An Open Resolver View of the New York Times Very Bad Day

Duane Wessels

OARC Fall 2013 Workshop

About This Talk

- What can Open Recursive Name Servers tell us about purging bad data from DNS caches around the Internet?
- To get a sense of the scale of the problem.

- Not about:
- Registrar hacking.
- Registry Lock.
- Automatically purging bad data.

The Hack

- August 27th between 1800-1900 UTC.
- Invalid registration data for nytimes.com (and others) inserted at the registrar level.
- NS records changed.
- Visitors to nytimes.com see a “hacked” web page.
- DNS-wise:

```
;; QUESTION SECTION:
;nytimes.com.                   IN      NS

;; ANSWER SECTION:
nytimes.com.            84349   IN      NS      ns1.syrianelectronicarmy.com.
nytimes.com.            84349   IN      NS      ns2.syrianelectronicarmy.com.
```

The Plea

Date: Tue, 27 Aug 2013 16:55:19 -0500
From: "david@--------.com" david@--------.com
Subject: [dns-operations] Request To Clear Cache: NYTimes.com

All,

I am a DNS Administrator at NYTimes.com. Earlier today we had issues with our registrar updating our NS records on the root servers to a malicious site. The registrar has since locked our domain with the registry on our proper Name Servers. We have had reports that the malicious site that our domain was redirected to was infecting users with malware. It would be a great service to the internet if everyone could please clear their cache for NYTimes.com. I understand that several other large websites/domains are experience the same thing. I would not be surprised if several request like this come in over the list today.

Thanks,
David Porsche
Systems Administrator
The New York Times

VERISIGN

The Big Idea

- Let’s ask the Internet’s Open Recursive Name Servers what they know about nytimes.com.

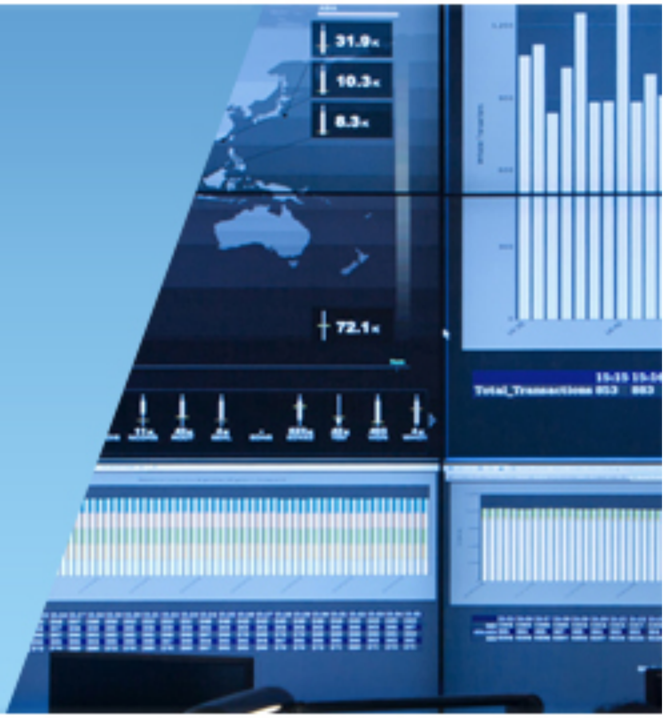
- Approx 33,000,000 ORNS!
- Not a static set – we’ll just query every IPv4 address.

- Scan started at 2013-08-28 00:18 UTC.
  - 6-7 hours after registrar incident.
- Scan completed 11 hours later.

