Grep for Evil
Leigh Metcalf, PhD

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
The Evil Bit

RFC 3514 defined the evil bit:

Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. We define a security flag in the IPv4 header as a means of distinguishing the two cases.
The Evil Bit

I didn’t look for the evil bit in packets…

..but I did in domain names!

Using a passive DNS database, I looked for domains with DDOS in them.
ez-ddos.com

EZ-DDOS.COM - professional, non-stop DDOS service specializing in the conduct of the most powerful high-speed attacks (up to 70 GBPS). We attack absolutely any goals in the IT segment. Here you can order a DDOS attack on any network resource. The best way to solve your problems. Fast. Qualitatively. Effectively. Low prices.

Client Anonymity guaranteed 200%

We attack protected from DDOS projects

Round the clock support

The attack on the server (IP)

from 3500 rubles./ ($ 60.) *

We attack any server - game (LineAge, Minecraft, CS etc.), E-mail, streaming (IP-*TV), Cardsharing (satellite TV) and others. The attack - server channel clogged with multi-gigabit stream.

* - Price is for 24 hours (one day).

Other prices ”

The attack on the website (URL)

3000 ./ rubles ($ 50.) *

We attack any sites and forums - the media, the Internet shops, entertainment resources, and any other. The attack on the site can be done in three ways: SYN, HTTP, UDP, thereby achieving the maximum effect.

* - Price is for 24 hours (one day).

About payment ”
Distributed Denial of Service

root@ddos#  

```
64 bytes from 127.0.0.1: icmp_seq=95 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=96 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=97 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=98 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=99 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=100 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=101 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=102 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=103 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=104 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=105 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=106 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=107 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=108 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=109 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=110 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=111 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=112 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=113 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=114 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=115 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=116 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=117 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=118 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=119 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=120 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=121 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=122 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=123 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=124 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=125 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=126 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=127 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=128 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=129 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=130 ttl=64 time=0.015 ms
```

© 2018 Carnegie Mellon University

"[Distribution Statement A] Approved for public release and unlimited distribution."
ddos-team.com

Order DDOS attack / DDOS Services / order DDOS attack / services DDOS / Order ddos on the site / DDOS services / order ddos for free / order DDOS

Professional DDOS service. Quickly and conveniently order DDOS attack at low prices! Only high-quality DDOS services - around the clock!

ICQ: eForall
719567311

ICQ: XaM
710936474

We work 24/7 and 365 days a year
Order ddos attack in the best DDoS Service

DDoS attack how many articles about it you can not re-read. This service, popular on the Internet and every day, dozens of attacks from hackers on various network structures are conducted. Order ddos come not only to sites of simple online stores, bloggers, news portals, but also to infrastructures that are critical in the Internet as a whole. Recently, people's interest in ddos has become more active, they are ready to pay a few thousand a day for the victim not to show signs of life. But to find a quality DDoS Services not as easy as it seems. Every little schoolboy can spend a free ddos attack while wasting nothing. In the vast search engine you can download any botnet, customize it and enjoy not going deep into the knowledge of how it all works. Such people are full and more and more often people become victims of such small scammers who can not cope with the goals all the time.

Tired of looking for where to order DDos attack? Then our comprehensive solutions for conducting ddos attacks on the server and sites are at your service. We can test the majority of existing hosting providers for the stability of the network. The specialists will give you a free consultation on your popular issues related to ddos attacks, recommend actions to provide protection if this is required.

The botnet that we use is unique in its kind. It does not use any third-party modules, it was written completely from 0 to .NET language. A huge number of methods of attacks from the simplest L3 to complex L7. Flexible customization of the bot's aggressiveness and support for JS, Flash, iframe protection of popular antibodies systems such as Cloudflare, Ovh, DDOS Guard, Vosility ... Allows to disguise as an ordinary client of the network. Thus, it is guaranteed delivering a request to the victim’s victim even through protection systems.

Price list for services

Paid, free or other tests do not. Testers, resilers, scammers ... please do not disturb.
ddos.ninja

DDOS NINJA

COMING SOON
Let’s Digress into DDOS for a bit…

And talk about who DDOSes and why they DDOS
First Question – Why DDOS?

A DDOS is a politico-economic act:

- Estonia 2007
  - Revenge
- Spamhaus 2012
  - Revenge
- Hong Kong 2013
  - Censorship
- BBC 2016
  - Terror
- Mirai 2016
  - Revenge
- Swedish Railways 2017
  - Test?
- Danish Railways 2018
  - Test?
- Bitfinex Exchange 2018
  - Competition/economic gain

Provides users asymmetric power for high-profile results.
Who DDOS?

