	192.64.119.157 NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Omission	wpegine.com	184.154.247.81 NS:ns43.domaincontrol.com MX:mailstore1.secureserver.net
Omission	wengine.com	89.31.143.16 NS:ns.udag.de MX:mx00.udag.de
Omission	wpengin.com	185.53.178.7 NS:ns1.parkingcrew.net MX:mail.h-email.net
Omission	pengine.com	66.96.163.196 NS:ns1.mydomain.com MX:mx.pengine.com
Omission	wpengne.com	192.64.119.69 NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Omission	wpengie.com	192.64.119.172 NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Omission	wpenine.com	192.64.119.110 NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Repetition	wpenngine.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wpengiine.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wpenginne.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wpeengine.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wwpengine.com	-
Repetition	wpengnine.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wppengine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpeng8ne.com	-
Replacement	wpengune.com	185.53.178.8 NS:ns1.parkingcrew.net MX:mail.h-email.net
Replacement	wpsengine.com	-
Replacement	wpenhine.com	-
Replacement	woengine.com	185.53.178.8 NS:ns1.parkingcrew.net MX:mail.h-email.net
Replacement	wpentine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	3pengine.com	50.63.202.45 NS:ns19.domaincontrol.com MX:mailstore1.secureserver.net
Replacement	xpengine.com	192.249.124.144 NS:ns1.webhostinghub.com MX:xpengine.com
Replacement	wpehgine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpzengine.com	-
Replacement	wpengibe.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpenginw.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpenginr.com	103.224.212.242 NS:ns1.above.com MX:mx92.m1bp.com
Replacement	wpengins.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpengihe.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wlengine.com	-
Replacement	wpengin3.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpenbine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	apengine.com	52.204.129.22 NS:ns1.namebrightdns.com
Replacement	wprngine.com	213.247.47.190 NS:ns1.expiereddnsmanager.com MX:mx7.wprngine.com
Replacement	epengine.com	69.83.31.185 NS:ns1.bluehost.com MX:mail.epengine.com
Replacement	wp4ngine.com	-
Replacement	2pengine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpeng9ne.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpengjne.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wp3ngine.com	-
Replacement	wmengine.com	-
Replacement	wpenvine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpebgine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpenginz.com	-
Replacement	wpengone.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpengin4.com	-
Replacement	wpengine.com	-

ns1.storeland.ru sounds shady as fuck



Omission	wpengine.com	192.64.119.157 NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Omission	wpegine.com	184.154.247.81 NS:ns43.domaincontrol.com MX:mailstore1.secureserver.net
Omission	wengine.com	89.31.143.16 NS:ns.udag.de MX:mx00.udag.de
Omission	wpengin.com	185.53.178.7 NS:ns1.parkingcrew.net MX:mail.h-email.net
Omission	pengine.com	66.96.163.196 NS:ns1.mydomain.com MX:mx.pengine.com
Omission	wpengne.com	192.64.119.69 NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Omission	wpengie.com	192.64.119.172 NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Omission	wpenine.com	192.64.119.110 NS:dns1.registrar-servers.com MX:eforward1.registrar-servers.com
Repetition	wpenngine.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wpengiine.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wpenginne.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wpeengine.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wwpengine.com	-
Repetition	wpengine.com	136.243.255.87 NS:ns1.storeland.ru
Repetition	wppengine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpeng8ne.com	-
Replacement	wpengune.com	185.53.178.8 NS:ns1.parkingcrew.net MX:mail.h-email.net
Replacement	wpsengine.com	-
Replacement	wpenhine.com	-
Replacement	woengine.com	185.53.178.8 NS:ns1.parkingcrew.net MX:mail.h-email.net
Replacement	wpentine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	3pengine.com	50.63.202.45 NS:ns19.domaincontrol.com MX:mailstore1.secureserver.net
Replacement	xpengine.com	192.249.124.144 NS:ns1.webhostinghub.com MX:xpengine.com
Replacement	wpehngine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpzngine.com	-
Replacement	wpengibe.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpenginw.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpenginr.com	103.224.212.242 NS:ns1.above.com MX:mx92.m1bp.com
Replacement	wpengins.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpengihe.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wlengine.com	-
Replacement	wpengin3.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpenbine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	apengine.com	52.204.129.22 NS:ns1.namebrightdns.com
Replacement	wprngine.com	213.247.47.190 NS:ns1.expiereddnsmanager.com MX:mx7.wprngine.com
Replacement	epengine.com	69.83.31.185 NS:ns1.bluehost.com MX:mail.epengine.com
Replacement	wp4ngine.com	-
Replacement	2pengine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpeng9ne.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpengjne.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wp3ngine.com	-
Replacement	wmengine.com	-
Replacement	wpenvine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpebgine.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpenginz.com	-
Replacement	wpengone.com	136.243.255.87 NS:ns1.storeland.ru
Replacement	wpengin4.com	-
Replacement	wpengine.com	-