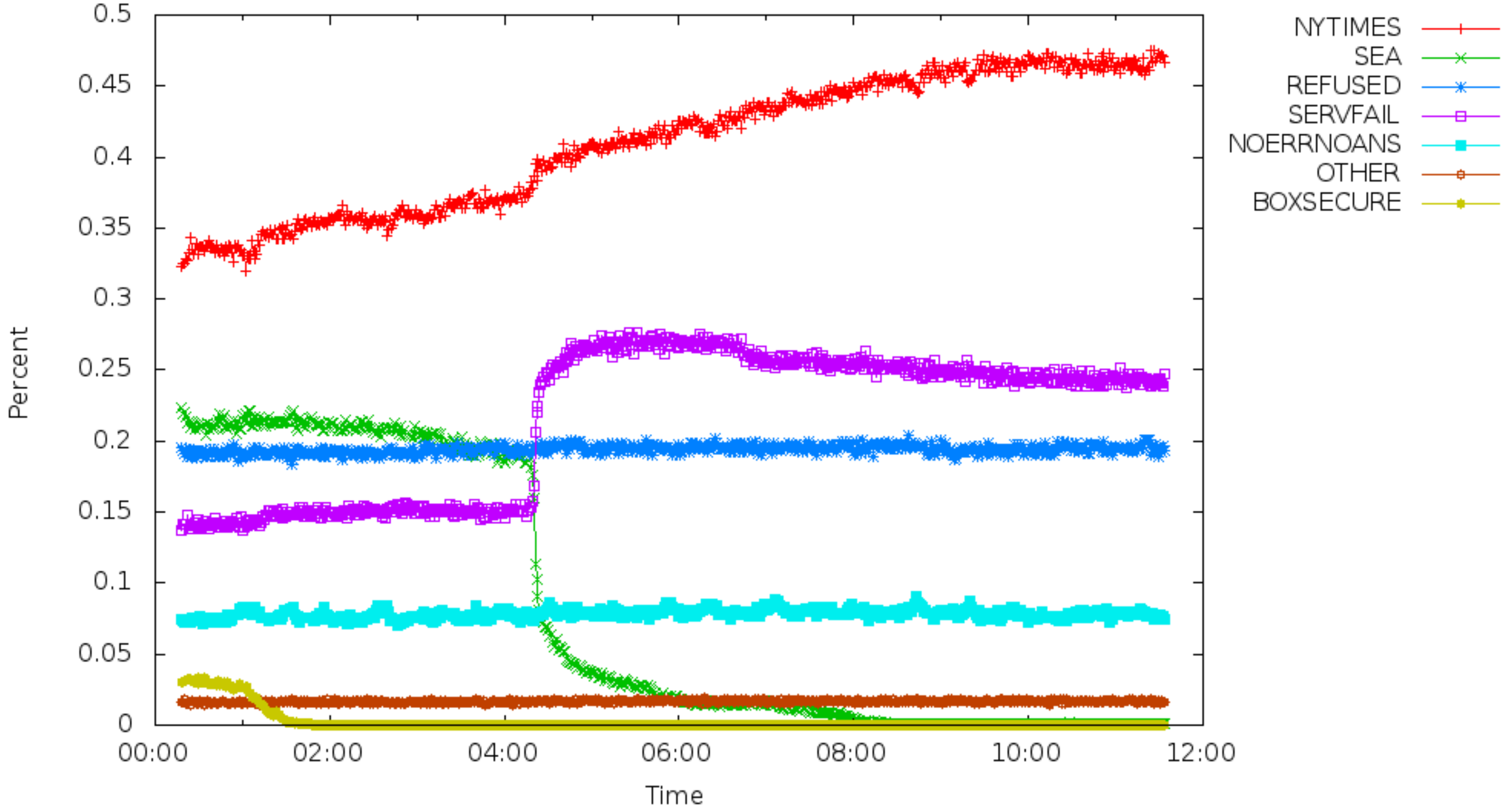
Concerns

- Does this scan impose a significant burden on nytimes.com name servers, when it is trying to recover from the incident?
- Unlike a traditional ORNS scan, here the query name is constant and subject to caching.
- From previous surveys we know all ORNS forward through approximately 300,000 shared caches.
- 300,000 / (11 * 3600) = 7.5 q/s

