DNSSEC
what lies ahead

29-11-2012

SIDN relatiedag

Utrecht

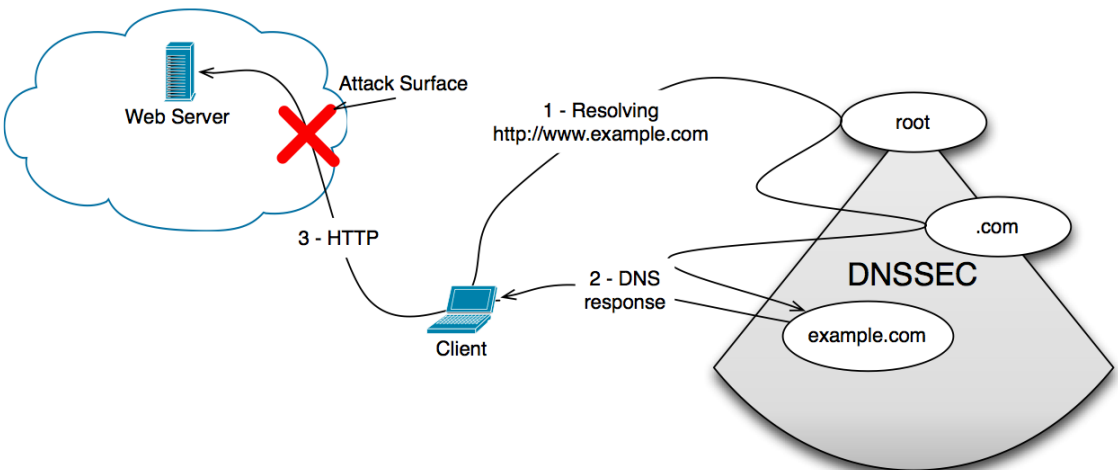
Antoin Verschuren

4 Thema's

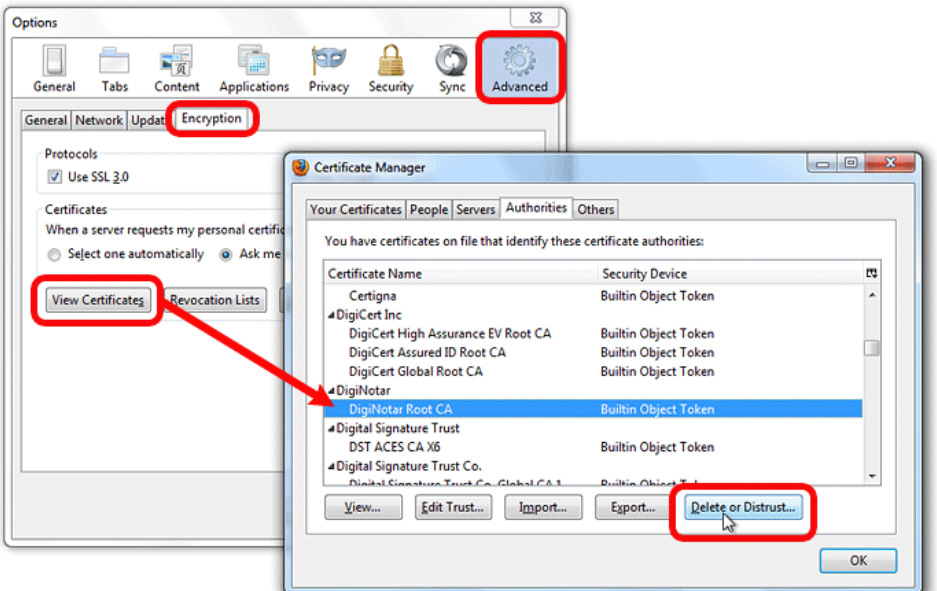
- DANE en de toekomst van CA's
- DNSSEC secure verhuizen
- Rate limiting DNS amplification attacks
- DNS abuse rapportage/onderzoek