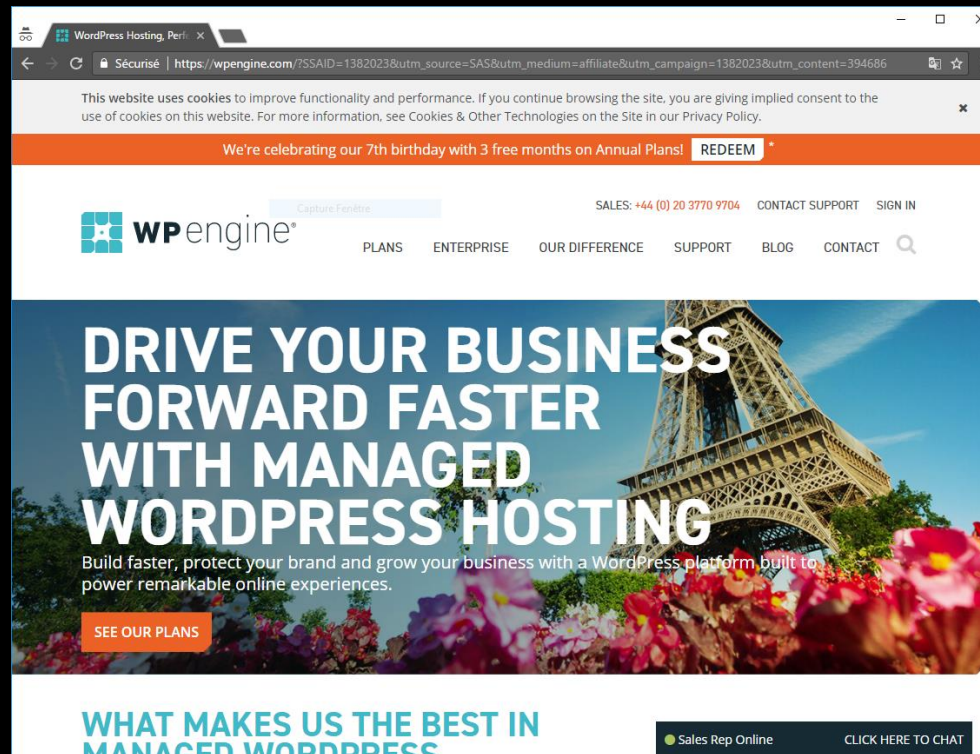
ns1.storeland.ru sounds shady as fuck



6,389 domains using this nameserver

In the wild

vpengine.com -> wpengine.com



Legit domain

What's going on?

Typosquatted *wpengine.com*

```
user@debian:~$ curl -sIL vpengine.com
HTTP/1.1 302 Moved Temporarily
Server: nginx/1.4.6 (Ubuntu)
Date: Thu, 18 May 2017 12:21:44 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.5.9-1ubuntu4.5
Location: http://vpengine.com/?utm_source=wpengine.com&utm_medium=vpengine.com&utm_campaign=vpengine.com&lid=fd8fe9f5b4a38ee4&lss=73c22
```

```
HTTP/1.1 302 Moved Temporarily
Server: nginx/1.4.6 (Ubuntu)
Date: Thu, 18 May 2017 12:21:44 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.5.9-1ubuntu4.5
Location: http://136.243.255.90/r50b3a
```

🇩🇪 AS24940 Hetzner Online GmbH

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Thu, 18 May 2017 12:21:44 GMT
Content-Type: text/html
Content-Length: 363
Last-Modified: Wed, 17 May 2017 14:09:19 GMT
Connection: keep-alive
ETag: "591c598f-16b"
Accept-Ranges: bytes
```



URL:	http://vpengine.com/	
Ratio de détection :	0 / 64	~_(ツ)_/~
Date d'analyse :	2017-05-18 13:41:20 UTC (il y a 0 minute)	

🇺🇸 Cloudflare