DDOS is surprisingly cheap.

- Barrier to entry is very low
- UI makes it easy for unskilled attackers to play in the game
- There are free stressers (aka, DDOS providers)
- Before the FBI took down Alpha Bay, I found DDOS for as low as $5
- Just searching the web (duckduckgo.com is my friend) I found it for as low as $10
- Unfortunately, I didn’t go buy these to find out what I’d get. Something something something IRB board Something.
- Also known as my boss saying “You want to WHAT?”
DDOS Traditional Attacker Economic Model

Attacker

Investment economic or otherwise

Infrastructure

Victim
DDOS Traditional Attacker Economic Model

Attacker

Investment

Infrastructure

Victim
DDOS Traditional Victim Economic Model

- Victim
  - Investment
  - Anti-DDOS Vendor
    - Infrastructure
      - Attacker
DDOS Traditional Victim Economic Model

[Diagram showing the economic model of a DDOS attack.]

- **Victim**
  - Investment
- **Anti-DDOS Vendor**
- **Infrastructure**
- **Attacker**
Anti DDOS Stops that DDOS

…right?

RIGHT?
DDOS Economic Model: A Trend

Victim

Investment

Anti-DDOS Vendor
DDOS Economic Model: A Trend
DDOS Economic Model: A Trend

Victim

Investment

Anti-DDOS Vendor

Anti-DDOS Vendor

Infrastructure

Investment

Attacker
Wanna buy a DDOS?

IP Booter - #1 Booter/Stresser

Running strong for 5+ months, IP Booter is the last booter/stresser you’ll ever need. Reliability, Power, and Security:

- Incredibly Fast (Instant Attacks)
- 100% Custom Source
- Minimal Logs (Optional Logging)
- Secure & Reliable (256-bit TLS Encryption)
- Standard & VIP Networks (Up to 40+ Gbps)
- Multiple Layer-4 Attack Methods (TCP & UDP)
- 24/7 Great Support (Ticket System)
- Very Affordable Pricing

Competitive Pricing

Our plans are some of the most affordable on the market. Please register/login to view all our available plans. Custom plans are also available; just open a support ticket and one of our agents will gladly assist you as soon as possible.
str3ssed networks booter
Pssst, DDOS for sale!

Free Trial!
All members can enjoy up to 200 Mbps for 300 seconds... for free!

* No credit card required, subject to terms of use and network availability.

Why IP Stresser
- Customizable Plans
  Build your plan from the ground up. Starting at only $9 USD a month!
- Revolutionary Source
  We custom coded our source code to meet the wants and needs of our customers.
- Guaranteed Power
  We guarantee at least 99% of the output power of your stress tests. Nobody else will do that.
- Layer 4 Scripts
  - DDoS
  - UDP
  - UDP-Lag
  - SYN
- Layer 7 Scripts
  - RUDY
  - Slowflood
  - AIMSS

Latest News
- Memorial Day Sale
- Black Friday Sale
- Scripts Updated
- Memorial Day Sale
- CloudFlare Memory Leak
- Black Friday Sale
- Scripts Updated
- Memorial Day Sale
Meteor Stressed

WHAT MAKES METEOR-STRESSER DIFFERENT?
If you are looking for a hard hitting and reliable booter, then you have come to the right place. Meteor Stressed specializes in hard hitting booter power 24/7. Don't worry about how many other floods are running, YOUR output will always be consistent, you haven't seen anything quite like it, until now.

Low Prices
We offer a cheap and high-quality booter.

Anonyma
We offer an irrevocable service.

Secured
All data is encrypted using the HTTPS protocol.
But what is that when I go there?
Maybe it’s just one domain?
There’s also a Chinese ISP supporting...

Each package has our dedicated VIP node. We guarantee 15-30Gbps per attack.

A revolutionary IP test platform

The best pressure on the market platform.
What about tacit DDOS support?

It’s one thing to directly allow the DDOS vendors to sell…

…but what about other support?
Youtube videos!

This Booter Can be used For free or Can be Bought to increase Bandwidth and Duration

Best Free Booters (2018)
99,220 views
Youtube videos

DDOS | TOP 5 FREE BOOTER / STRESSER |

9,317 views
Youtube videos

Zombie Stresser (made by me)
186 views
We also have blogspot sites
blogspot.ru sites

ddos attack

Tuesday, October 15, 2013

kurdish hacker

[Anonymous kurdistan]

[#H A L O] -- [kurdish hacker]
Want to do your own DDOS?

