nominum™

Harness Your Internet Activity

Zeroing in On Zero Days
DNS OARC
Spring 2014

Ralf Weber

Ralf.weber@Nominum.com

Nominum Data Sources

- Worldwide ISP DNS data
  - ~Terabyte of data per day
  - Rough estimate 5% of ISPs resolver traffic
  - Activity from around the world, including China
  - Limited response data
  - Lots of other data sources – various threat feeds etc

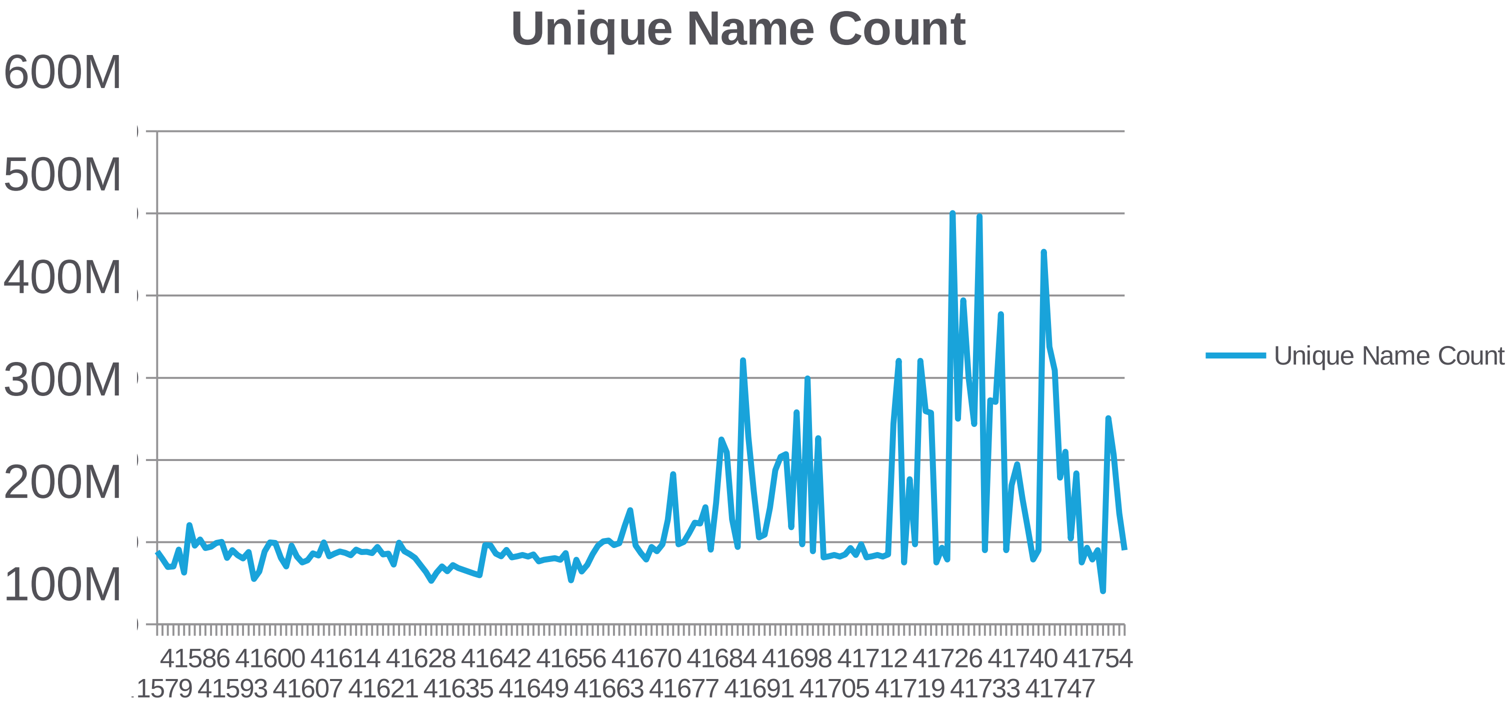
Have You Been Seeing This?

```
krsfwzohwdghqx.liebiao.800fy.com.
wxctkzubkb.liebiao.800fy.com.
avytafkjad.liebiao.800fy.com.
gfqhuxenun.liebiao.800fy.com.
uv.liebiao.800fy.com.
ivatsnkb.liebiao.800fy.com.
wfmlgzyrufaxid.liebiao.800fy.com.
qzgziliv.liebiao.800fy.com.
qxgtqfyv.liebiao.800fy.com.
```

Interesting Recent Trend
Pseudo Random Subdomain Attacks

- First observed Jan 2014
- ~950 names attacked
  - 1 – 2 day spikes
  - Queries observed at resolvers worldwide
  - Queries start and stop about the same time worldwide
- Usually one more label than a resolvable domain
  - First label random, but often follows a pattern
  - Millions – tens of millions of randomized subdomains
  - Auth servers often fail, if they stay up they usually give back NXDOMAIN
  - Recently we also see NODATA, NOERROR returned
- Mostly very low normal daily query volumes, from within China
  - Predominantly Chinese gaming & adult sites, some exceptions
- IPs sending attack-related queries strongly correlated with Open DNS Proxies or Resolvers

Uptick in Unique Names



Characteristics of Target Names

- Some names w/high Alexa rank
- Chinese gaming sites
  - evidence suggests some reside on hacked legit sites
- Adult content
- UK gaming site

Alexa Data for Attacked Names

Name under attack	**“Core” name**	**Alexa rank**
baidu.com.	baidu.com	5
blog.sina.com.cn.	sina.com.cn	13
xlscq.blog.163.com.	163.com	30
www.bet365.com.	bet365.com	179
www.appledaily.com.tw.	appledaily.com.tw	915
hk.apple.nextmedia.com.	nextmedia.com	2017
nextmedia.com.	nextmedia.com	2017
tw.nextmedia.com.	nextmedia.com	2017
1.92xin.sinaapp.com.	sinaapp.com	4786
applevideo.edgesuite.net.	edgesuite.net	5579