```
<script>setTimeout("window.location='http://www.shareasale.com/r.cfm?B=394686&U=1382023&M=41388&urllink=';", 1);</script><noscript><meta http-equiv="refresh" content="1;url=http://www.shareasale.com/r.cfm?B=394686&U=1382023&M=41388&urllink=" /><a href="http://www.shareasale.com/r.cfm?B=394686&U=1382023&M=41388&urllink=">Click here</a> for redirection</noscript>
```

Gray Affiliate Marketing Network

The screenshot shows the ShareASale website, which is part of the Awin network. The header includes the ShareASale logo, navigation links for 'AFFILIATE LOGIN' and 'MERCHANT LOGIN', and a section for 'WHAT IS AFFILIATE MARKETING?' with links to 'MERCHANTS JOIN HERE' and 'AFFILIATE SIGN UP'. Below the header is a category bar with links to 'POPULAR MERCHANTS', 'HOME & GARDEN MERCHANTS', 'FASHION MERCHANTS', 'GREEN MERCHANTS', 'BUSINESS MERCHANTS', and 'MORE MERCHANTS'. The main content area features a 'FEATURED MERCHANT' section for 'The RealReal', described as 'AUTHENTICATED LUXURY CONSIGNMENT', with a '5% Commission | 7 Day Cookie | \$50 New Customer Bonus'. Below this are two call-to-action buttons: 'I WANT TO PROMOTE THIS MERCHANT ON MY WEBSITE' and 'I WANT TO BE ONE OF THESE MERCHANTS'. The footer includes the text 'Welcome to the ShareASale Performance Marketing Network' and 'A LEADING PROVIDER OF PERFORMANCE MARKETING SOLUTIONS FOR THE PAST 17 YEARS'.



https://wpengine.com/?SSAID=1382023&utm_source=SAS&utm_medium=affiliate&utm_campaign=1382023&utm_content=394686

wpebgine.com	2017-03-28	intreserver.net	2017-05-15	graphicriveer.net	2017-05-15
wpeengine.com	2017-05-16	intrserver.net	2017-03-21	graphicriverr.net	2017-05-15
wpegnine.com	2017-03-28	intterserver.net	2017-05-15	graphicrivers.net	2017-05-15
wpehgine.com	2017-03-28	iterserver.net	2017-05-15	graphicrivir.net	2017-05-15
wpejgine.com	2017-05-11	itmeweb.ru	2017-05-16	graphicrivre.net	2017-05-15
wpenfine.com	2017-05-16	itnerserver.net	2017-05-15	graphicrivver.net	2017-05-15
wpengayne.com	2017-03-28	niterserver.net	2017-05-15	graphicrivyr.net	2017-05-15
wpenggine.com	2017-05-16	nterserver.net	2017-05-15	graphicriwer.net	2017-05-15
wpengibe.com	2017-03-28	perfectmoney.date	2017-04-09	graphicrriver.net	2017-05-15
wpengihe.com	2017-03-28	perfectmoney.loan	2017-04-09	graphicrvier.net	2017-05-15
wpengije.com	2017-03-28	perfectmoney.online	2017-04-09	graphicryver.net	2017-05-15