Results



How do Open Resolvers answer queries for nytimes.com?
Shortly After Attack

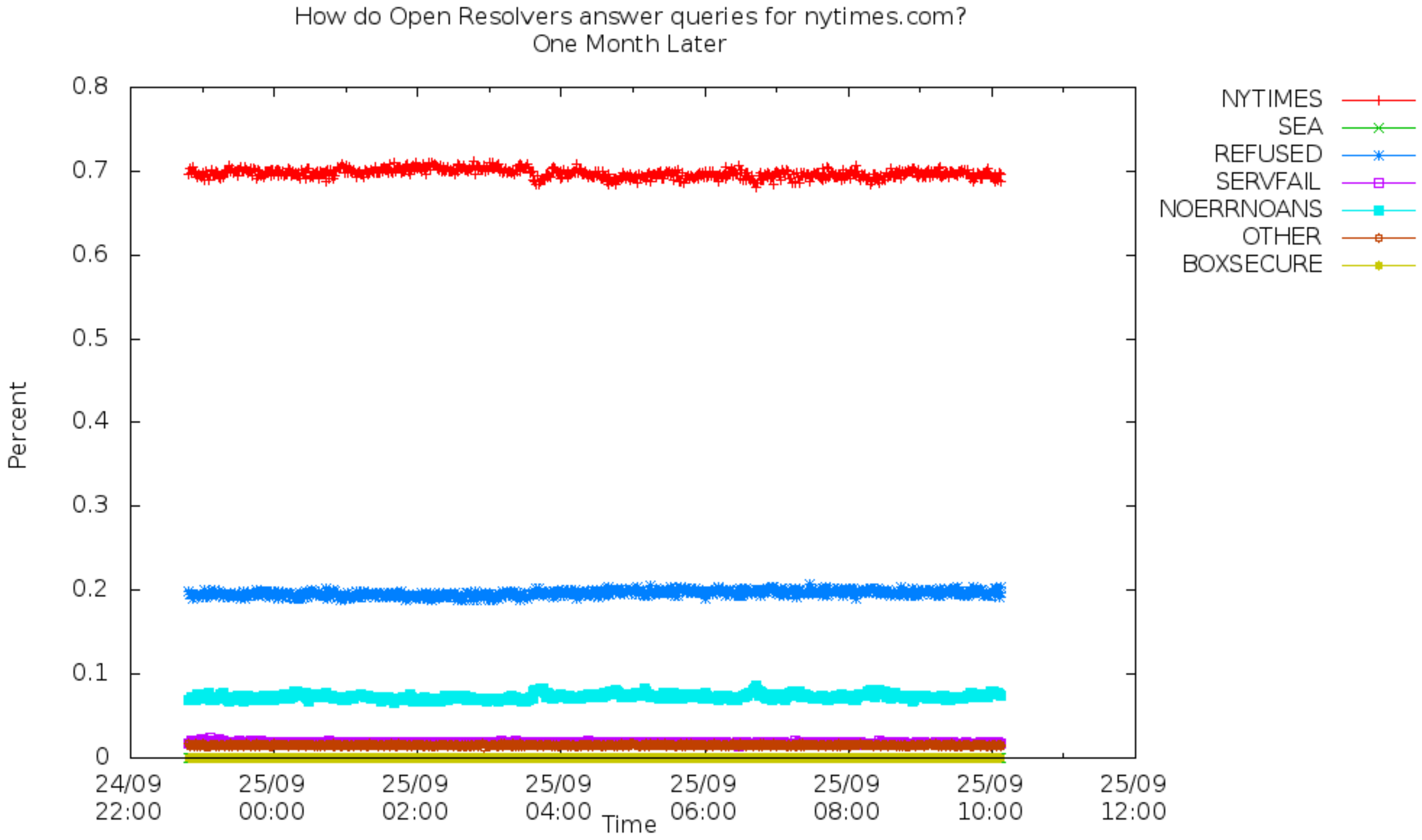


Results

- Percentage of ORNS returning correct data went from 35% to 45% over the course of the scan period.
- “boxsecure” is the first site that nytimes.com was redirected to. A few ORNS have it cached still at the start.
- “SEA” is the second site that nytimes.com was redirected to. It persists in ORNS caches until about 04:30 and then drops off noticeably.
  - Queries that were resolving to SEA become SERVFAIL at this time.
  - Probably syrianelectronicarmy.com was deleted from the com zone at this time.
- There is a constant amount of REFUSED and “No Answer” responses which are probably unrelated to the attack.

How does this compare to Normal?

- Since we don’t have data from before the attack, we ran the scan again one month after the attack for a baseline comparison