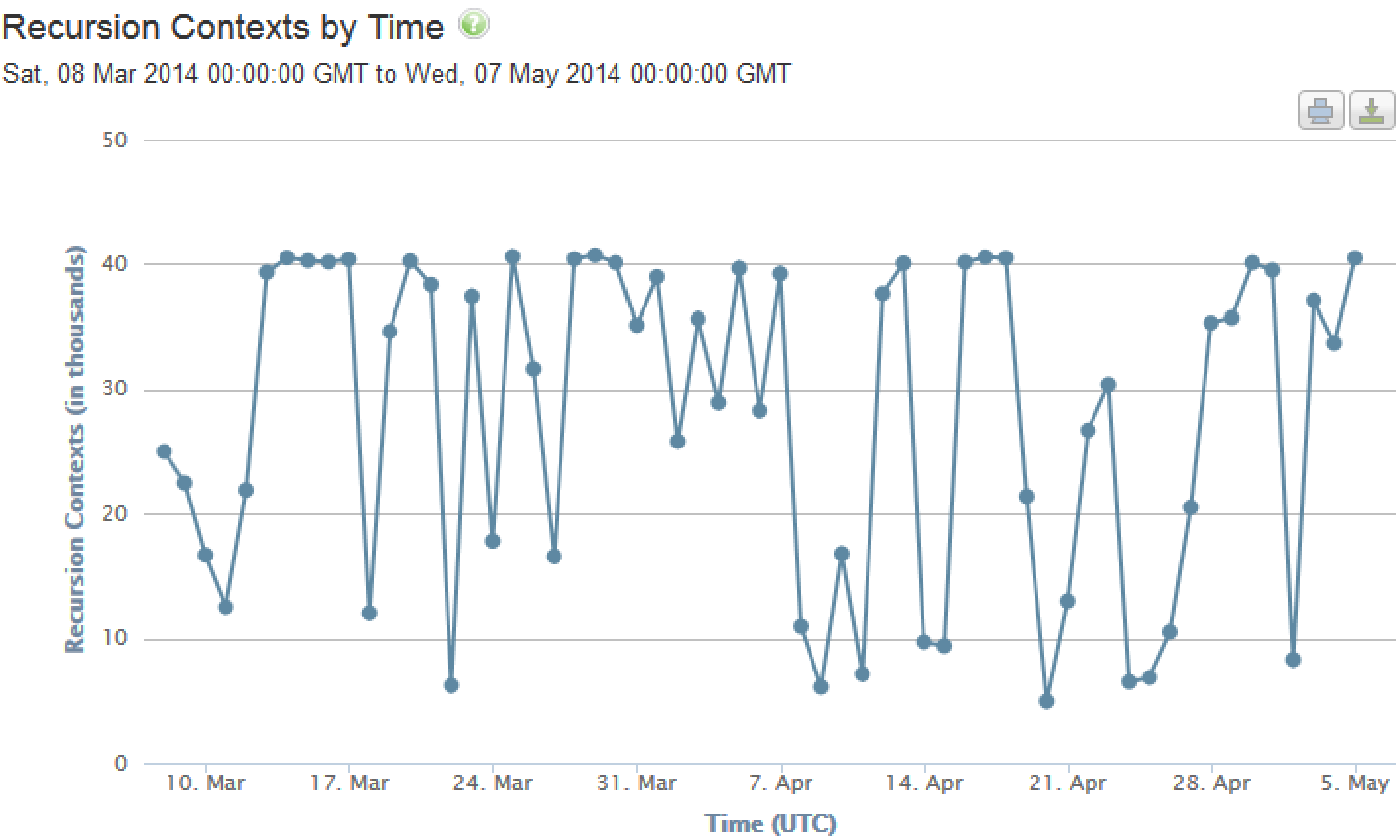
7% of names attacked in Alexa 1M

Some *very* high ranking

92% of names have never been in Alexa 1M

Data was normalized to reflect different ranks over time

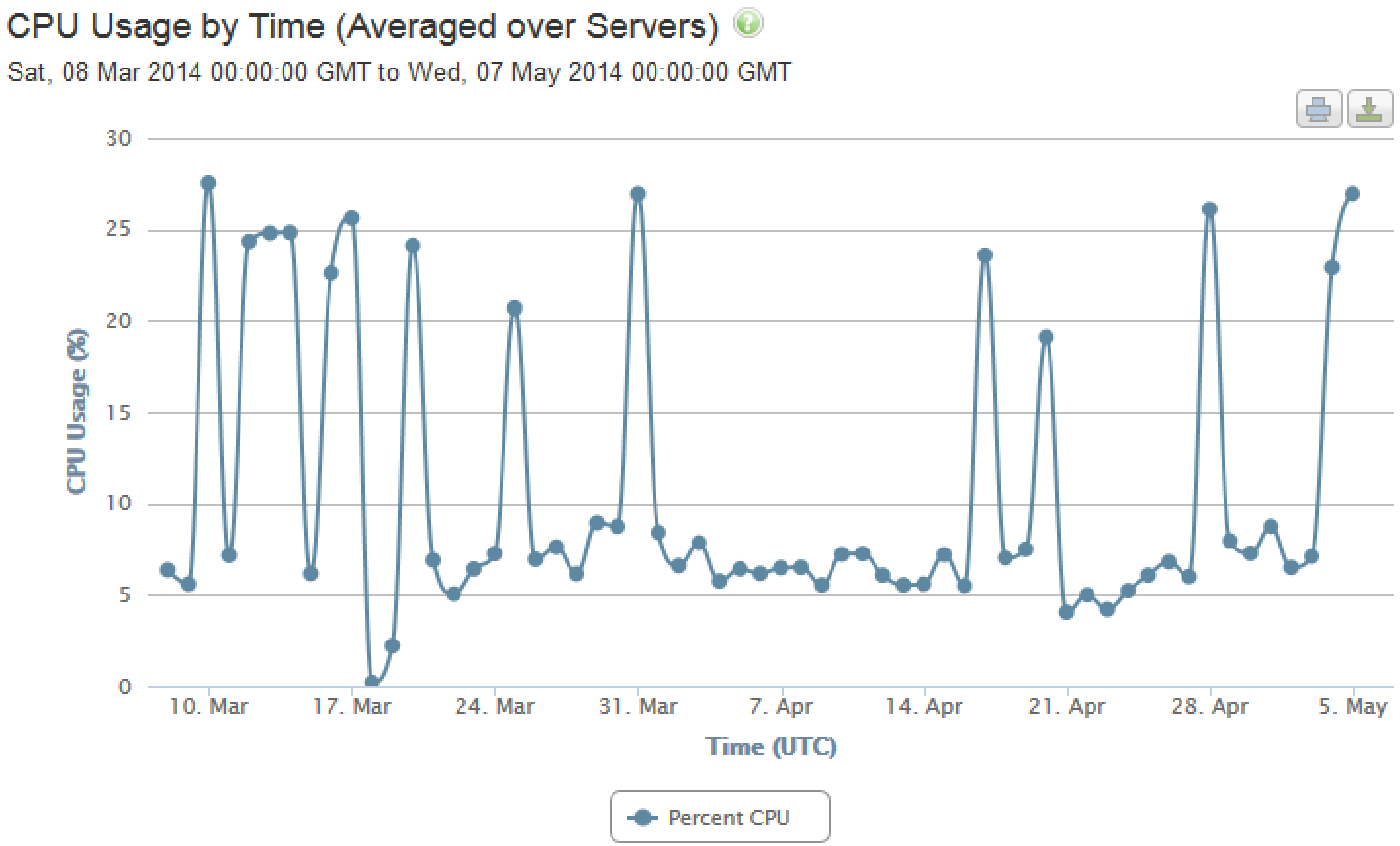
Resolver Impact



Recursion Contexts by Time

Sat, 08 Mar 2014 00:00:00 GMT to Wed, 07 May 2014 00:00:00 GMT

Resolver Impact



CPU Usage by Time (Averaged over Servers)

