afnic

"Random qnames - dafa888 DoS attack"

13/10/2013

afnic

Some background

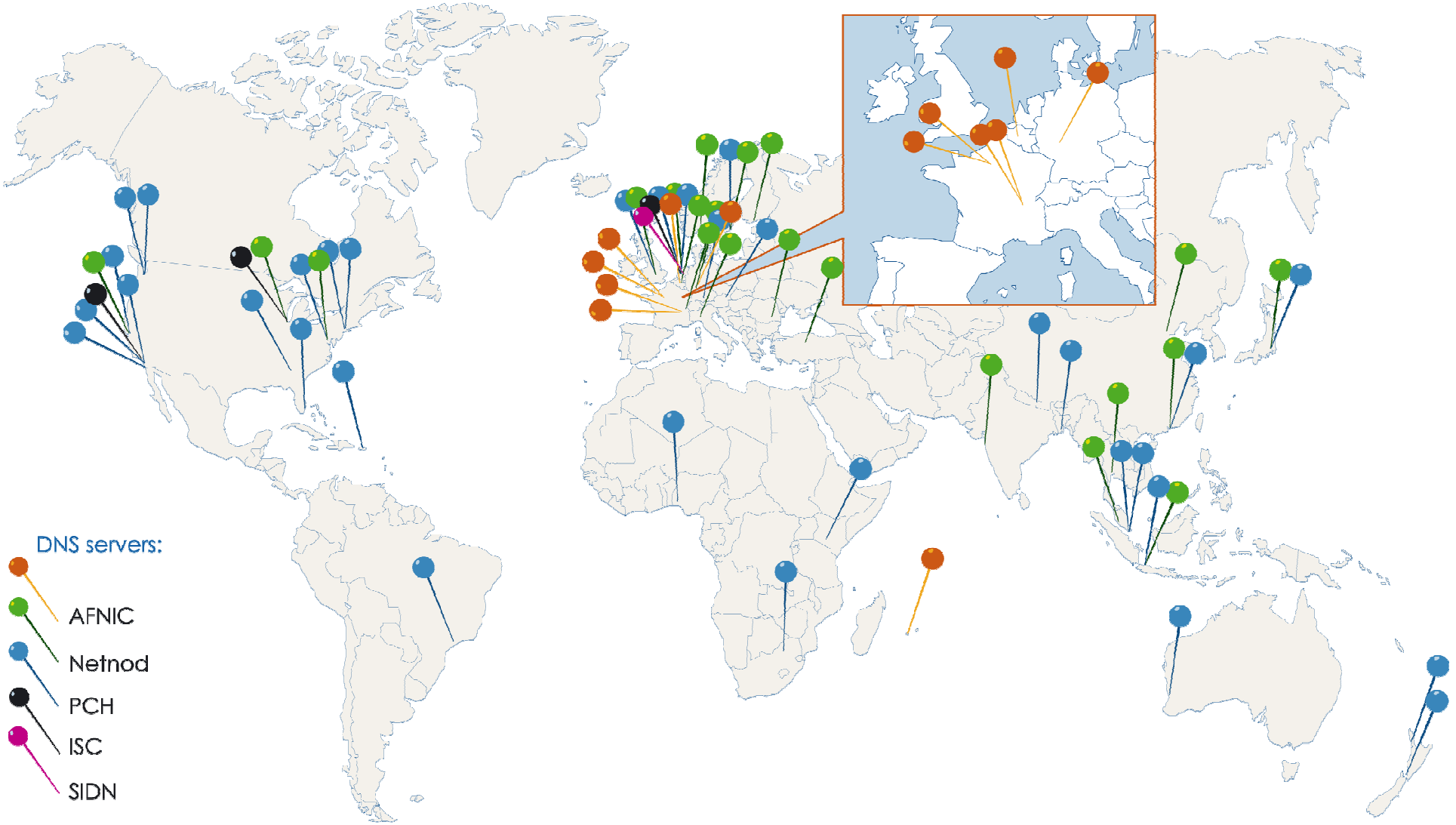
- ✓ Large DoS attack using the DNS
- ✓ ******.www.dafa888.wf
  - ✓ SLD and TLD remains the same
- ✓ Whois : "dafa888.wf"
  - ✓ [….]
  - ✓ Contact : Kaiwei chen
  - ✓ Address : 572400 lingshui
  - ✓ Country : CH
  - ✓ Registrar : EuroDNS S.A.
- ✓ Not visible to common man, but visible on network monitoring tools

