

Frontrunning the Frontrunners

Dr. Paul Vixie, CEO Farsight Security, Inc.

© Copyright 2016 Farsight Security, Inc.
All Right Reserved.

Introduction

FORESIGHT SECURITY

Frontrunners Exploit Non-Public Information To Register Domain Names For Profit

- "**This Advisory considers the opportunity for a party with some form of insider information to track an Internet user's preference for registering a domain name and preemptively register that name.** SSAC likens this activity to front running in stock and commodities markets and calls this behavior domain name front running. **In the domain name industry, insider information would be information gathered from the monitoring of one or more attempts by an Internet user to check the availability of a domain name.**"

"SAC 022: SSAC Advisory on Domain Name Front Running," ICANN Security and Stability Advisory Committee, October 2007, [emphasis added] https://www.icann.org/en/system/files/files/sac-022-en.pdf

FORESIGHT SECURITY

Classic "Add Grace Period" Frontrunning Was Terminated By ICANN Policy Changes

- "In response to community concerns about the excessive use and abuse of the five-day AGP (Add Grace Period), **ICANN implemented two measures to address these problems that have resulted in a 99.7% decrease in AGP deletes from June 2008 to April 2009.** [* * *] The solution in brief means that if a company registers and then returns more than a certain number or percentage of domains each month, they are charged for each additional registration above that amount. The result is that domain tasting becomes increasingly expensive the more a company engages in the practice [...]

  "Aside from the problem that domain names may have been difficult to register, domain tasting also had a series of negative consequences on the manner in which people used the Internet. If individuals accidentally allowed their domain names to lapse, it had become extremely difficult for them to get the domain back (since it was being picked up and dropped by automated systems). Domain tasting also saw an enormous proliferation in the number of websites featuring nothing but advertisements, thus leading to a form of Internet graffiti."

  https://www.icann.org/news/announcement-2009-08-12-en

FARSIGHT SECURITY

DNS Query Failure Traffic As A New Potential Source of "Insider Information" For Frontrunners?

- We hypothesize that **recursive DNS traffic** collected from above caching recursive resolvers can also potentially drive (and/or expose!) speculative domain registration efforts.

- Admittedly, **DNS instrumentation normally focuses on domains that do resolve rather than domains that don't.**

- **In contrast, professional domainers need information about**
  - **(a) domain names that people hit, and**
  - **(b) which AREN'T registered.**

- **WHY do domainers need data?**

FARSIGHT SECURITY

Ad-hoc vs. Programmatic Registrations

- **Small-scale amateur domainers** may register a comparative handful of domain names:
  - Brainstorm a few names while watching TV or taking a shower.
  - Manually register those domains.
  - A*d hoc*/low volume/sporadic activity.
  - We're NOT very interested in these folks.
- **Professional domainers,** working at scale, tend to be much more **"data-driven"** -- and a bigger problem. They:
  - Identify domains based on empirical data sources, not just "hunches."
  - Programmatically register those names.
  - Do so for a material volume of domains on an ongoing basis.
  - **<u>These</u> are the people/companies we should be paying attention to...**

- **Does passive DNS have the data the professionals need?**

FARSIGHT SECURITY

Passive DNS Data Focuses on Successful DNS Queries

However, We ALSO Have Other Data on DNS Failures

- **Data about domain names that people cannot resolve (such as NXDOMAINS) would be golden for domainers.** They'd love to have that sort of data.
- **Farsight's not going to give them (or sell them) that data. Why? Well...**
- **Domainers hurt the Internet.** They increase costs for those who want domains for actual use, complicate life for search engines, and decrease the overall Internet signal/noise ratio. Domaining is a lot like email spamming.
- **We DO need to know if two hypothesized phenomena are occurring, however.**

FARSIGHT SECURITY

The Two Behaviors We Expect We'll See

1) **Volumetrically-driven typosquatting:** hypothetically, domainers may be:
   - Watching DNS query/response traffic
   - Tallying the volume of NXDOMAINs seen by domain, and then
   - Registering the highest volume domains for use in conjunction with online advertising programs.