Sat, 08 Mar 2014 00:00:00 GMT to Wed, 07 May 2014 00:00:00 GMT

Attack Distribution # Days
Mar 10 – May 6 2014

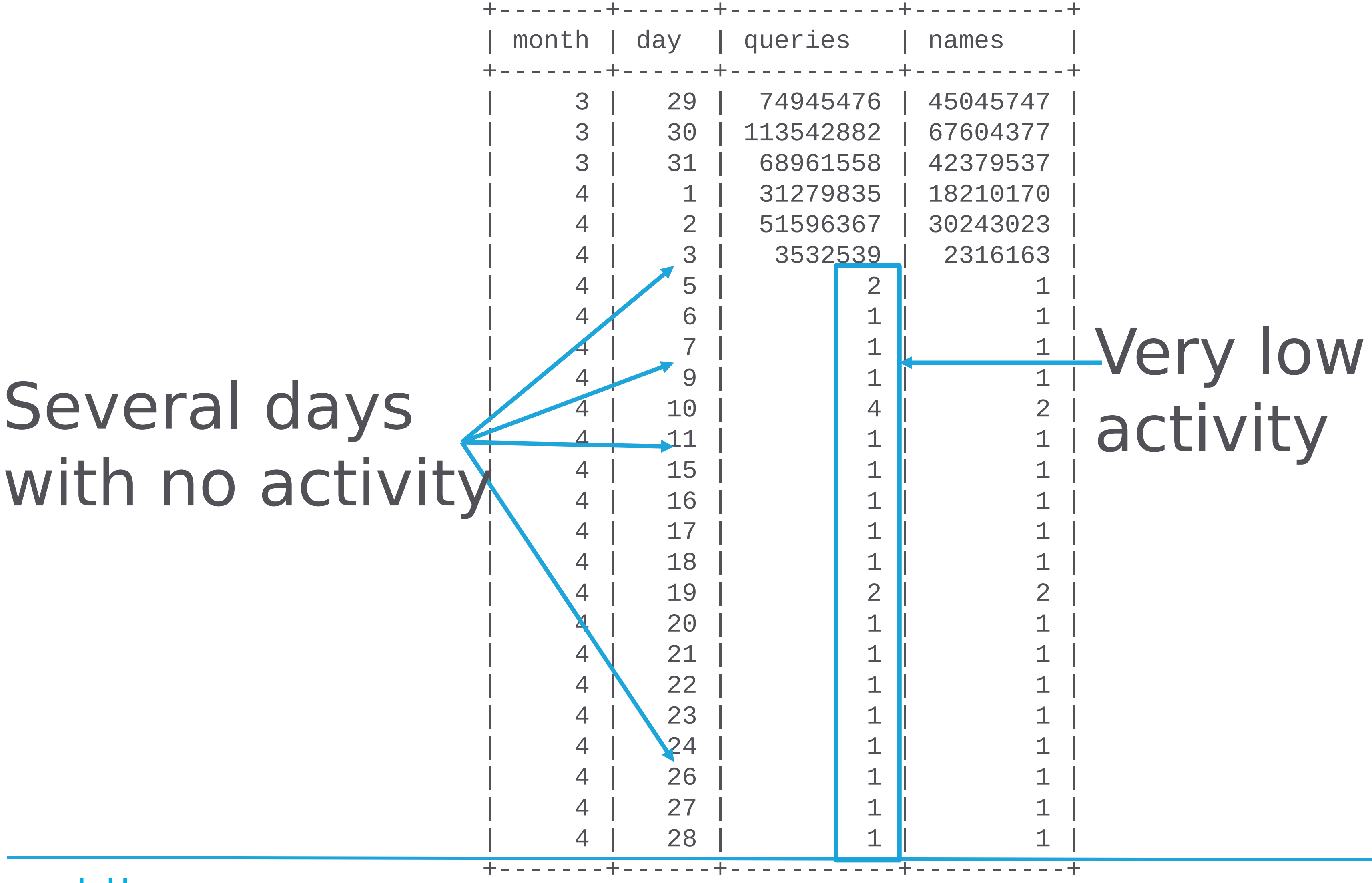
% domains attacked	Cumulative %	Total domains attacked	Days domain attacked
71.9%	71.9%	373	1
18.7%	90.6%	97	2
3.5%	94.0%	18	3
2.5%	96.5%	13	4
1.5%	98.1%	8	5
0.6%	98.7%	3	6
0.4%	99.0%	2	7
0.4%	99.4%	2	8
0.4%	99.8%	2	9
0.2%	100.0%	1	17

Top Ten Names Used

Ranked by days used

2.1%	2.1%	17	www.500sf.com.
1.1%	3.3%	9	www.yuerengu.com.cn.
1.1%	4.4%	9	liebiao.800fy.com.
1.0%	5.4%	8	www.23us.com.
1.0%	6.4%	8	www.uc711.com.
0.9%	7.3%	7	wuyangairsoft.com.
0.9%	8.2%	7	web.pay1.cn.
0.8%	8.9%	6	www.zhaobjl.com.
0.8%	9.7%	6	978sf1111.ewc668.com.
0.8%	10.4%	6	vip.mia0pay.net.