wpengijne.com	2017-03-28	perfectmoney.party	2017-04-09	graphiicriver.net	2017-05-15
wpengin3.com	2017-03-28	perfectmoney.press	2017-04-09	graphikriver.net	2017-05-15
wpengind.com	2017-03-28	perfectmoney.racing	2017-04-09	graphiqriver.net	2017-05-15
wpenginee.com	2017-05-16	perfectmoney.review	2017-04-09	graphirciver.net	2017-05-15
wpenginne.com	2017-05-16	perfectmoney.site	2017-04-09	graphjicriver.net	2017-05-15
wpengins.com	2017-05-11	perfectmoney.website	2017-04-09	graphuicriver.net	2017-05-15
wpenginw.com	2017-05-16	pjurevpn.com	2017-05-11	graphycriver.net	2017-05-15
wpenginy.com	2017-05-06	poorevpn.com	2017-05-16	grapihcriver.net	2017-05-15
wpengkne.com	2017-03-28	ppurevpn.com	2017-05-16	grapphicriver.net	2017-05-15
wpengnie.com	2017-03-28	pqrevpn.com	2017-05-16	grpahicriver.net	2017-05-15
wpengone.com	2017-05-16	puervpn.com	2017-05-16	grraphicriver.net	2017-05-15
wpengyne.com	2017-03-28	pureevpn.com	2017-05-16	...	
wpenngine.com	2017-05-16	purevpnn.com	2017-05-16		
wpentine.com	2017-03-28	purevppn.com	2017-05-16		
wppengine.com	2017-05-16	purevvpn.com	2017-05-16		
...		...			

CATPHISH

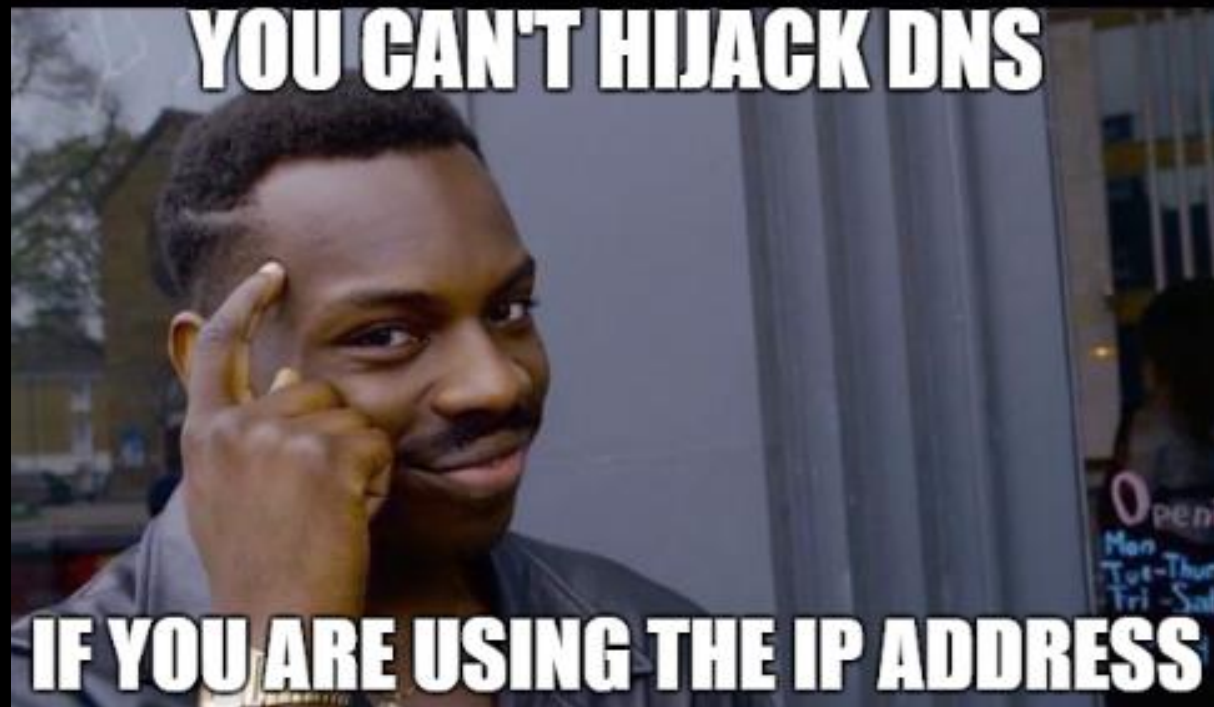
[v]0.0.2

Author: Mr. V

Web: ring0lab.com

Type	Domain	Status
standard	linkedin.com	Not Available
SingularOrPluralise	linkedsins.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	linkeddin.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	linkedsins.co	Available
homoglyphs	linkeclin.co	Available
mirrorization	linnedin.co	Available
homoglyphs	llnkedln.co	Available
mirrorization	linkeein.co	Available
mirrorization	linkeddin.co	Available
mirrorization	linkediin.co	Available
mirrorization	liikedin.co	Available
mirrorization	linkkdin.co	Available
standard	linkedin.net	Available

<https://github.com/ring0lab/catphish>



Why is there traffic

Typing/Spelling errors with RFC1918 networks



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

Hit wrong key	192.x.z.y →	193.x.y.z
	172.x.y.z	152.x.y.z
Omission of number	192.x.y.z →	12.x.y.z
Doubling of keys	10.a.b.c →	100.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>

Key takeaways

- ✓ Powerful attacks can be cheap
- ✓ Only one hit is necessary to enter your target network: statistically typosquatting will work very well using an efficient exploit kit
 - **Redteam**: abuse those!
 - **Blueteam**: monitor those!

<https://blog.0day.rocks/practical-waterholing-through-dns-typoquatting-e252e6a2f99e>