2) **Programmatic exploration of domain permutations around high value existing brands:** "reconnoitering via DNS query."
   - The online analog of Vietnam-war era "recon by fire"
   - May be seeking available domains that a brand owner might be presupposed to buy for brand protection purposes.
   - May be looking for domains that can be used in phishing campaigns, or for spamming knock-off products

FARSIGHT SECURITY

Data From the Security Information Exchange

FORESIGHT SECURITY

The Security Information Exchange (SIE)

- Farsight Security may be best known for its passive DNS service, **DNSDB,** but Farsight also operates another service, the less-well-known **Security Information Exchange (SIE).**
- SIE is a set of physical locations where Farsight distributes **real-time streaming DNS data** as well as other security-relevant data received from an international network of hundreds of sensors.
- Cybercrime analysts or academic researchers can select specific SIE channels of interest, and then receive (just) those streams
- They can receive this data on a locally-attached system, or via an encrypted tunnel started from a remote system.
- While SIE is a commercial service, **Farsight provides free (or out-of-pocket-cost-recovery-only) grant access to vetted (but unfunded) "Internet Superheroes" working to independently combat cybercrime, and to approved university researchers.**

FARSIGHT SECURITY

The Two SIE Channels We Used

- **Channel 221 NXDOMAIN data**: This channel answers the question, "What (FQDN, rectype)-tuples do we see people trying to resolve that don't exist?"

- **Channel 212 Newly Observed Base Domains (NOD) data** answers the question, "What new effective-2nd-level ("base") domains did we just see for the first time?"

FARSIGHT SECURITY

1st Channel -- Channel 221: NXDOMAINS

- Volume: 15K observations per second (12-13 Mbps).
  1.3 billion observations/day. That's quite a few observations.
- **IMPORTANT: NXDOMAINS are VERY "specific" -- an NXDOMAIN for a (FQDN/RecType at time/date foo) does NOT imply that the underlying effective 2nd-level domain doesn't exist**
- ***NXDOMAINS is NOT just typos – it's also got LOTS of "junk"***
  - DNSBL traffic (query for a non-spammy host? ➔ NXDOMAIN)
  - Missing in-addr.arpa's (and ip6.int's, deprecated in **Aug 2005**)
  - Illegal/impossible domains (no dot, too long, illegal characters, leaking bogus or locally-made-up "TLDs"),
- Passive DNS does NOT currently incorporate NXDOMAIN data. You CANNOT just query Farsight's DNSDB (or any other passive DNS database) to see NXDOMAIN traffic. You MUST wrestle with SIE data.

Sample Obs From Ch221 In Presentation Format

[88] [**2016-06-07 19:01:03.560975962**] [2:6 SIE dnsnx] [a1ba02cf] [] []

qname: **ipv4_1-lagg0-c997.1.sjc002.ix.nflxvideo.net.**

qclass: IN (1)

qtype: **AAAA** (28)

response_ip: 204.13.251.30

soa_rrname: ix.nflxvideo.net.

bold=bita forming the unique tuple (FQDN, recordtype) at date/time

red=the bits of interest to this study

nflxvideo.net: already registered, even if "NXD'ing"

$ **whois nflxvideo.net**

Domain Name: nflxvideo.net

Creation Date: 2011-05-25T12:47:43-0700

Registrant Name: Domain Administrator

Registrant Organization: **Netflix, Inc.**

Registrant Street: 100 Winchester Circle,

Registrant City: Los Gatos

Registrant State/Province: CA

Registrant Postal Code: 95032

[etc]

NXDOMAINs do NOT mean the base domain is available to register! We MUST CHECK TO SEE IF A DOMAIN IS REGISTERED.

2nd Channel -- Channel 212 (Newly Observed Domains)

- Volume: roughly three observations per second
  - ~3 obs/sec*(60 sec/min)*(60 min/hr)*(24 hrs/day) = ~259,200 obs/day **(comparatively low volume/easy to process)**

- **2nd-level effective domains** ("delegation point") data: example.com, not www.example.com

- **Does NOT include domains first seen by Farsight in ICANN ZFA zone files**

- NOD's a pretty clean data stream

- NOD data DOES gets incorporated into DNSDB

Sample Obs From Ch212 In Presentation Format

[98] [2016-07-19 04:14:00.932154893] [2:5 SIE newdomain] [a1ba02cf] [] []

domain: **startjobs.xyz.**

time_seen: **2016-07-19 04:11:31**

bailiwick: xyz.

rrname: startjobs.xyz.

rrclass: IN (1)

rrtype: NS (2)