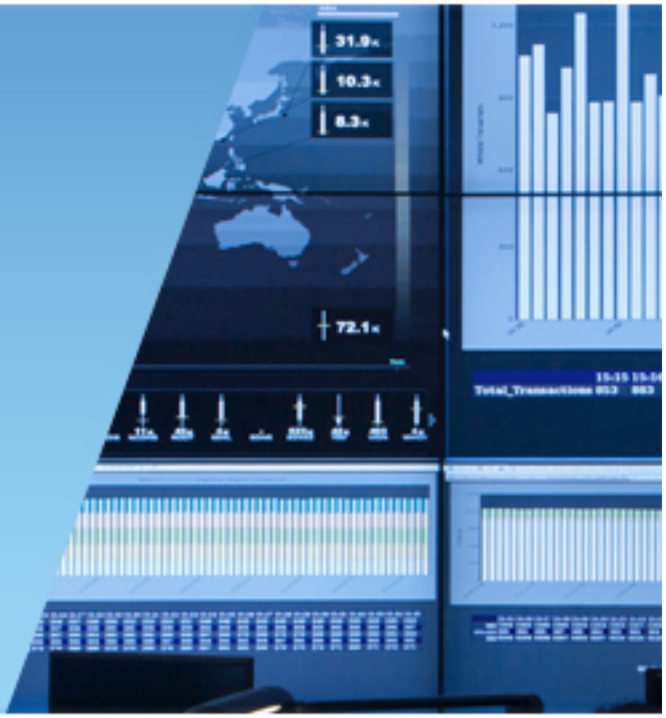


How do Open Resolvers answer queries for nytimes.com?
One Month Later

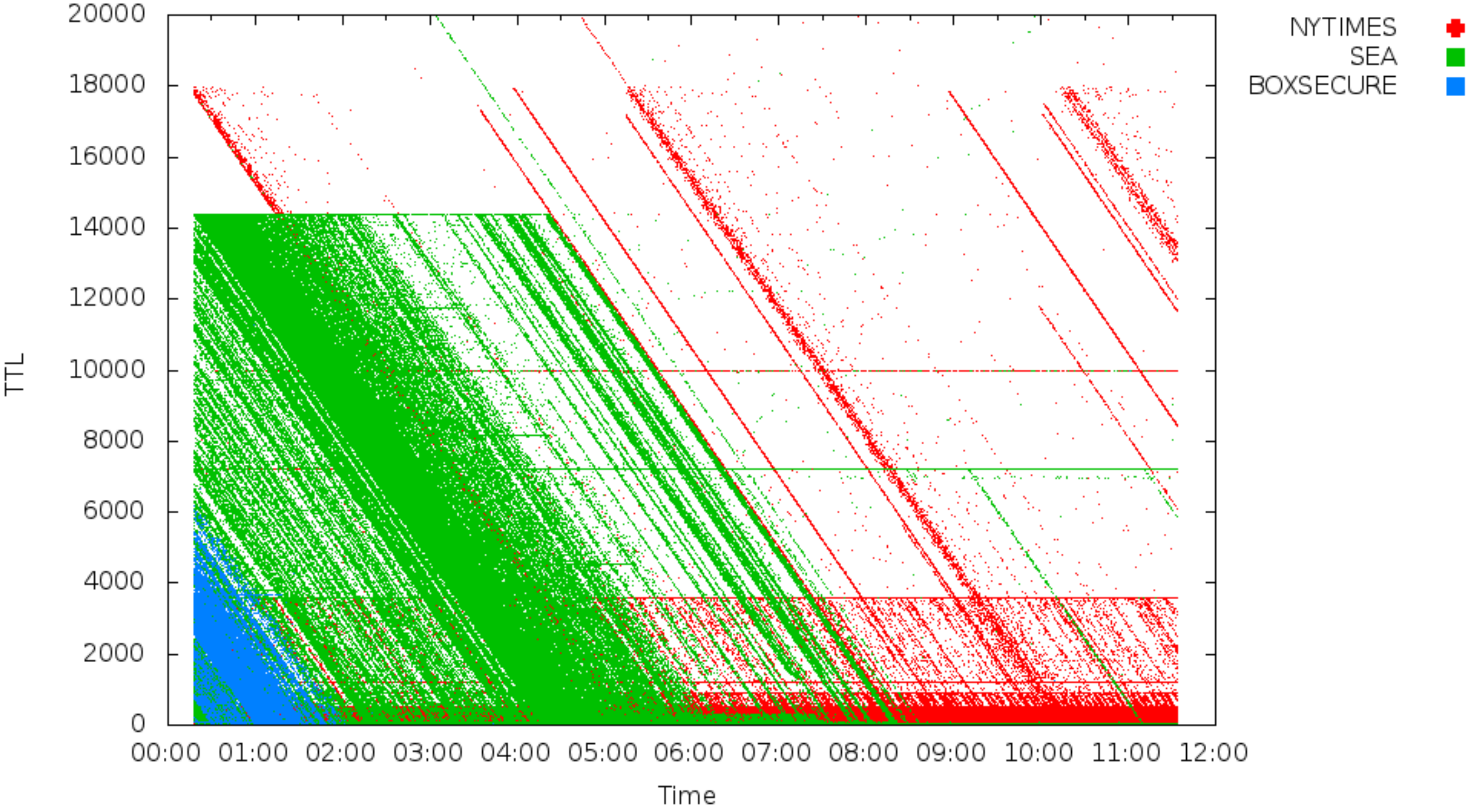
Any lingering effects one month later?

- 545 ORNS responses with SEA IP!
  - Mostly with very long (15 month) TTLs
- 3 ORNS responses with Boxsecure IP!