The vector

09:12:34.802102 IP (tos 0x0, ttl 48, id 11149, offset 0, flags [none], proto UDP (17), length 86) 74.125.43.82.48819 > 194.0.9.1.53: 12752 [1au]
A? abwvgxmfktotuh.www.dafa888.wf. (58)

Such request are not cached by resolvers

Direction of the attack



The sources

- ✓ Many resolvers
  - ✓ Biggest being Google public DNS
  - ✓ OpenDNS was not used
- ✓ Most of the attack came from Europe

Unusual patterns

- ✓ TCP packets (20 %– 40%)

07:04:08.333642 IP (tos 0x0, ttl 48, id 50035, offset 0, flags [none], proto TCP (6), length 171) 74.125.45.21.41037 > 194.0.9.1.domain: Flags [P.], cksum 0xccac (correct), seq 5601:5720, \ ack 58868, win 1364, options [nop,nop,TS val 259543224 ecr 2239507455], length 11944830 [1au] \ A? kfgzybwjobuv.www.dafa888.wf. (117)

- ✓ IPv6 requests

07:04:08.335188 IP6 (hlim 58, next-header UDP (17) payload length: 57) \ 2a00:1450:400b:c02::155.65516 > 2001:678:c::1.domain: \ [udp sum ok] 62614 [1au] A? jcibs.www.dafa888.wf. (