- DANE en de toekomst van CA’s

Kwetsbaarheid van HTTP



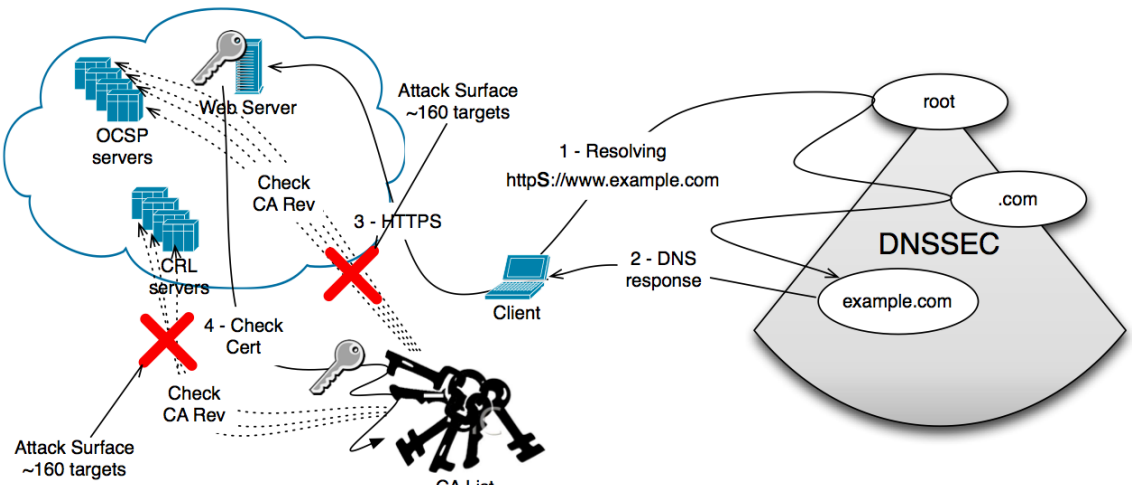
Oplossing HTTPS: Niet echt schaalbaar



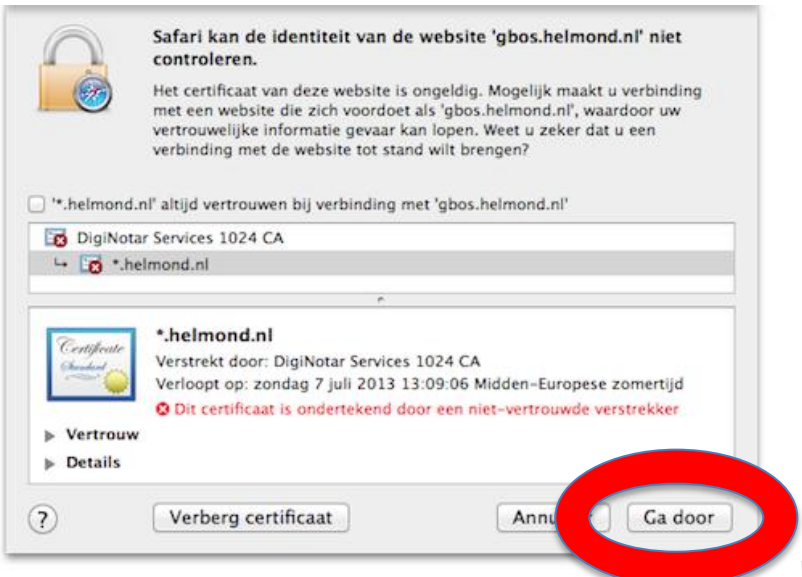
Probleem

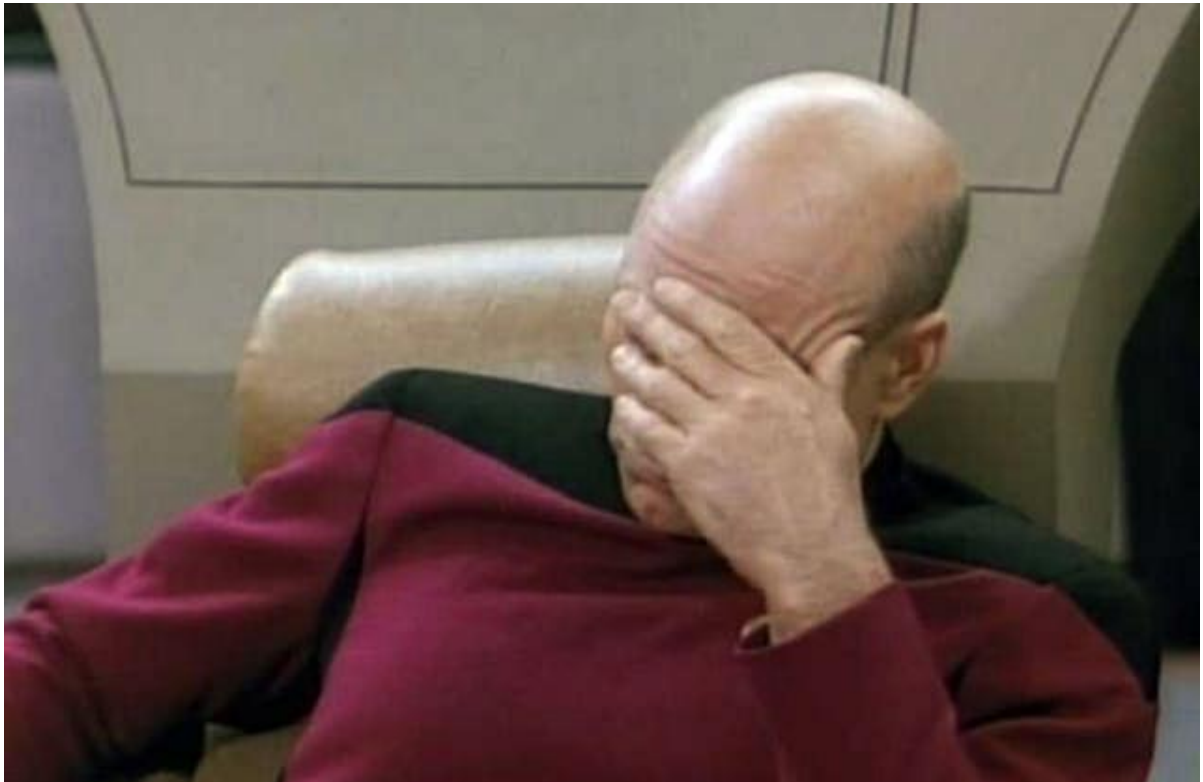
- CA=Certificate Authority: geeft certificaten uit
- Te veel CA's om allemaal te vertrouwen
- Rotte appels tussen de CA's
- Certificaten kunnen door willekeurige CA worden uitgegeven
- Geen mogelijkheid als website CA te definieren
- Verschil in certificaten onduidelijk voor eindgebruikers
- Revocation ipv vertrouwen
- Statisch in browsercode, software updates

