



# Passive Detection of Misbehaving Name Servers

Based on CMU/SEI-2013-TR-010

*Jonathan Spring, Leigh Metcalf*  
netsa-contact (AT) cert.org  
NANOG 59, Phoenix



## NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

# Fast Flux – so last decade

---

- In early 2008, the ICANN SSAC detailed fast flux networks<sup>†</sup>
- In case you've forgotten:
  - One domain uses multiple IPs
  - Optionally, one IP hosts multiple related domains
  - If both, we have a malicious CDN

<sup>†</sup> “SSAC Advisory on Fast Flux Hosting and DNS.” ICANN TR# SAC-025.

# So why am I talking about this now?

---

A bunch of people talked about fast flux domains for delivering malicious software and add redirection

Standard approach: find and block the domains

Realization: Whack-a-mole is tiring.

Second realization: Whack-a-mole is actually impossible to win

- If you want more about this, ask about my APWG eCRS paper just published (*Modeling Malicious Domain Name Take-down Dynamics: Why eCrime Pays*)

# How can we jump out ahead?

---

Domains need two things:

- Location (A, AAAA, or CNAME)
- NS

IP works fine reactively, and reputation for some AS

But it's hard to jump out ahead

Name servers, then!

# Two sources

---

## Zone files

Pro:

- Complete for the zones we have

Con:

- Only have gTLDs (by policy), updated daily

## Passive DNS

Pro:

- Visibility across TLDs, finer time resolution

Con:

- Incomplete; no data until someone issues the query

# Process

---

- Look for name servers that move IP addresses.
- Map IPs to ASNs, and look at IP changes that also change ASN.
- Since NS are more stable, the parameters for “fast” flux need to be adjusted.
- This is the key point – NS are by definition stable. In a CDN, Akamai e.g., each *NS* does *not* change IP.
- They may change what NS you point to, but the NS is stable.

# Surprise!

---

There are suspicious name servers



# In Zone Files

(2011)

# Changes	# NS change IP	% of total	# NS change ASN	% of total
0	2734327	97.8%	2754332	98.5%
1	52741	1.9%	36645	1.3%
2	4855	0.2%	1846	0.1%
3	551	0.0197%	635	0.0227%
4	198	0.0071%	838	0.0300%
5	233	0.0083%	531	0.0190%
6	482	0.0172%	500	0.0179%
7	660	0.0236%	401	0.0143%
8	706	0.0252%	224	0.0080%
9	607	0.0217%	30	0.0011%
10	478	0.0171%	19	0.0007%
11	138	0.0049%	9	0.0003%
more	152	0.0053%	118	0.0041%