Time To Live Values



TTLs returned by Open Resolvers for nytimes.com
Shortly After Attack



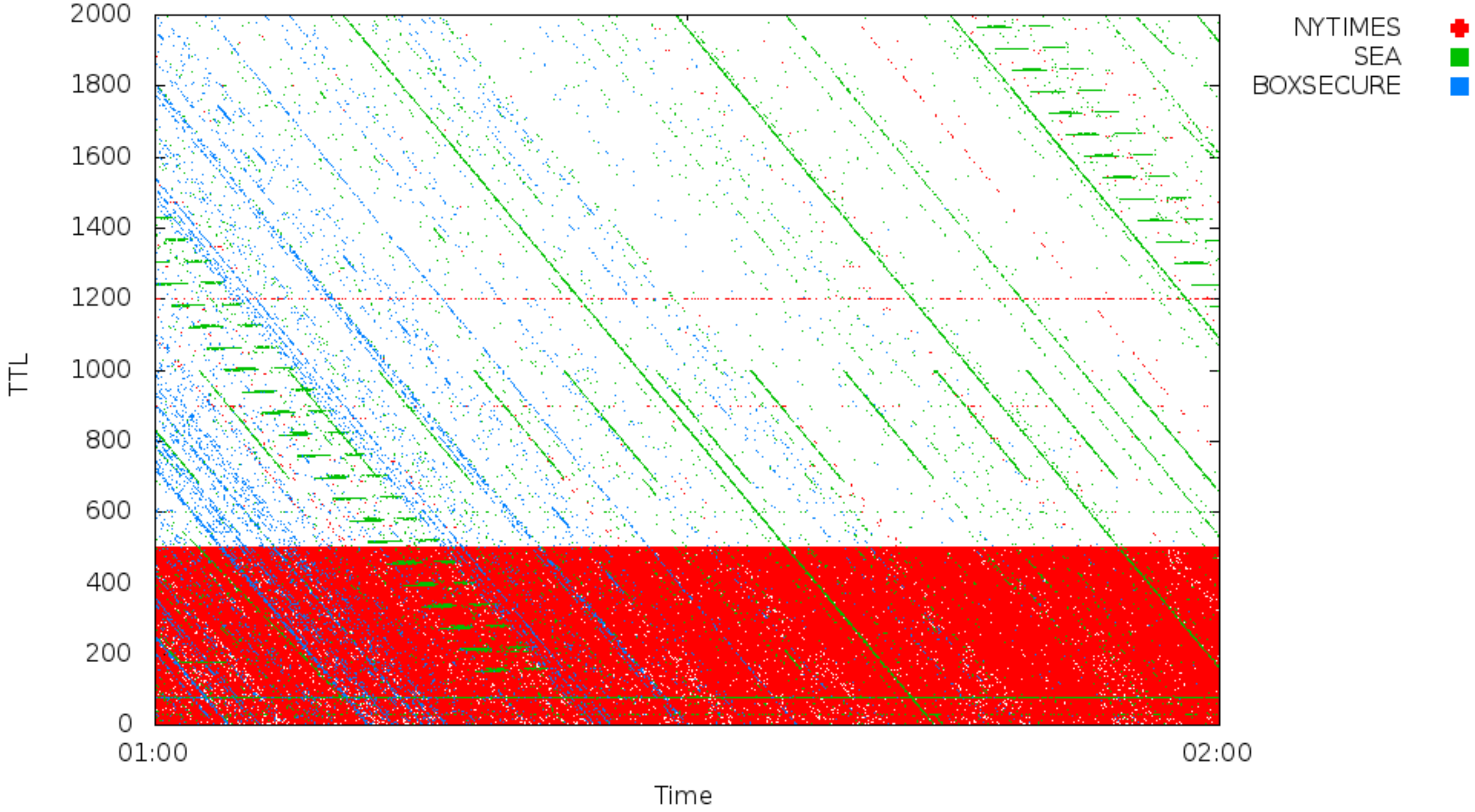
TTLs

- We know from previous research that many ORNS forward queries to shared caches. Here the strong diagonal lines show that very clearly.
- The red points indicate “good” data while the green and blue indicate “bad” data. These are “A” records.
- Data points along horizontal lines most likely indicate uncached responses. The TTL for the “SEA” records appears to be 14400 seconds (4 hours).
  - It appears that bad data was still entering caches until 04:30 UTC.
- NS records likely had much longer TTLs.
  - Even though problem was fixed in the registry, bad A records could be reloaded until bad NS records expire.
- Horizontal green line at 7200 seconds – TTL limiting?

TTLs

- Let’s zoom in….