DISCLAIMER: USE ON YOUR OWN RISK. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER OR CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES.

Project Samples
Or what about…

UBoat HTTP

A POC HTTP Botnet designed to replicate a full weaponised commercial botnet

Disclaimer

This project should be used for authorized testing or educational purposes only.

The main objective behind creating this offensive project was to aid security researchers and to enhance the understanding of commercial HTTP loader style botnets. I hope this project helps to contribute to the malware research community and people can develop efficient counter mesures :)  

Usage of uboat without prior mutual consistency can be considered as an illegal activity. It is the final user's responsibility to obey all applicable local, state and federal laws. Authors assume no liability and are not responsible for any misuse or damage caused by this program.

What is a Botnet?
Beyond DDOS

It makes sense that these guys would advertise themselves, they want people to buy them. That’s their economic motive.

So I went looking for botnets.
botnet.cc

A revolutionary IP test platform

The best pressure on the market platform.

LOGIN(LOGIN.PHP)  REGISTER(REGISTER.PHP)

Take down anyone with the best ip stresser / booter!
Botnet Servicex

We are the best in our job!

Botnet-Servicex is an underground business dedicated to setup botnets. We give the control panel + exe totally lud = 400 bots. We have Banking, DDoS, Stealers, Bitcoin Miners and Pos Malwares. Best prices on the net, pay via Bit or Pm. You can contact us via icq.

How our botnet works

The botnets have a control panel allocated in a Secure Private Server. We help you to use it, depending on the quantity of bots (pc zombies) you have you will receive more or less logs. We are working since 2009 without any problem with our clients.

Features

of the botnets depends the botnet you choose, it can be: grab password, steal password, attack web via ddos, grab dumps (track 2), load exe...

Botnet-Servicex, Inc 2009-2017
Botnet Servicex

Ransomware Winlockers

The Winlockers its a type of Malware, blocks the PC, encrypt the files and the victims need to pay a quantity of money to recov the PC. The pay usually in Etc, if the victim not pay the files of pc are deleted.

List and Prices

WinLocker Builder 4.0 - 100$  
MultiLocker v3.0 { Panel + Builder + Fud Exe + Lending Page + 100 Bots } - 200$  
Silent WinLocker v5.0 { Panel + Fud Exe + Lending Page + 100 Bots } - 250$

Features
- Build Exe Malware (...) 
- Control Pys of Bots 
- And More

Botnet-Servicex .Inc 2009-2017
Cythosia botnet
Mirai botnet Shop

Trusted

Find out why:

---

**BENEFITS OF CHOOSING ME**

**LIGHTING FAST**

I'm always on call, ready to provide sales and support at any given time.
freetrojanbotnet.com

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Type</th>
<th>Video</th>
<th>Risk</th>
<th>Verified</th>
<th>Price</th>
<th>Facebook</th>
</tr>
</thead>
<tbody>
<tr>
<td>07-02-2017</td>
<td>Will have a bigger update</td>
<td>php</td>
<td>yes</td>
<td>low</td>
<td>true</td>
<td>false</td>
<td>0 facebook</td>
</tr>
<tr>
<td>05-02-2016</td>
<td>I NEED PANEL AND DNS BOT ANDREMEDA LAST VERSION</td>
<td>php</td>
<td>yes</td>
<td>low</td>
<td>true</td>
<td>false</td>
<td>0 facebook</td>
</tr>
<tr>
<td>01-06-2016</td>
<td>self SMTP Bot+rooter c0ded in c8</td>
<td>php</td>
<td>yes</td>
<td>low</td>
<td>true</td>
<td>false</td>
<td>0 facebook</td>
</tr>
<tr>
<td>01-06-2016</td>
<td>Client 64.1.1 (Anon) Backdoor trojan</td>
<td>php</td>
<td>yes</td>
<td>low</td>
<td>true</td>
<td>false</td>
<td>0 facebook</td>
</tr>
<tr>
<td>03-09-2015</td>
<td>Betroot 1.8.8.1 full panel function+Raid + 1008 full gui!</td>
<td>c/c++</td>
<td>yes</td>
<td>low</td>
<td>true</td>
<td>false</td>
<td>1008 facebook</td>
</tr>
</tbody>
</table>

Search:
Phishing – phishtown.com

JOIN THE REBELLION
E-Mail the Admiral
What about ransomware?

Why on earth would someone put ransomware in a domain name?

Well…

(DO NOT GO TO THESE SITES....)
Windows Defender Alert: Zeus Virus Detected In Your Computer !!