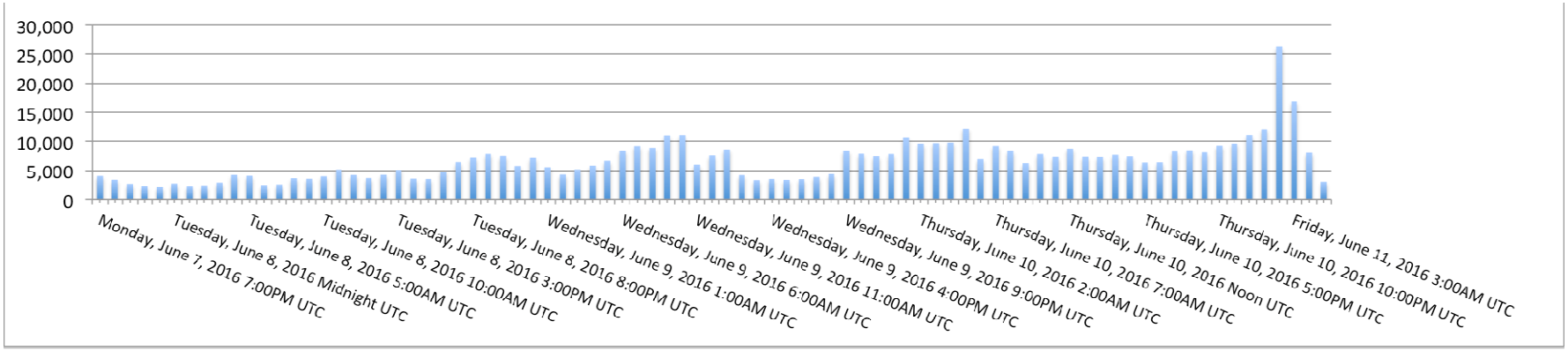
rdata: ns1.sedoparking.com.

rdata: ns2.sedoparking.com.

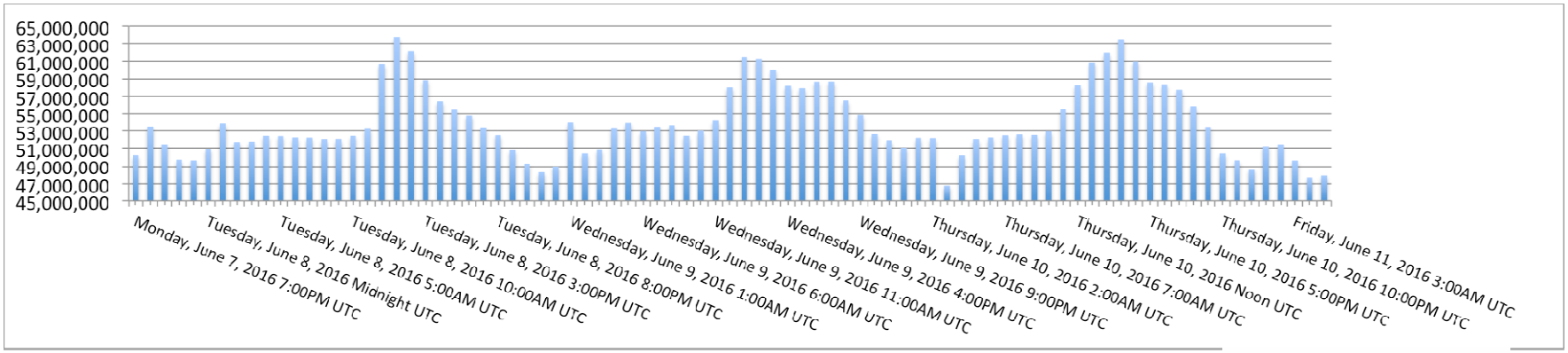
Note that this is likely an example of a monetized domain (Sedoparking is a parked-domain domain-monetization firm)

Extracted Obs Per Hour, Ch212 and Ch221, During The Data Collection Period (Note Diff Y-Axis Scales)

Ch212 (Newly Observed Domains)



Ch221 (NXDOMAINS)



FARSIGHT SECURITY

Hottest 2nd Level Domains From The Full Ch221 Data

440,096,845 **ip6.int**
121,874,848 **spamhaus.org**
110,977,781 **sophosxl.net**
107,574,211 **mcafee.com**
48,898,438 **sophosxl.com**
48,469,077 **2.ip6.arpa (RIPE NCC)**
35,907,658 **[large ISP]**
33,909,121 **spamcop.net**
28,726,297 **nflxvideo.net**
23,916,000 **104.in-addr.arpa (ARIN)**
21,220,352 **barracudacentral.org**
19,808,193 **surbl.org**
18,998,295 **intensive.int**
17,209,896 **sorbs.net**
16,007,599 **bondedsender.org**

14,902,090 **10.in-addr.arpa (RFC1918)**
14,055,285 **[large insurance company]**
13,637,914 **brightmail.com**
13,262,841 **habeas.com**
12,408,765 **isc.org**
12,368,645 **spameatingmonkey.net**
12,284,337 **mailspike.net**
11,181,446 **95.in-addr.arpa (RIPE NCC)**
11,058,385 **173.in-addr.arpa (ARIN)**
10,982,352 **17.in-addr.arpa (Apple)**
[etc]

These are NOT domains that the domainers COULD do anything with...