One Month Worldwide Activity For A Name liebiao800fy.com Mar 28-Apr 28 2014



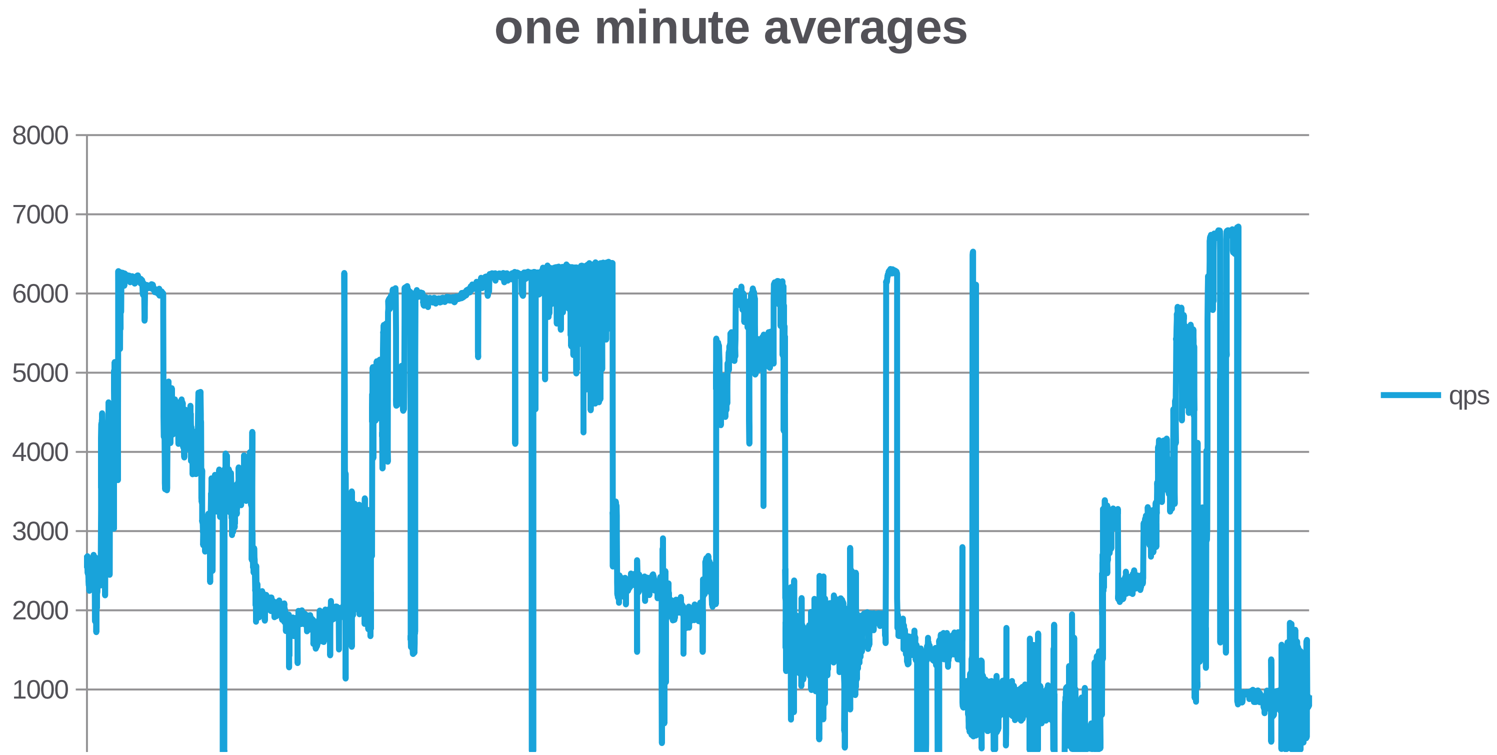
```
+-------+------+-----------+----------+
| month | day  | queries   | names    |
+-------+------+-----------+----------+
|     3 |   29 |  74945476 | 45045747 |
|     3 |   30 | 113542882 | 67604377 |
|     3 |   31 |  68961558 | 42379537 |
|     4 |    1 |  31279835 | 18210170 |
|     4 |    2 |  51596367 | 30243023 |
|     4 |    3 |   3532539 |  2316163 |
|     4 |    5 |         2 |        1 |
|     4 |    6 |         1 |        1 |
|     4 |    7 |         1 |        1 |
|     4 |    9 |         1 |        1 |
|     4 |   10 |         4 |        2 |
|     4 |   11 |         1 |        1 |
|     4 |   15 |         1 |        1 |
|     4 |   16 |         1 |        1 |
|     4 |   17 |         1 |        1 |
|     4 |   18 |         1 |        1 |
|     4 |   19 |         2 |        2 |
|     4 |   20 |         1 |        1 |
|     4 |   21 |         1 |        1 |
|     4 |   22 |         1 |        1 |
|     4 |   23 |         1 |        1 |
|     4 |   24 |         1 |        1 |
|     4 |   26 |         1 |        1 |
|     4 |   27 |         1 |        1 |
|     4 |   28 |         1 |        1 |
+-------+------+-----------+----------+
```