Please Do Not Shut Down or Reset Your Computer.

The following data will be compromised if you continue:
1. Passwords
2. Browser History
3. Credit Card Information
4. Local Hard Disk Files.

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.

Call Technical Support Immediately at +1 888-441-1595

Call Microsoft Technical Department:
(888)441 1595(Toll Free)
microsoft-protection-from-ransomware.info

There’s a phone number listed on this site. 888-441-1595

….It belongs to behappy2day.com. A mail order bride service.
ransomware-threat-detected-remove-it-now.info
ransomware-threat-detected-remove-it-now.info

Googling the phone number in this site goes to websites that claims it belongs to either Microsoft, Apple, iTunes…

I’m going to go out on a limb here and claim it’s ‘bad’.
Looking for ransomware in TXT records

I thought, why not? I’m grepping for evil.

I have a passive DNS data set.

Let’s see what happens!

(Spoiler Alert: I found some…)
Looking for ransomware in TXT records

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>..</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a (1).exe</td>
<td>2017-09-11 18:18</td>
<td>155K</td>
<td></td>
</tr>
<tr>
<td>a (11).exe</td>
<td>2017-09-11 18:18</td>
<td>209K</td>
<td></td>
</tr>
<tr>
<td>a (15).exe</td>
<td>2017-09-11 18:18</td>
<td>208K</td>
<td></td>
</tr>
<tr>
<td>a (16).exe</td>
<td>2017-09-11 18:18</td>
<td>1.3M</td>
<td></td>
</tr>
<tr>
<td>a (17).exe</td>
<td>2017-09-11 18:18</td>
<td>1.3M</td>
<td></td>
</tr>
<tr>
<td>a (18).exe</td>
<td>2017-09-11 18:18</td>
<td>224K</td>
<td></td>
</tr>
<tr>
<td>a (19).exe</td>
<td>2017-09-11 18:18</td>
<td>224K</td>
<td></td>
</tr>
<tr>
<td>a (20).exe</td>
<td>2017-09-11 18:18</td>
<td>224K</td>
<td></td>
</tr>
<tr>
<td>a (21).exe</td>
<td>2017-09-11 18:18</td>
<td>1.7M</td>
<td></td>
</tr>
<tr>
<td>a (27).exe</td>
<td>2017-09-11 18:18</td>
<td>224K</td>
<td></td>
</tr>
<tr>
<td>a (28).exe</td>
<td>2017-09-11 18:18</td>
<td>1.3M</td>
<td></td>
</tr>
<tr>
<td>a (29).exe</td>
<td>2017-09-11 18:18</td>
<td>319K</td>
<td></td>
</tr>
<tr>
<td>a (30).exe</td>
<td>2017-09-11 18:18</td>
<td>319K</td>
<td></td>
</tr>
<tr>
<td>a (32)</td>
<td>2017-09-11 18:18</td>
<td>319K</td>
<td></td>
</tr>
<tr>
<td>a (33).exe</td>
<td>2017-09-11 18:18</td>
<td>1.3M</td>
<td></td>
</tr>
<tr>
<td>a (34).exe</td>
<td>2017-09-11 18:18</td>
<td>100K</td>
<td></td>
</tr>
<tr>
<td>e (4).exe</td>
<td>2017-09-11 18:18</td>
<td>523K</td>
<td></td>
</tr>
<tr>
<td>e (5).exe</td>
<td>2017-09-11 18:18</td>
<td>210K</td>
<td></td>
</tr>
<tr>
<td>e (6).exe</td>
<td>2017-09-11 18:18</td>
<td>1.9M</td>
<td></td>
</tr>
<tr>
<td>e (7).exe</td>
<td>2017-09-11 18:18</td>
<td>164K</td>
<td></td>
</tr>
<tr>
<td>e (8).exe</td>
<td>2017-09-11 18:18</td>
<td>1.3M</td>
<td></td>
</tr>
<tr>
<td>e (9).exe</td>
<td>2017-09-11 18:18</td>
<td>319K</td>
<td></td>
</tr>
<tr>
<td>e (10).exe</td>
<td>2017-09-11 18:18</td>
<td>319K</td>
<td></td>
</tr>
<tr>
<td>e (11).exe</td>
<td>2017-09-11 18:18</td>
<td>224K</td>
<td></td>
</tr>
<tr>
<td>e (12).exe</td>
<td>2017-09-11 18:18</td>
<td>1.3M</td>
<td></td>
</tr>
<tr>
<td>e (13).exe</td>
<td>2017-09-11 18:18</td>
<td>1.3M</td>
<td></td>
</tr>
<tr>
<td>e (14).exe</td>
<td>2017-09-11 18:18</td>
<td>12M</td>
<td></td>
</tr>
<tr>
<td>e (15).exe</td>
<td>2017-09-11 15:36</td>
<td>58K</td>
<td></td>
</tr>
<tr>
<td>e (16).exe</td>
<td>2017-09-11 15:36</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>e (17).exe</td>
<td>2017-09-11 15:37</td>
<td>1.4M</td>
<td></td>
</tr>
</tbody>
</table>
Another thing I learned...