FARSIGHT SECURITY

Processing The NXDOMAINS

- We ended up with ~4.5 billion observations for Ch221.

- To be relevant to potential domainers, the 2nd level effective domain cannot be already registered. We need to check to find out if each potential domain is already registered, and that's **TOUGH** to do if we need to do it for ~4.5 billion domains.

- We MUST find ways to reduce the number of NXDOMAINS we need to check.

- "Good news:" NXDOMAIN observations have **lots of "junk"** we can dump....

We Can Drop…

- **Domains with Bad Characters**
  &(\001r\008\011mk\026bcl08\025 2016-06-07 19:19:22
- **Domains with Bad Formats**
  For example, labels that are too long (RFC 1035 2.3.4 says max label length is 63 octets)
- **Domains with invalid TLDs/no TLD**
  - 00004109a10090400000000000f01fec**.local**
  - **000fff11668b-home-controller-300**
  - What's determinative for valid/invalid TLDs? See http://data.iana.org/TLD/tlds-alpha-by-domain.txt
- **Duplicates/repetitive hits throughout the hour**
  - 0000.jp had 630 hits during one hour
  - Reduce the query load by ONLY checking for non-existence of the effective domain the FIRST time we see it... This is an intentional "simplification" -- the domain COULD get registered during the hour if it wasn't already...

Ensure Discovered Effective 2LD's Can Be Registered

- We need to ensure that an an interested party (such as a domainer) COULD register the effective 2nd-level domain shown in our NXDOMAINs observation, **IF they wanted to do so...** In some cases:
  - **The TLD might be closed except to some narrowly defined community** (example: dot int is reserved for nato.int and similar international treaty organizations, even if it is often used "informally" for "internal" domains)
  - **Some effective 2nd-level domain name might already be registered**
- **We repeat: just because you saw a domain name mentioned in NXD doesn't mean it's registrable for domaining purposes!**

What Do We Find?
Did Domains First Seen in NXDOMAINS Eventually Show Up Registered/Used in NOD?

FARSIGHT SECURITY

Reduce Scope and Winnow That Data Down...

- To keep this manageable, we're actually only going to look at a sample -- an hour's worth of processed NXDOMAIN data.

- We'll start with just 50,233,247 Channel 221 observations from a single hour

- We used a custom piece of code to remove ip6.int, ip6.arpa, in-addr.arpa, and some other "easy-pickin," "readily-cull-able" stuff, plus some illegal characters (!,#,etc) leaving 36,508,570 observations for further processing.

Having processed the entire hour's worth of NXDOMAINS, we ended up keeping 1,662,832 domains...

1,662,832/36,508,570*100=4.5% of the original

So the culling process worked, BUT it was slow, taking nearly four DAYS worth of processing time (single threaded) for just one *hour's* worth of Ch221 NXDOMAINS data...

We could run more parallel threads to speed that up, obviously. This is a nice example of the classic embarrassingly parallel problem (c.f., https://en.wikipedia.org/wiki/Embarrassingly_parallel).

We can also pre-filter more efficiently to reduce the number of domains to check.

Matching NXD Domains Against NOD Data

We then read in all 83 hours worth of NOD data, hoping that we'd see some of our 1,662,832 residual NXD domains eventually show up as having been newly registered in NOD.

We DID see that pattern, just not a lot. We saw 181 NXDOMAIN domains from CH221 subsequently show up as registered/used in NOD (Ch212).

That's not really very many... That may be:

- A **good sign** (people aren't culling names to register from NXDOMAINs), **or**
- It may be a sign that we can't see the phenomena: domains getting registered aren't getting hit within the first few days, **or** what's getting registered shows up in ZFA before we see it in NOD.