Several days with no activity

Very low activity

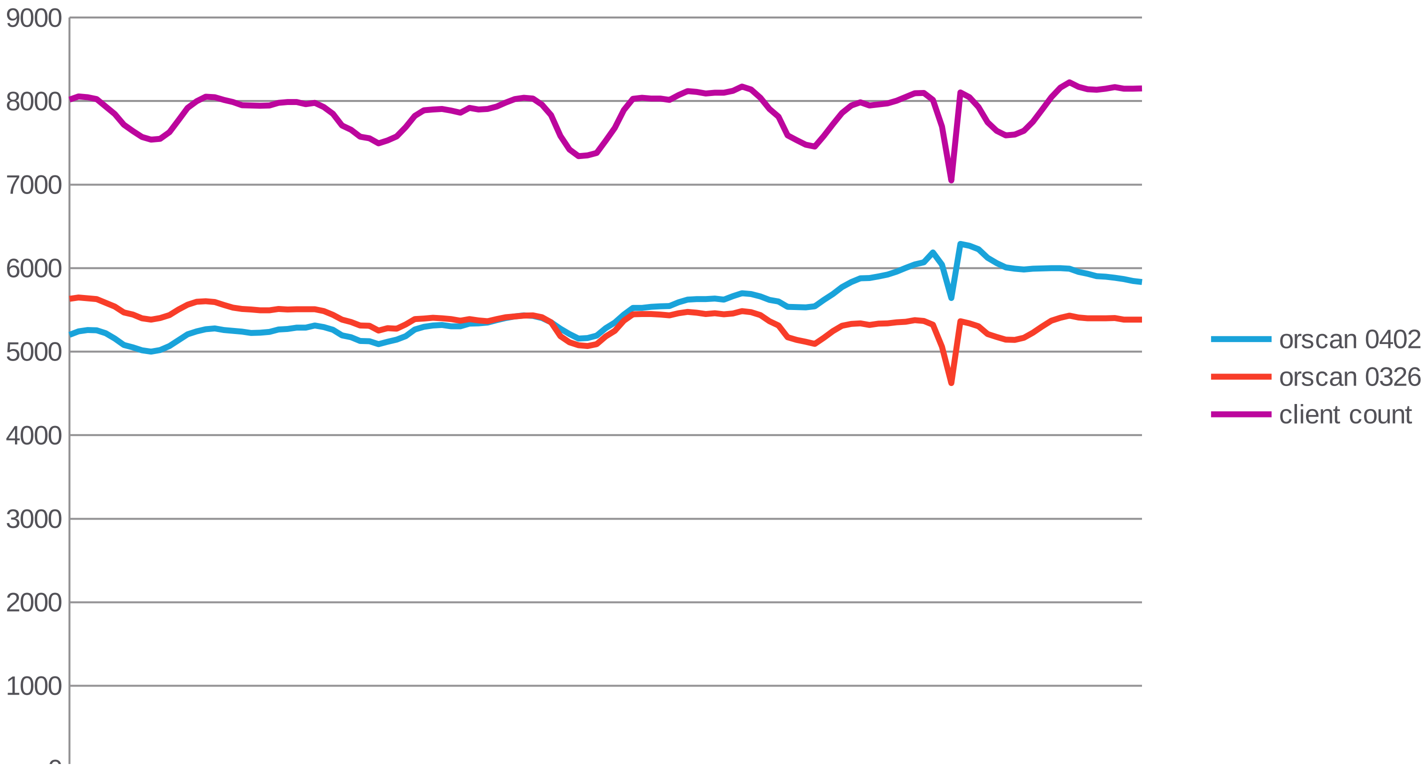
Daily Query Pattern
QPS for *.800fy.com

March 29 00:00 GMT through Apr 3 00:00 GMT



Matches with openresolverproject scans liebiao800fy.com 0326 and 0402

March 29 00:00 GMT through Apr 3 00:00 GMT

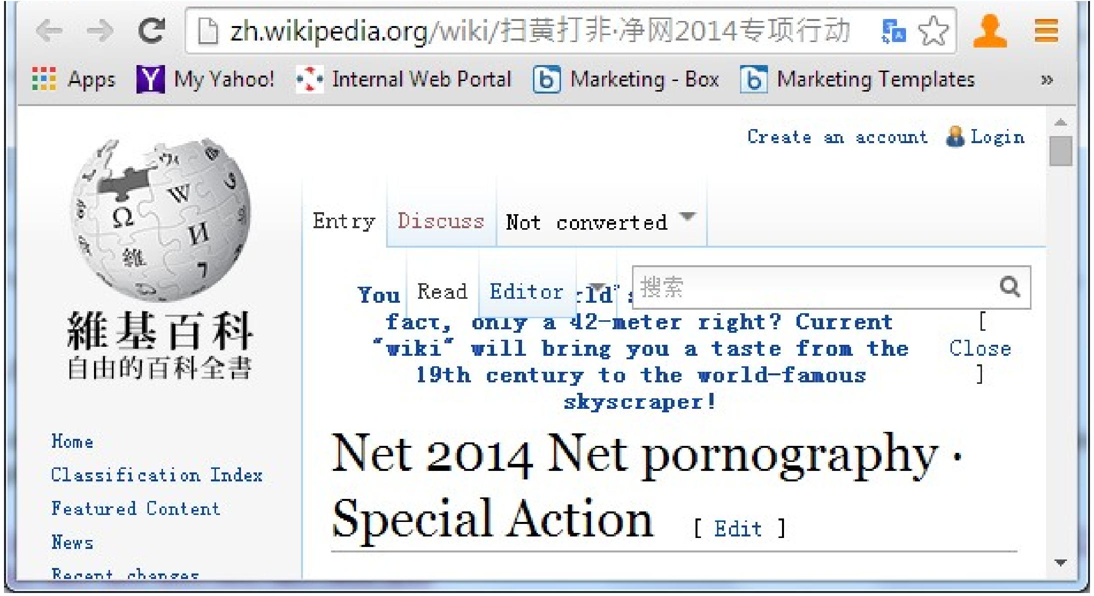


Zeroing In On Zero Days

- Some success figuring out randomization algorithms
  - Detect spikes
  - Analyze subdomains
  - Known pattern?
    - Move to a monitor and block list
  - New pattern?
    - Monitor
- Enables very fast detection
  - New domains with familiar patterns - ~20 mins
  - New patterns – working on algorithms to automate
- We can add affected domains to block or monitor lists quickly
  - They get distributed instantly
- It will get harder – attackers will adapt

Abrupt End to Major Attack Activity

- Is Chinese gov crackdown on certain kinds of web content responsible?

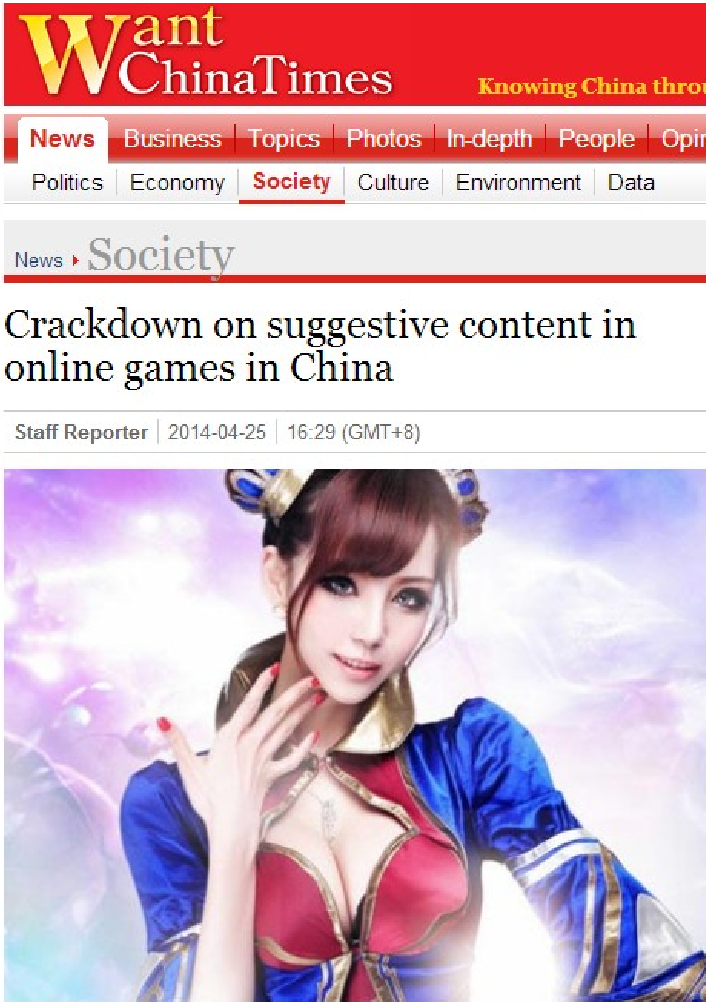


zh.wikipedia.org/wiki/扫黄打非·净网2014专项行动

You ...ld' ... fact, only a 42-meter right? Current "wiki" will bring you a taste from the 19th century to the world-famous skyscraper!

[Close]

Net 2014 Net pornography · Special Action [Edit]