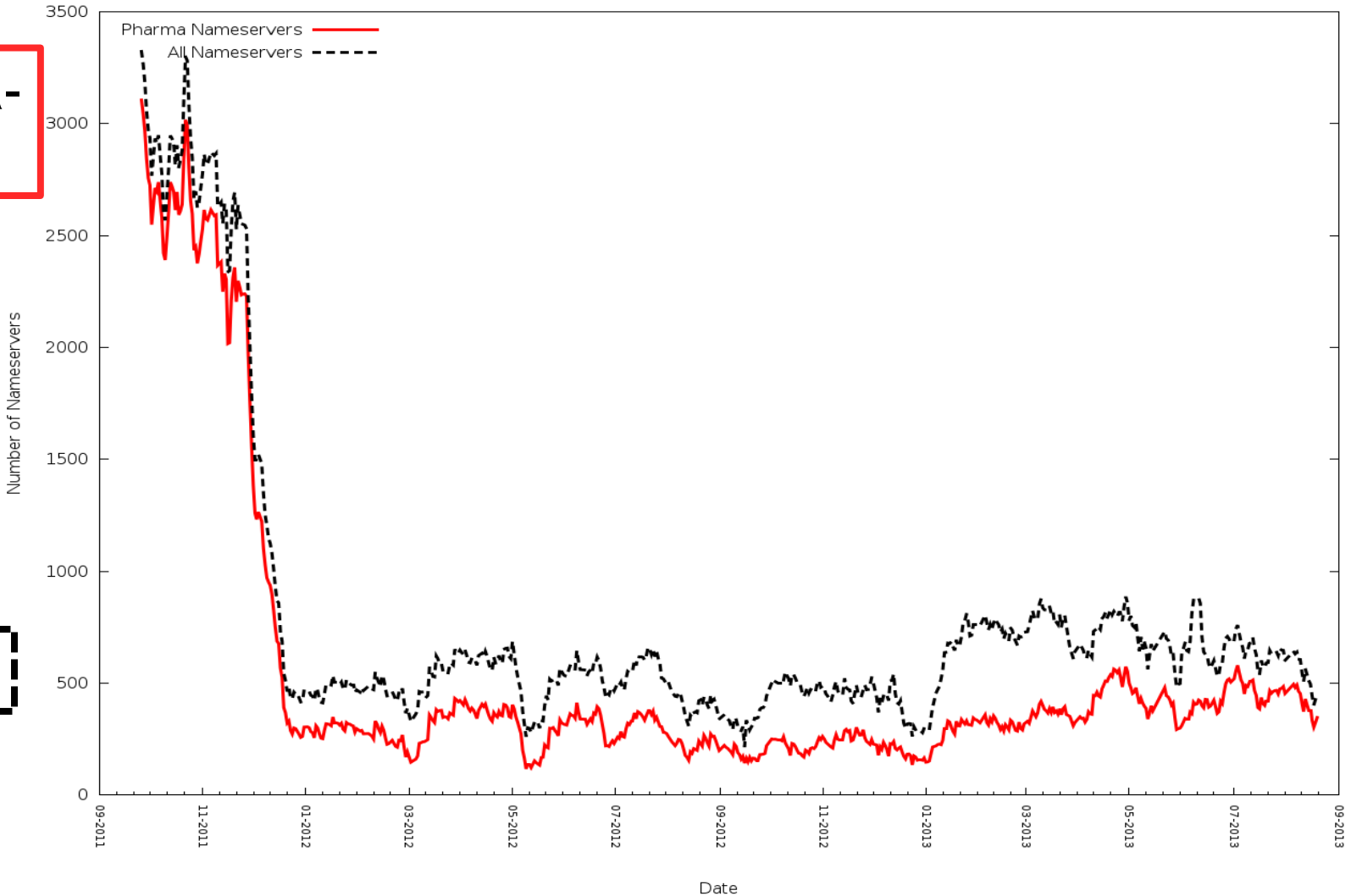
# In Passive DNS

(2011)

# Changes	# NS change IP	% of total	# NS change ASN	% of total
0	1846152	95.8%	1877654	97.5%
1	68401	2.4%	40422	1.4%
2	5134	0.2%	3276	0.1%
3	1420	0.0508%	1232	0.0441%
4	1177	0.0421%	966	0.0345%
5	1123	0.0402%	684	0.0245%
6	566	0.0202%	450	0.0161%
7	535	0.0191%	388	0.0139%
8	439	0.0157%	279	0.0100%
9	322	0.0115%	220	0.0079%
10	248	0.0089%	152	0.0054%
11	140	0.0050%	76	0.0027%
more	710	0.0254%	568	0.0204%