Sample Matches With NXD Time, NOD Time

23623viaortega.com	2016/06/07 18:59:04	2016/06/09 22:41:09
2de333fe8d257c3b07b176da743b35d0.org	2016/06/07 19:13:25	2016/06/09 0:13:45
488d9b5889ba01fc4a0015926945c0f5.org	2016/06/07 19:13:25	2016/06/08 0:12:43
4la3shezkt6r.com	2016/06/07 19:13:25	2016/06/08 0:11:57
505hostel.com	2016/06/07 18:59:31	2016/06/10 2:18:21
7wlibclab0py.com	2016/06/07 19:13:25	2016/06/10 0:09:53
7wpy34hu345y.com	2016/06/07 19:13:25	2016/06/08 0:11:57
abreforming.site	2016/06/07 19:00:38	2016/06/10 17:38:34
acardianmc.com	2016/06/07 19:05:04	2016/06/10 22:01:07
acegambling.xyz	**2016/06/07 19:07:34**	**2016/06/07 19:42:07**
amerirech.net	2016/06/07 19:23:55	2016/06/08 2:37:33
amountstraight.net	**2016/06/07 19:07:04**	**2016/06/07 21:31:55**
arivefloor.net	2016/06/07 19:00:37	2016/06/08 9:31:01
asapnow.xyz	**2016/06/07 19:54:17**	**2016/06/07 21:43:30**
aurenol.at	2016/06/07 19:27:13	2016/06/09 13:06:13
azmastergrower.com	**2016/06/07 19:04:44**	**2016/06/07 22:25:08**
bartholomewwinthrop.net	2016/06/07 18:59:35	2016/06/08 21:20:52
beatseemorearound.net	2016/06/07 18:59:39	2016/06/09 21:06:54
being.group	2016/06/07 19:04:09	2016/06/08 17:31:40
besttulsacondos.com	**2016/06/07 19:38:31**	**2016/06/07 23:26:28**

[etc]

➔ **[GREEN=showed up in NOD Relatively soon after seen in NXDOMAINS]**

FARSIGHT SECURITY

What Else In NXDOMAINS Do We See?

FARSIGHT SECURITY

Eyeball This List of Top NXDomains (From One Hour's Worth of NXDOMAINs Data): See How Fast It "Tails Off?"

1,842,849 spamhaus.org
1,301,461 sophosxl.net
928,353 mcafee.com
857,609 sophosxl.com
[major ISP elided]
426,533 spamcop.net
302,823 barracudacentral.org
274,890 surbl.org
266,065 brightmail.com
263,549 phishmongers.com
225,268 sorbs.net
217,585 intensive.int
205,159 bondedsender.org
192,874 nflxvideo.net

180,838 habeas.com
172,880 mailspike.net
147,415 webcfs00.com
145,143 isc.org
140,217 support-intelligence.net
135,593 spameatingmonkey.net
117,550 beeline.ru
107,424 rackspace.net
97,713 [major university elided]
87,540 com.belkin
85,307 edgecastcdn.net
82,334 surriel.com
74,921 us-east-1.elb.amazonaws.com
[etc]