Do NOT go to sites with both **bank** and **login** in the name.
Deceptive site ahead

Attackers on bankofamerica.com.login.sign-in.signonv2.screen.castadotaciones.com may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

[ ] Automatically report details of possible security incidents to Google. Privacy policy

 DETAILS

 Back to safety
bankofamerica.com.login.sign-in....
Deceptive site ahead

Attackers on pnc-bank-online-banking-login.com may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

☐ Automatically report details of possible security incidents to Google. Privacy policy.
pnc-banking...
bank AND login

Neither of those were actually Bank sites.

Isn’t it nice they tell me they are?
Zero Days

What else to look for?

How about 0days? I found a website that promised to sell me some.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>OriensDB 2.2.x Remote Code Execution Exploit</td>
</tr>
<tr>
<td>Date</td>
<td>06-18-2017</td>
</tr>
<tr>
<td>Category</td>
<td>remote exploits</td>
</tr>
<tr>
<td>Platform</td>
<td>Java</td>
</tr>
<tr>
<td>Verified</td>
<td>✔</td>
</tr>
<tr>
<td>Price</td>
<td>Free</td>
</tr>
<tr>
<td>Risk</td>
<td><strong>High</strong> [Severity: High, Critical]</td>
</tr>
<tr>
<td>Platforms</td>
<td>Linux, Windows, macOS</td>
</tr>
<tr>
<td>Description</td>
<td>This Metasploit module leverages a privilege escalation on OriensDB to execute unauthorized OS commands. All versions from 2.2.2 up to 2.2.24 should be vulnerable.</td>
</tr>
<tr>
<td>Author</td>
<td>Reznicek Juraj, Bogdanovski Almosen</td>
</tr>
<tr>
<td>EOL</td>
<td>29</td>
</tr>
<tr>
<td>Exploits</td>
<td>1</td>
</tr>
<tr>
<td>Ranks</td>
<td>8</td>
</tr>
</tbody>
</table>

**0day.today**
So this looks easy, right?

I found:

- DDOS
- botnets
- ransomware
- 0days…

And that’s not even including the malware!
On the other hand…

<table>
<thead>
<tr>
<th>Report</th>
<th>Total Lists</th>
<th>Lists Gained</th>
<th>Lists Lost</th>
<th>Unique Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012.1</td>
<td>11</td>
<td>--</td>
<td>--</td>
<td>6468501</td>
</tr>
<tr>
<td>2012.2</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>9235902</td>
</tr>
<tr>
<td>2013.1</td>
<td>20</td>
<td>10</td>
<td>1</td>
<td>12592250</td>
</tr>
<tr>
<td>2013.2</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>5027066</td>
</tr>
<tr>
<td>2014.1</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>2772391</td>
</tr>
<tr>
<td>2014.2</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>10446624</td>
</tr>
<tr>
<td>2015.1</td>
<td>35</td>
<td>19</td>
<td>4</td>
<td>12231742</td>
</tr>
<tr>
<td>2015.2</td>
<td>35</td>
<td>0</td>
<td>0</td>
<td>13051429</td>
</tr>
<tr>
<td>2016.1</td>
<td>31</td>
<td>7</td>
<td>11</td>
<td>24359712</td>
</tr>
<tr>
<td>2016.2</td>
<td>26</td>
<td>4</td>
<td>9</td>
<td>26274848</td>
</tr>
<tr>
<td>2017.1</td>
<td>27</td>
<td>4</td>
<td>3</td>
<td>26805987</td>
</tr>
<tr>
<td>2017.2</td>
<td>26</td>
<td>5</td>
<td>6</td>
<td>40857873</td>
</tr>
</tbody>
</table>
While finding these domains was fun…

We’re not even making a dent in the total amount of badness out there by just looking for the easy things.

In summary: Finding the guys that are hiding is hard.
Finding the guys that aren’t hiding isn’t.
Questions?

PS. Don’t go to domains with both bank and login in them!