# Following this out 2 years...NS that changed IP 5+ times within 30 days:

Pharma-related



All NS

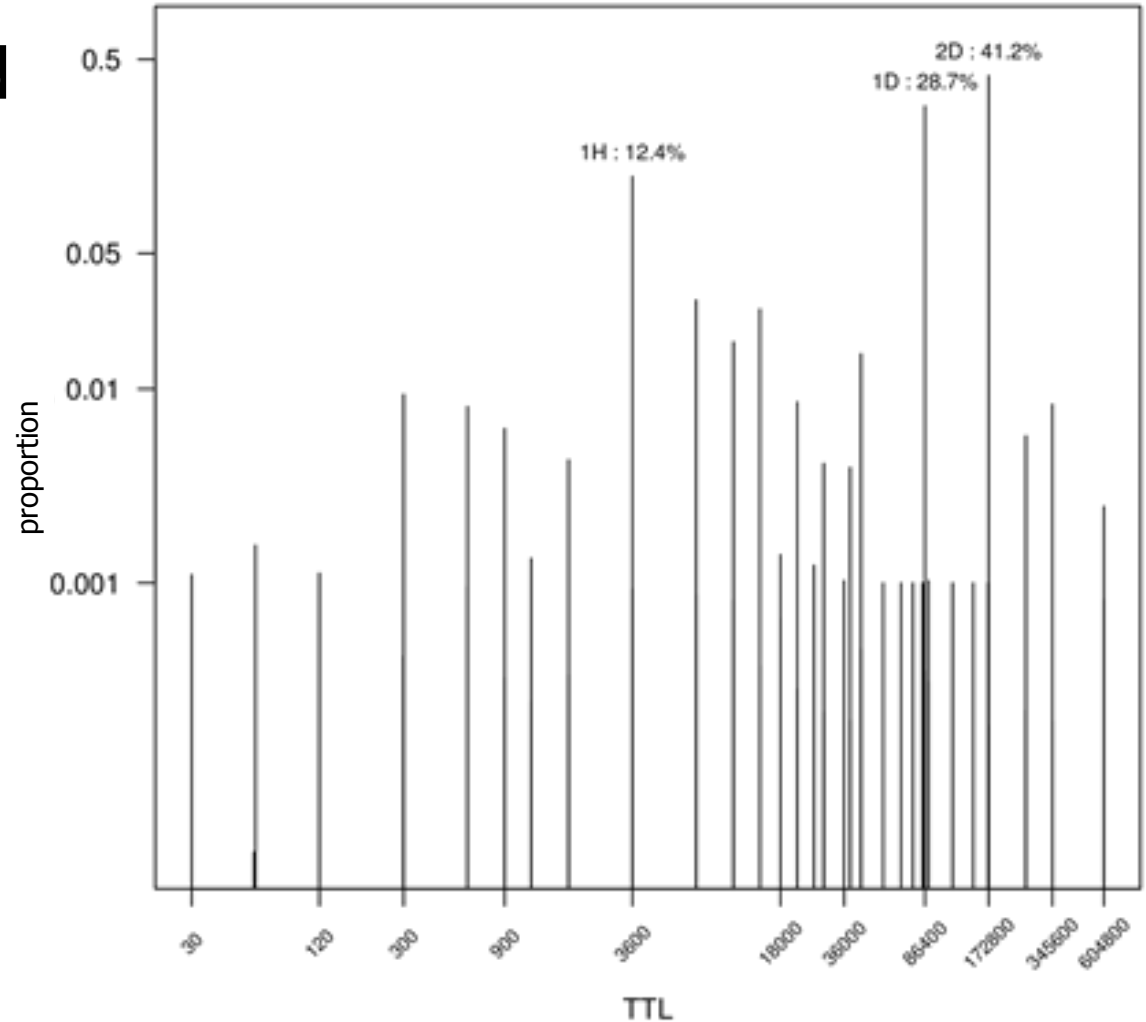
# Is the flux really fast?

Well, no.

But most NS record TTLs are quite long.

Note *log-log scale*.

82.3% of pDNS TTLs are 1 of 3 values [1 hour, 1 day, 2 days]  
(760M records)



# So what?

---

- NS flux is rather slow
- But a high confidence indicator.
- Also, blocking the NS has a bigger effect than blocking a single domain.

I don't think anyone looks at this in order to block things. Does anyone here? Has anyone tried and not had success?

# Future Work

---

- I could try to “Prove” that these NS are bad
- I can’t run incidents to ground at Internet scale, but I could try taking a sample.
- And intersecting with a dozen or more black lists is, surprisingly, not necessarily fruitful (Another CERT white paper in press, CERTCC-2013-39, demonstrates this)
- Continue to keep track of this, for awareness of badness.

# Hope

---

It'd be nice if registries could put rules on zone file changes that looked for this and nipped it in the bud

- In the mean time
  - You can keep track of this at your NS and prevent it from talking to these suspicious ones
    - (RPZ, firewall, etc.)



**Questions/comments?**