Crackdown on suggestive content in online games in China

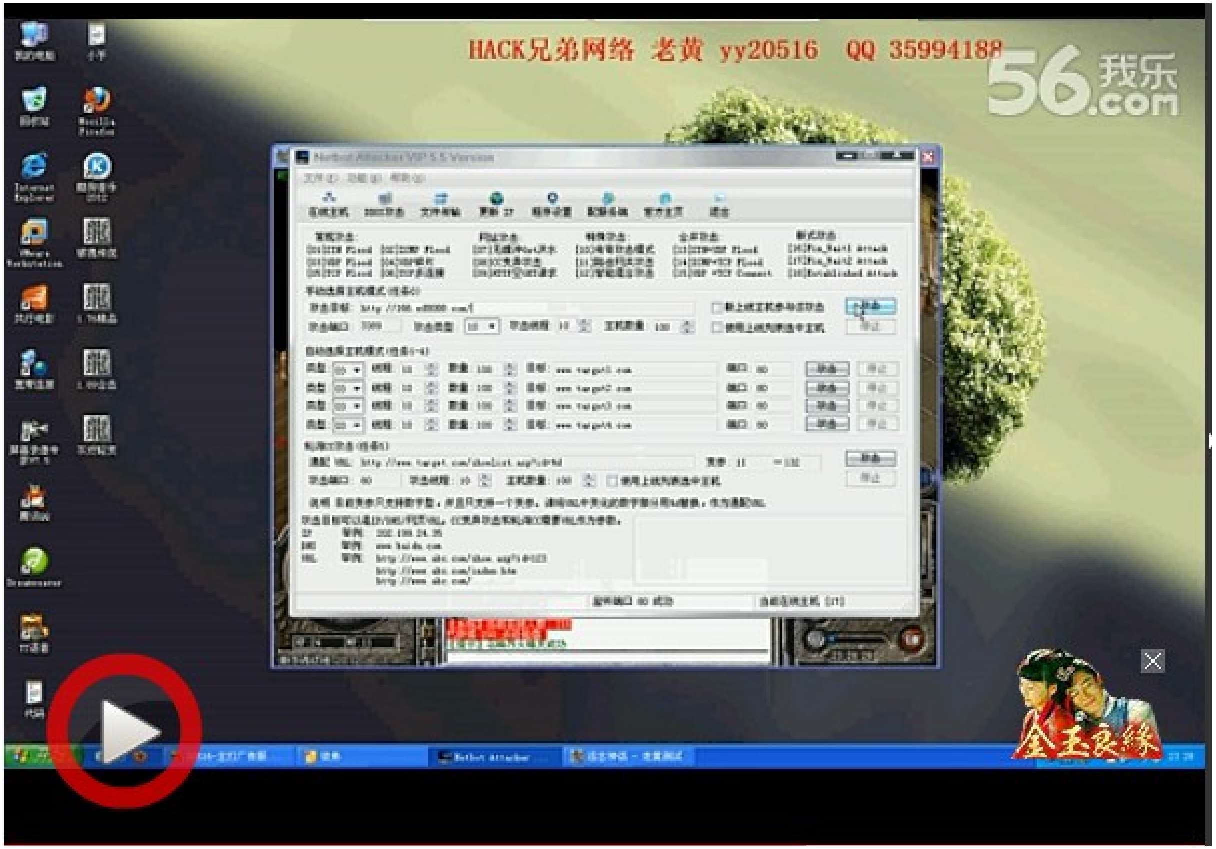
Staff Reporter | 2014-04-25 | 16:29 (GMT+8)

What’s The Motive?

Skirmishing among small game/adult site owners?

Testing and perfecting techniques for a bigger event?