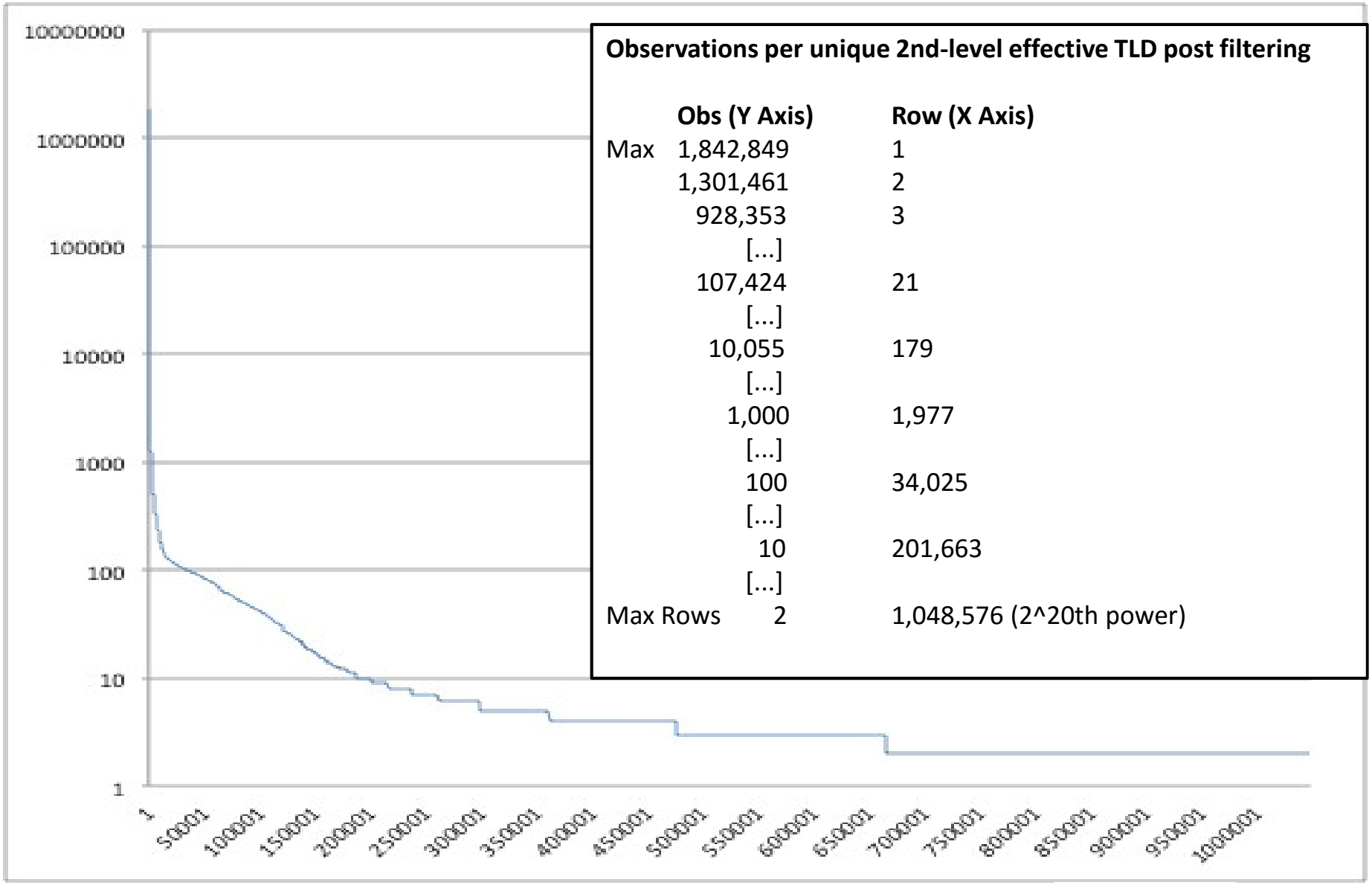
FARSIGHT SECURITY

High Volume NXD Base Domains Are Pretty Rare...

- We go from 1.8 million NXDOMAINS/hour in the case of spamhaus.org, all the way down to less than 75,000/hour in one slide's worth of domains.
- The drop off gets even faster after that. **See the graph on the next slide, and note the log-linear axes...**
- Within 179 unique effective 2nd level domains, you're down to only 10,000 NXDOMAINS/hour
- Within 1,977 unique effective 2nd level domains, you're down to 1,000 NXDOMAINS/hour
- Within 34,025 unique effective 2nd level domains, you're down to 100 NXDOMAINS/hour
- **That shows that "high volume" NXDOMAINS are pretty tightly distributed – there aren't a lot of them. Most 2nd level effective domains only attract a comparative handful of NXDOMAINs/hr**

FARSIGHT SECURITY

Distribution of Unique Effective 2nd-Level Domains



Observations per unique 2nd-level effective TLD post filtering

	Obs (Y Axis)	Row (X Axis)
Max	1,842,849	1
	1,301,461	2
	928,353	3
	[...]	
	107,424	21
	[...]	
	10,055	179
	[...]	
	1,000	1,977
	[...]	
	100	34,025
	[...]	
	10	201,663
	[...]	
Max Rows	2	1,048,576 (2^20th power)

FARSIGHT SECURITY

Some "False Positives"/"False Negatives" We Noticed, Too

[unavailable TLD – probably should filter .int, .mil, .gov, .edu, etc. outright]

intensive.int 18,998,295

ladco.int 585,486

axway.int 222,985

corp.int 174,797

pxl.int 156,083

[administratively filtered from DNSDB]

us-east-1.elb.amazonaws.com 6,057,472

us-west-2.elb.amazonaws.com 1,778,403

eu-west-1.elb.amazonaws.com 879,902

us-west-1.elb.amazonaws.com 418,916

We must ensure that we filter un-registerable domains (and domains that we administratively filter from DNSDB) out of our NXDOMAIN study data, too.