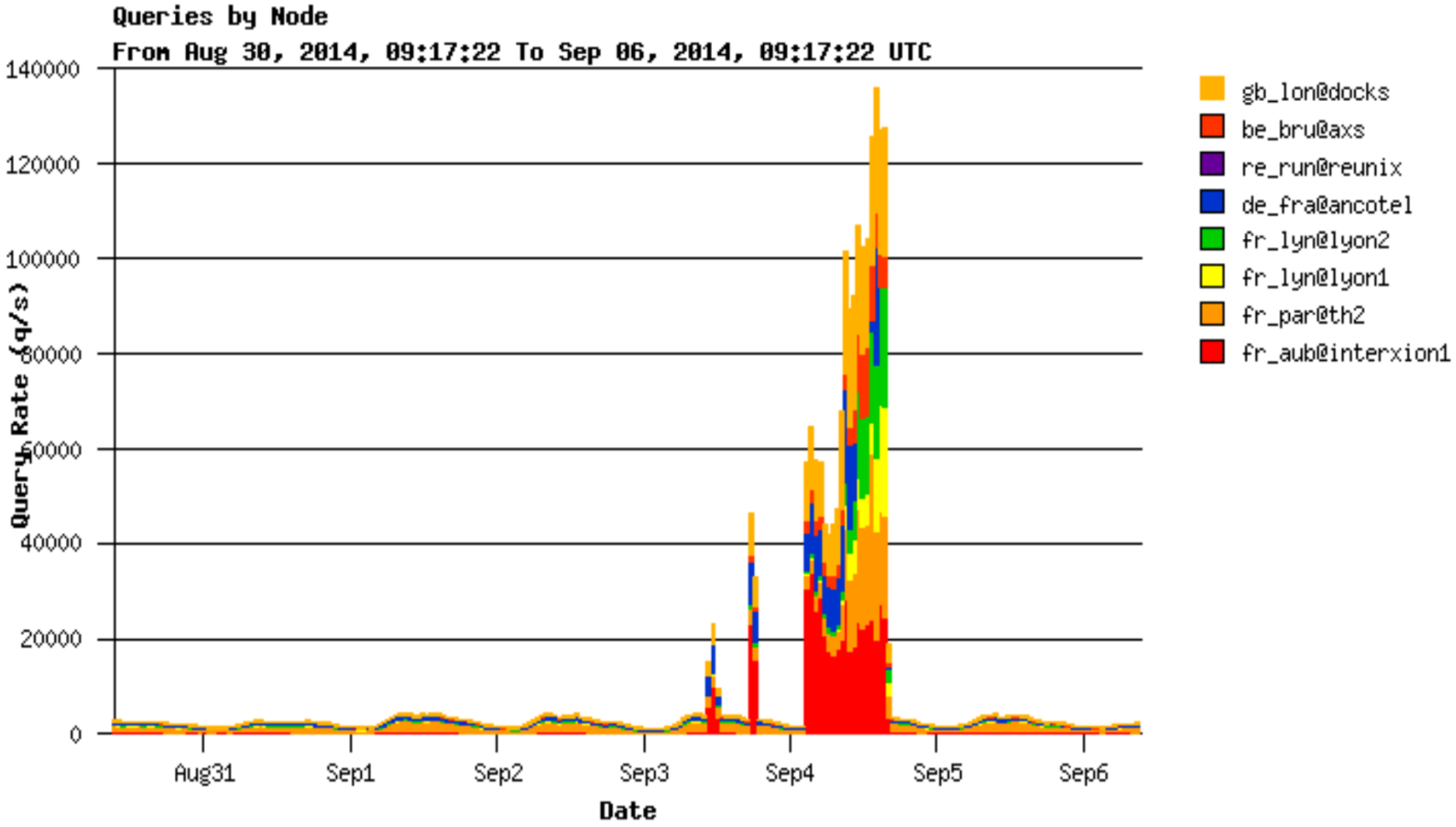
Events

- ✓ Sept:4, 2014 (d.nic.fr)
  - ✓ 02:52 – Start of the attack. ~60 Kr/s
  - ✓ 05:47 – Technical support of netnod is alerted (1 – 7% packet loss according to DNSmon)
  - ✓ 07:05 – SIDN ('Arjen Zonneveld') informs 'Bortzmeyer ' via XMPP
  - ✓ 07:59 – Netnod informs Afnic