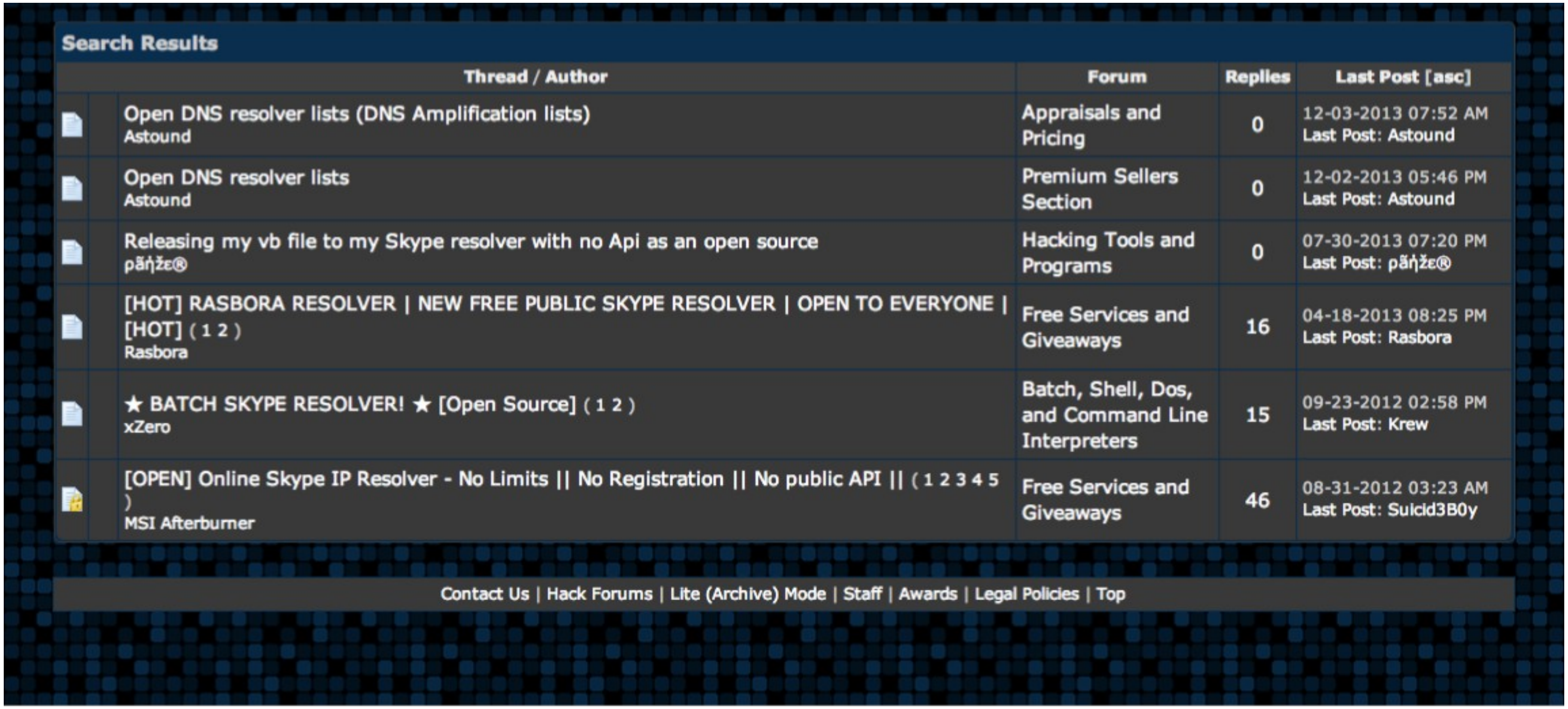
Your Friendly Neighborhood DDoS Service



A *real* Chinese menu

□

Your Friendly Neighborhood DDoS Service



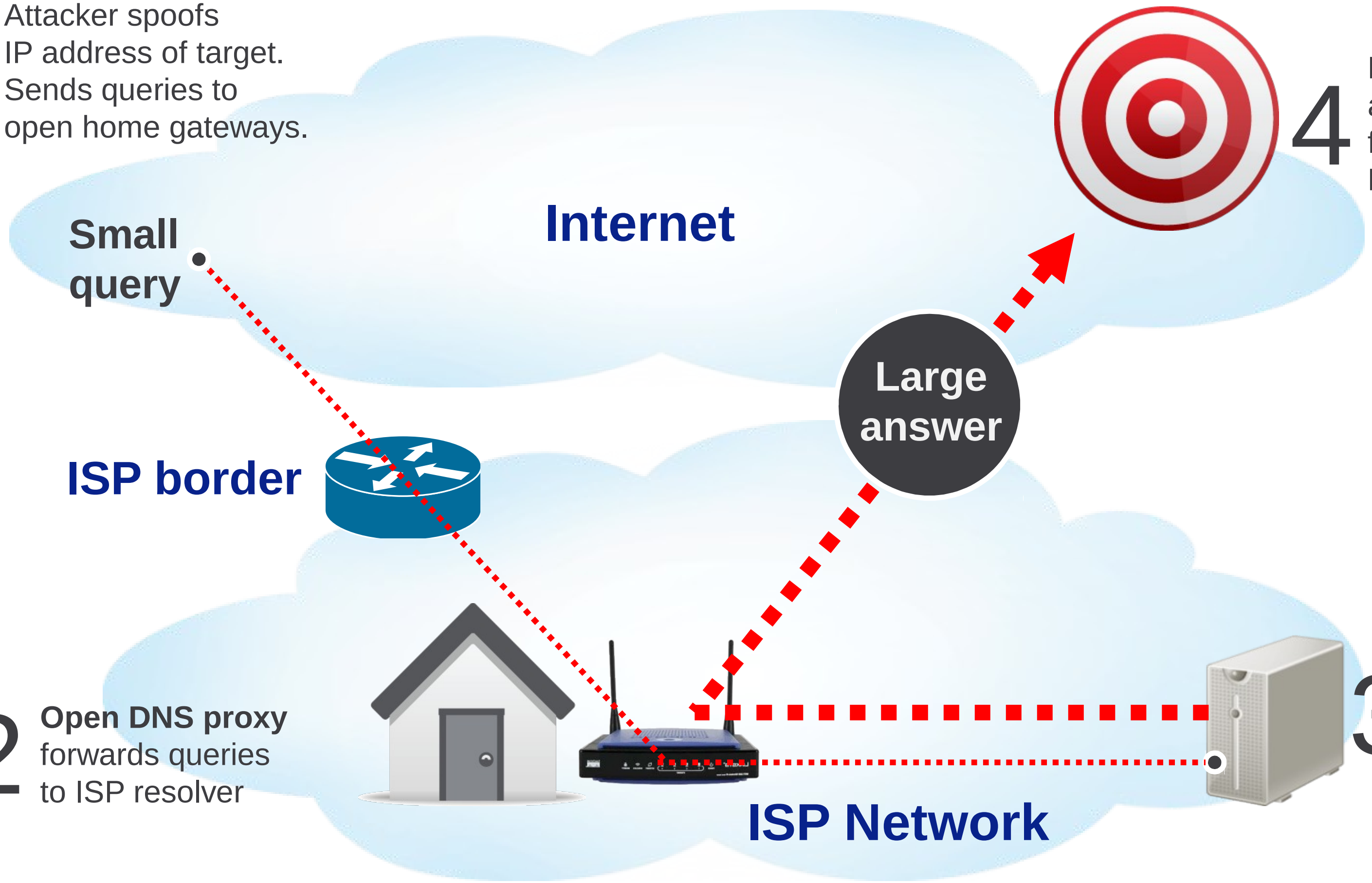
Search Results

Thread / Author	Forum	Replies	Last Post [asc]
Open DNS resolver lists (DNS Amplification lists) Astound	Appraisals and Pricing	0	12-03-2013 07:52 AM Last Post: Astound
Open DNS resolver lists Astound	Premium Sellers Section	0	12-02-2013 05:46 PM Last Post: Astound
Releasing my vb file to my Skype resolver with no Api as an open source păῆžε®	Hacking Tools and Programs	0	07-30-2013 07:20 PM Last Post: păῆžε®
[HOT] RASBORA RESOLVER | NEW FREE PUBLIC SKYPE RESOLVER | OPEN TO EVERYONE | [HOT] (1 2) Rasbora	Free Services and Giveaways	16	04-18-2013 08:25 PM Last Post: Rasbora
★ BATCH SKYPE RESOLVER! ★ [Open Source] (1 2) xZero	Batch, Shell, Dos, and Command Line Interpreters	15	09-23-2012 02:58 PM Last Post: Krew
[OPEN] Online Skype IP Resolver - No Limits || No Registration || No public API || (1 2 3 4 5) MSI Afterburner	Free Services and Giveaways	46	08-31-2012 03:23 AM Last Post: Suicid3B0y

Contact Us | Hack Forums | Lite (Archive) Mode | Staff | Awards | Legal Policies | Top

http://www.hackforums.net/search.php?action=results&sid=b4baf426ad4820f75922f2444ab90254&sortby=lastpost&order=desc Thu May 08 2014 15:16:06 GMT-0700 (UTC)