More Unregistered "Top NXDOMAINS"
... But These Are Unlikely to Attract Many "Typos"

jjetwqy.com 183,903
lzeaeac.ru 179,271
enyzyeq.ru 179,125
bjqlscz.ru 179,019
qlpyewm.ru 178,846
lnjgukh.ru 178,340
kdcmwuz.ru 178,269
dpyabij.ru 178,221
ryorpcr.ru 177,940
qbasipa.ru 177,872
lutmkwr.ru 177,794
bllpkrp.ru 177,721
jxevrvv.ru 177,551

jzgjldk.ru 177,432
coqqtuy.ru 177,427
othihmm.ru 177,403
uqhbgyb.ru 177,321
klcgduk.ru 176,942
swsad.com 176,671
qeprhiu.ru 176,651
gmdqfbb.ru 176,315
uvttrpa.ru 176,260
mcuyfnh.ru 176,231
rqtcxnh.ru 176,213
usildbq.ru 176,210
mefzluk.ru 175,996

whtjpzk.ru 175,966
cxabxmn.ru 175,908
trawxsf.ru 175,414
hnizvkjk.com 145,641
ovjelvjn.com 145,578
txyuybax.com 145,532
odhpdtov.com 145,459
opfuuixw.com 145,093
etrhqdfy.com 145,076
irpnyppz.ru 144,063
juzviyxs2.ru 143,740
lwdlkcgy.ru 143,570
[etc]

FARSIGHT SECURITY

Maybe All The "Good NXDOMAINS" Are *Already* Gone?

- If domainers have already been watching DNS traffic, as we hypothesized, **we wouldn't EXPECT to see lots of really juicy "typo bait" left just waiting to be registered – it presumably would have already been noticed and monetized**

- **However, have we just managed to find a way to identify DGA domains? Is much of the higher volume NXDOMAIN traffic actually BOT-related?**

- ***Rhetorical question:*** Should we register and sinkhole these and see what hosts check in over time?

Could You Make A Living As A Domainer Off "Crumbs?"

- Many of the highest volume NXDOMAIN-generating domains appear to be already be registered or impossible to register.

- However, could you cover your costs and make a profit by registering lots of lower-popularity domains?

- Potentially, but it's not my intent to encourage domaining. We'll let the domainer's figure that out based on what they can figure out a way to see...

High Value Brands Seen In NXDOMAIN Traffic

FARSIGHT SECURITY

"Recon By Fire"

- Remember that we also suggested that some popular brands might be targeted for "recon by fire", or probes for unregistered variants of popular names.

- Given our limited time, let's just consider one example where NXDOMAINS may still be interesting to security people, as a heads up about what may be coming, or what might make sense to target for a defensive domain name registration.

- Let's look for domains related to the substring "payp"

Some Selected "payp" NXDOMAIN base domains

accont-paypal.com
cgq-paypal.com
clickpaypal.com
email-support-paypal.com
es-paypal.com
gewerbe-paypal.com
guangzhoupaypal.org
handbagpaypal.com
inbox-paypal.com
infoaccountpaypal.tk
iservicepaypal.com
m-paypale.com
my-paypal-account.net
mypaypalshopping.tk
noreply-paypalmail.com
onlinestatus-paypal.com
oo-paypol.co.uk
papaypals.com
paypaal-limitedd.com
paypai.com
paypail-confirmed.com
paypaill.tk
paypaiservice.ml
paypal-account-recovery.com
paypal-accounts.net
paypal-auth.com
paypal-cgn-bin.com
paypal-com-update.cf
paypal-confirmations.ga
paypal-ee.com
paypal-global.ml
paypal-inc-secure.com
paypal-limitation.gq
paypal-mail-secure.com
paypal-merchent.com
paypal-onlinestatus.com
paypal-police.com
paypal-securecenter.us
paypal-selfhelp.com
paypal-service.info
paypal-services.ml
paypal-sicher.eu
paypal-sicherer.de
paypal-sichern.eu
paypal-sr.com
[etc]

Some Selected "payp" NXDOMAIN base domains (cont.)

paypal-suport.co.uk
paypal-unlimidation.com
paypal-update-info.eu
paypal-update.gq
paypal-view.com
paypal-webrsc.com
paypal-you.com
paypal.om
paypalclients.net
paypall-services.com
paypallaskl.com
paypalobjetcs.com
paypalresolve-login.com
paypalservice-info.com
paypalsupportss.com
paypalsystem.com
paypaltojapan.com
paypaluddates.com
paypalupdate.tk
paypalupdateservice.tk
paypapcredit.com
paypl-connection.com
paypl-limit.com
payplservices.com
redirect-securepaypal.gq
scure-paypal-lnc.gq
secure-paypai.com
secure-paypeil.com
securiry-paypal.com
securityintlpaypal.com
signinpaypal.com
signup-paypal.com
support-paypali.com
update-paypal-accounts.com
usa-paypal.com
verifity-paypal.com
veriification-paypal.com
www-paypael.com