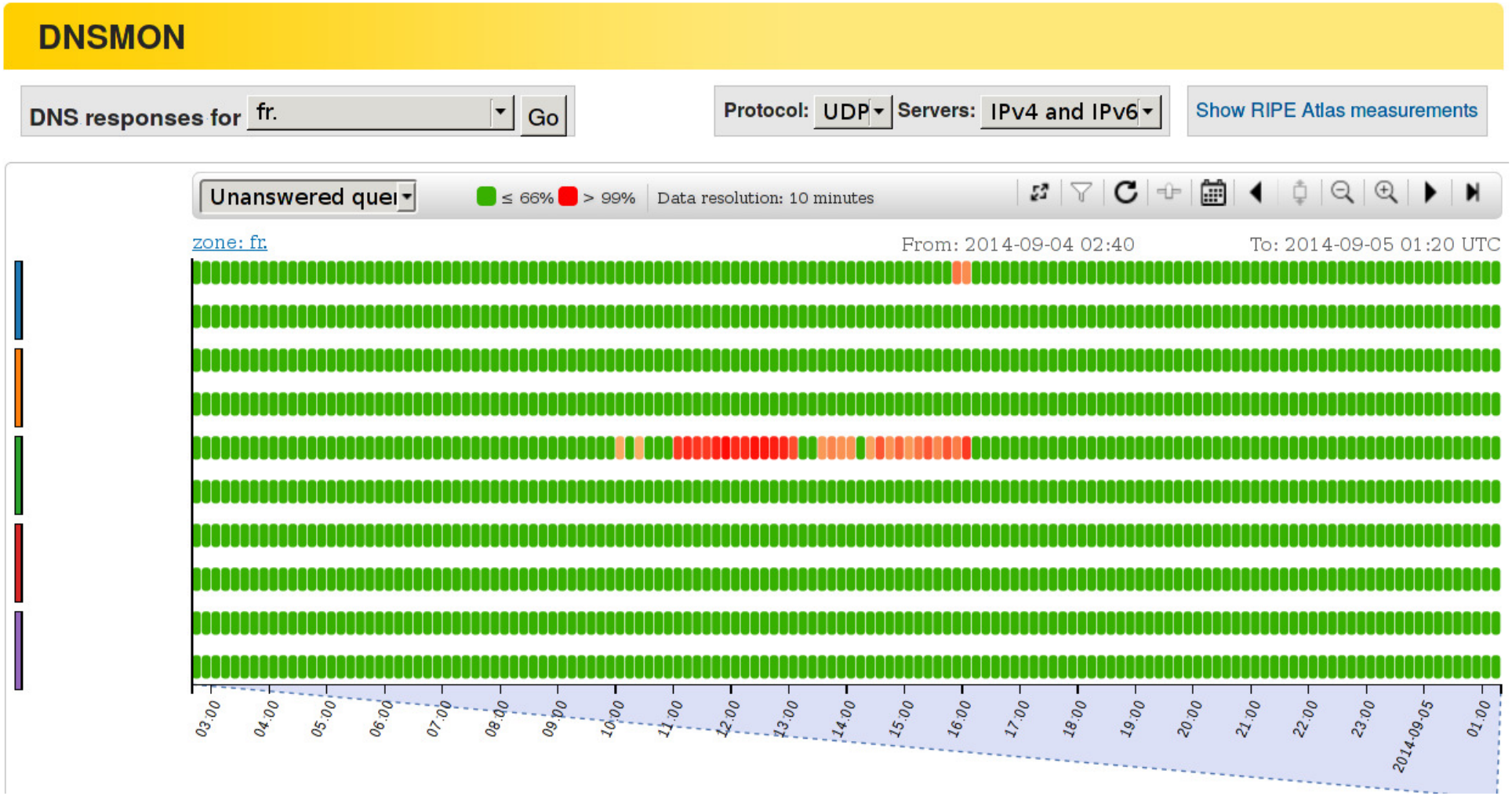
First actions

- ✓ Sept:4, 2014 (d.nic.fr)
  - ✓ 08:30 – dafa888.wf is blocked
  - ✓ 08:41 – The traffic increases to ~100 Kr/s
- ✓ Lasted 14 hrs
- ✓ > 1Mr/s (mega-requests per second)

Visual view of the attack



Effects


DNSMON
DNS responses for fr.
Go
Protocol: UDP
Servers: IPv4 and IPv6
Show RIPE Atlas measurements
Unanswered quei
≤ 66%
> 99%
Data resolution: 10 minutes
zone: fr.
From: 2014-09-04 02:40
To: 2014-09-05 01:20 UTC
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
2014-09-05
01:00

How the attack was mitigated?

- ✓ Sept:4, 2014 (d.nic.fr)
  - ✓ 15:06 – Request to Google (google-public-dns@google.com) to filter the requests pour 'dafa888.wf'
  - ✓ ~16:00 – Google blacklists 'dafa888.wf'
- ✓ 17:00 : Information regarding the attacked in Afnic's web site

Lessons learned

- ✓ Undelegating the domain was a bad idea
- ✓ During the time of the attack:
  - ✓ Combating the attack
  - ✓ Safe-guard the evidence
- ✓ Even though automised monitoring is required, it is important to have technical human competency capable of mitigating the new methods used by the attacker
- ✓ Have right contacts/partners in the technical community

Conclusion

- ✓ Thanks to our colleagues at SIDN, Netnod, PCH, ISC,
- ✓ Google, CERT .lv. . .
- ✓ Coordination and information sharing are essential
- ✓ Prepare in advance, test counter-measures
- ✓ The DoS problem is not solved yet

For further information contact :

stephane.bortzmeyer@nic.fr

afnic