Open DNS Proxies



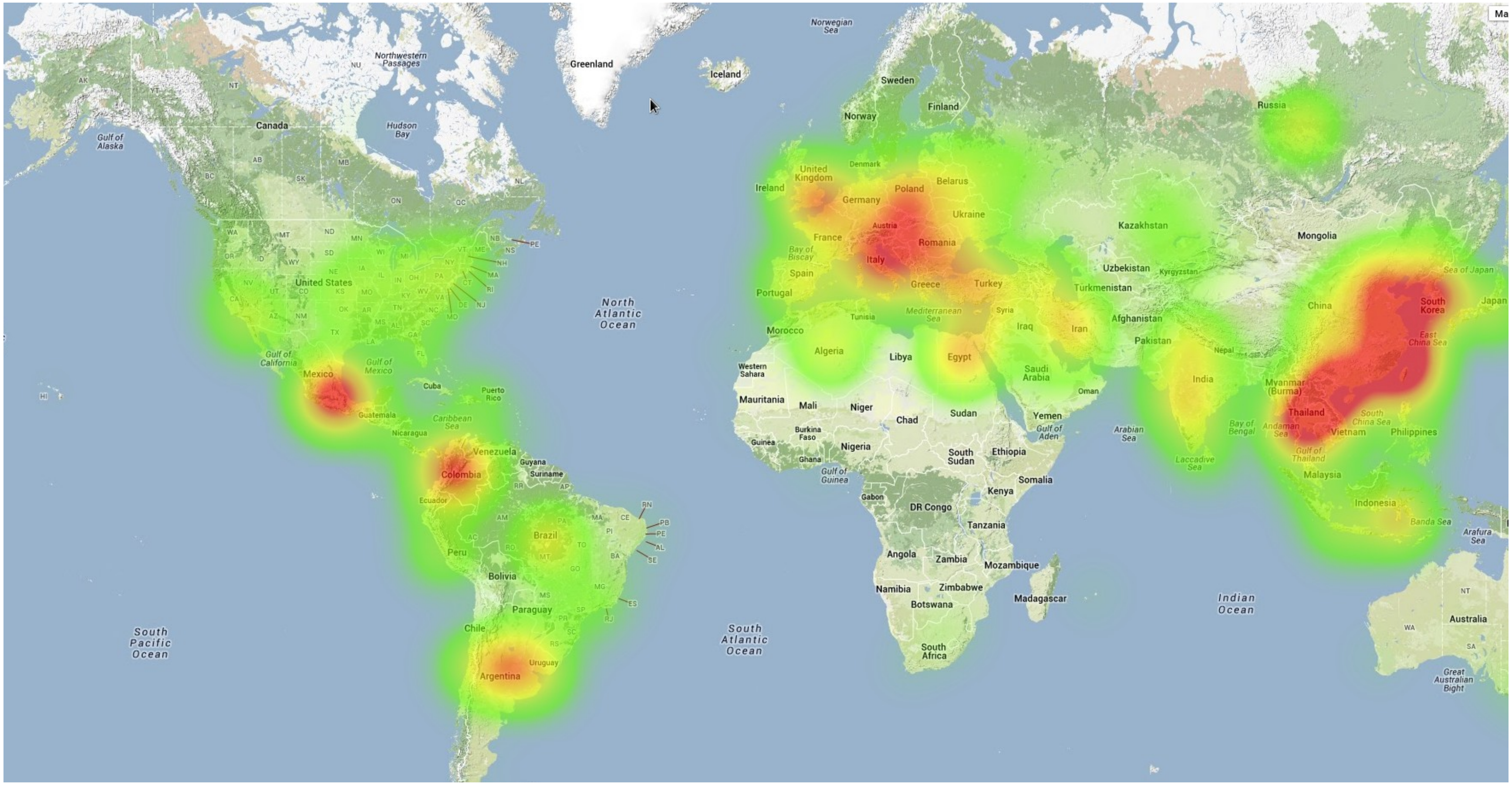
1 Attacker spoofs IP address of target. Sends queries to open home gateways.

2 **Open DNS proxy** forwards queries to ISP resolver

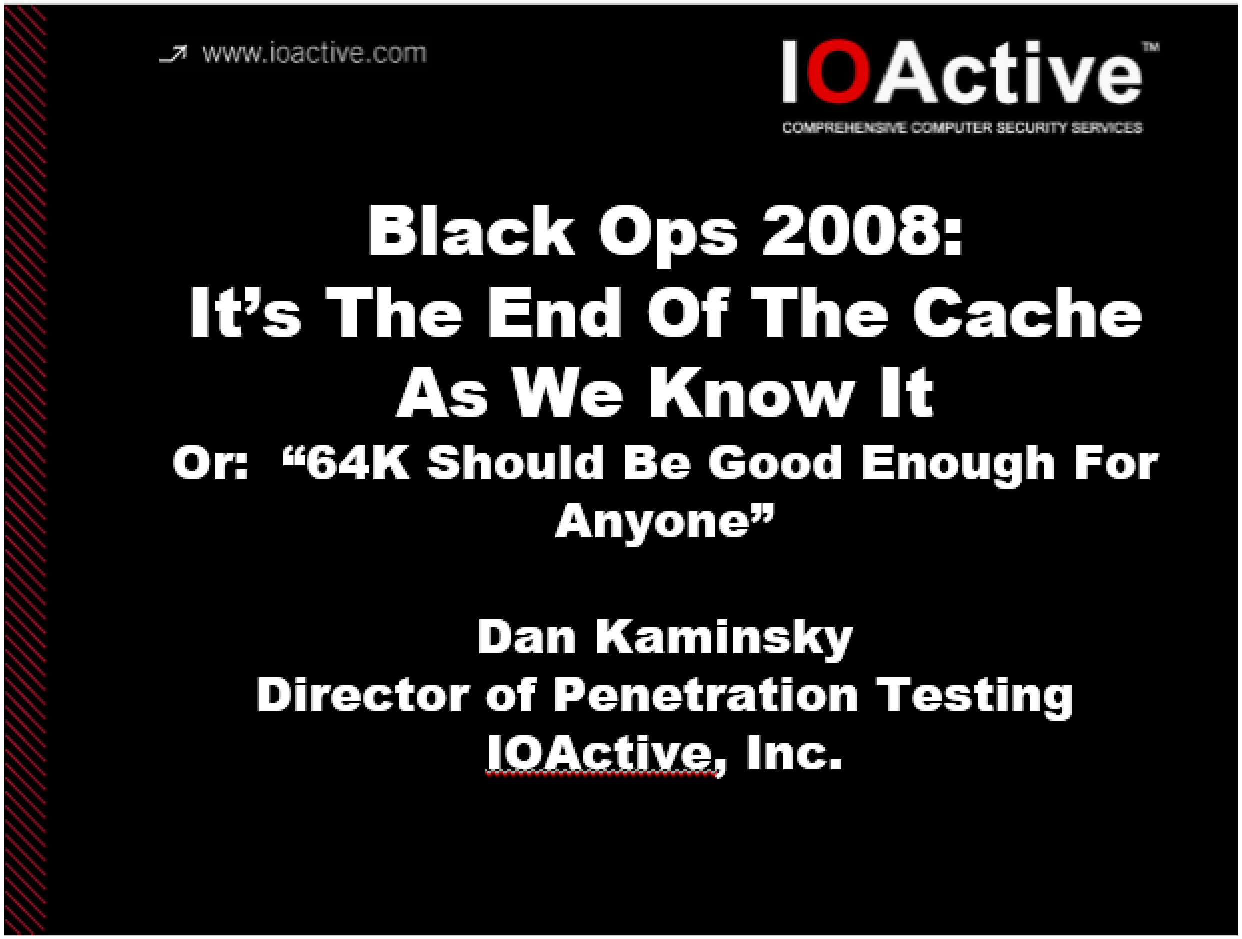
3 ISP resolver replies to proxy with amplified answer

4 Proxy forwards answer to target, floods it with DNS traffic.

Open DNS Proxies Globally



Other Uses for Random Subdomains



www.ioactive.com

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Black Ops 2008:
It's The End Of The Cache As We Know It
Or: "64K Should Be Good Enough For Anyone"

Dan Kaminsky
Director of Penetration Testing
IOActive, Inc.

Interesting Tension

A Perfect Storm?

✓ Open DNS proxies and resolve
✓ Infra for sending fake queries
✓ Lots of testing
? Infra for sending fake answers

- Minimally there’s DDoS exposure
- Potential cache poisoning exposure

Way Forward

- Data!   Logging is a “Good Thing”
  - We are starting to get response data
- Fast, automated detection
- Dynamic lists derived from fast detect
- Robust policy framework
- DNSSEC