FORSIGHT SECURITY

Some of Those Domains Might Be Innocent

- I'd be willing to bet, however, that **some of those domains are NOT innocent,** and you will be seeing them again, under unsavory circumstances.
- Wouldn't you rather know about then in advance?
- You should be watching NXDOMAIN traffic!

- **Are there other security-related reasons why you should be watching NXDOMAINs?**
- **Yes: it might help you spot DDoS attacks.**

The Distribution of TLDs: Something Odd...

FARSIGHT SECURITY

An Interesting Anomaly: Volume By TLDs in Ch221

59,233,002 co
58,678,751 rs
57,628,777 il
15,601,516 com ***[Baseline for gTLDs]***
5,283,561 dlink *[An INVALID TLD]*
4,122,552 ru
2,019,325 uk
1,936,868 home
1,252,101 net
798,756 org
590,990 info
579,536 lan
554,598 us
553,504 localnet
470,943 cn
441,932 ca

400,226 de
379,458 asus
363,750 biz
265,937 xn--p1ai
254,002 eu
229,278 fr
228,079 ampedwireless
226,923 nl
199,791 cisco
197,359 ch
169,027 br
151,683 at
148,371 be
141,897 au
138,393 ua
[etc]

FORSIGHT SECURITY

Surprising To See .rs, .co, and .il As The Top TLDs

- Generally speaking, we'd **not** expect those particular ccTLDs to be the top TLDs seen in the NXDOMAINs channel (and by a substantial margin at that).

- Farsight does not disclose the geographical distribution of its global sensors, however we can say that there is **not** a particularly dense deployment of sensors in Serbia, Colombia or Israel that might account for this sort of skewed domain distribution.

- Closer inspection of the traffic makes it clear that this is likely **not** organic traffic primarily associated with end-user errors; potentially that traffic looks like DDoS-related to us...

Examples of Some Unusual .rs Domains We Saw

Vast majority of our .rs domains were seen only once, and looked like...

201ny42yvx5kvlmiviejxqgrtdei1fmrvmbrmcgfrcwwrtrrdcciim5bcw**.rs**
201nze3wjyt1h28hvakzssd9h5yib7edvaj5px7koxidc560knocpcbngxpap**.rs**
201oqdcegyhfr8jlaegdan8d0ytaiim1rgjnakrljqsybjggnicmeduhdmb5wow**.rs**
201phnf8wqgx2pj2zyr8tziamogejkxkcq4jikqrlxulqptzewevge9zio6lgln**.rs**
[etc]

or

20160224104304**.rs.**
20160224104446**.rs.**
20160224104659**.rs.**
20160224104453**.rs.**
[etc]

FARSIGHT SECURITY

Can We Tell Who's Being Targeted by That Traffic?

- Because we collect above the recursive resolver, as a general rule, **you cannot see an individual end-user's system's IP address**. You cam, however, see the large recursive resolvers that may be answering on his or her behalf as an apparent query source.

- In this case, however, **the condensed format that SIE NXDOMAINS employs does not include the apparent query source,** so you can't localize this potential attack traffic even to the large recursive resolver contributing the data.

- **The recursive resolver seen making the query IS available in another SIE Channel, Channel 220, "DNS Errors,**" however our terms of service preclude you from bothering (or disclosing the apparent identify of) our sensor operators.

Conclusion

FARSIGHT SECURITY

Key Takeaways

1) NXDOMAINS may not be particularly fruitful for frontrunners (must admit, that doesn't exactly make me sad...)
2) However, we did find out that NXDOMAINs may be terrific when it comes to finding:
   - Potentially-suspicious DGA-related domains
   - Domains potentially involved in distributed denial of service attacks, and
   - Potential phishing or mark-infringing sites being reconnoitered prior to an attack
3) **You should be paying attention to domains that don't resolve**
4) **You can probably build far better tools to grind NXDOMAINs data – maybe you'd like to give it a try?**

Questions?

- Thanks for the chance to talk today!
- Are there any questions?
- Contact information:

Dr. Paul Vixie

vixie@fsi.io