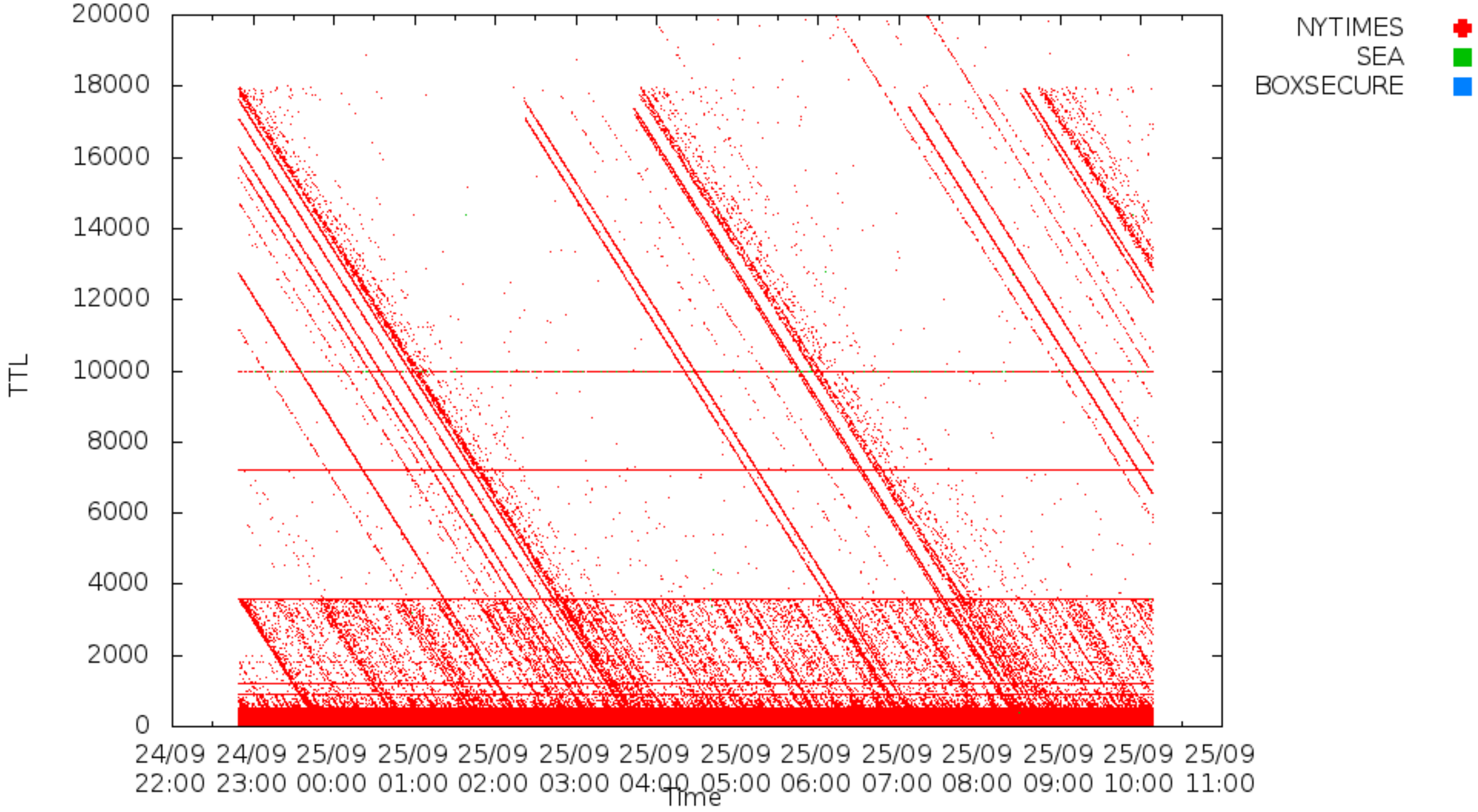
TTLs returned by Open Resolvers for nytimes.com
Shortly After Attack



Zoomed TTLs

- The dense red area represents good data with short (500 second) TTLs.
- Some periodic green diagonals between 1000 and 700 seconds – cache refreshing?

TTLs returned by Open Resolvers for nytimes.com
One Month Later



Concluding Thoughts

- nytimes.com not an isolated incident:
  - regions bank (April 2013)
  - yelp, linkedin, fidelity, usps (June 2013)
- Mailing list pleas to clear caches are marginally effective.
- draft-jabley-dnsop-dns-flush-00.txt
- draft-vixie-dnsext-resimprove-00.txt, section 2

Thank You

VERISIGN®