Kwetsbaarheid HTTPS



Oplossing HTTPS: Schijnveiligheid

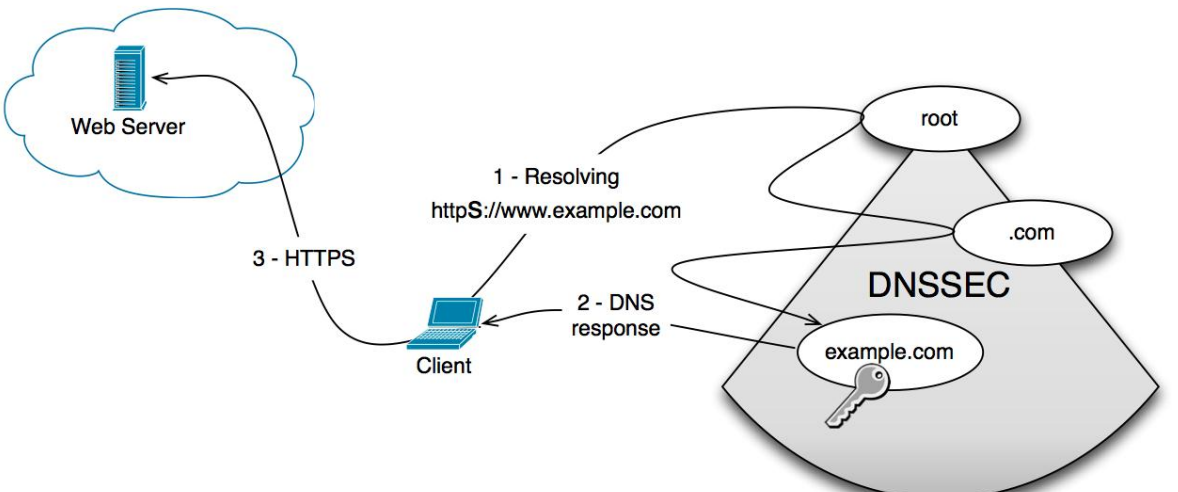


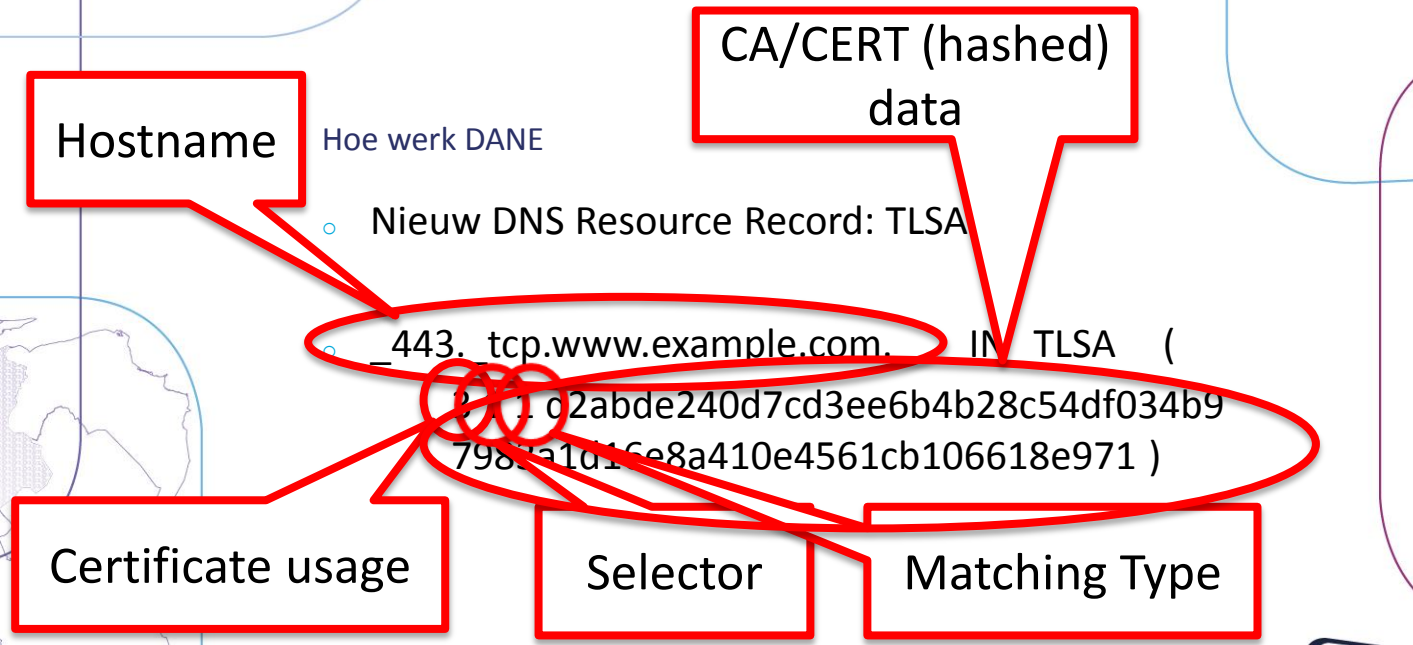


DANE: DNS-based Authentication of Named Entities

- DNSSEC bied de mogelijkheid gevalideerde data te publiceren in DNS
- Laat de domeinnaamhouder zelf definieren welke CA hij vertrouwt
- Laat de domeinnaamhouder zelf definieren welke mate van security hij nodig acht
- Revocation of verandering van certificaat kan door domeinnaamhouder zelf worden gedaan

HTTPS met DNSSEC en DANE




Hostname
CA/CERT (hashed) data
Hoe werk DANE
Nieuw DNS Resource Record: TLSA
_443._tcp.www.example.com. IN TLSA (
d2abde240d7cd3ee6b4b28c54df034b9
7983a1d16e8a410e4561cb106618e971)
Certificate usage
Selector
Matching Type

Certificate usage

0: CA constraint	1: Service certificate constraint
• CA certificaat • Moet PKIX validatie doen • “use only this CA”	• Eindgebruiker certificaat • Moet PKIX validatie doen • “use only this cert from this CA”

2: Trust anchor assertion	3: Domain-issued certificate
• Zelf gemaakt CA certificaat • Voeg CA als nieuw trust-anchor toe • “use my own CA”	• Zelf gemaakt server certificaat • Exacte match met certificaat • “use my own certificate”

Waarom nog CA certificaten nodig met DANE ?

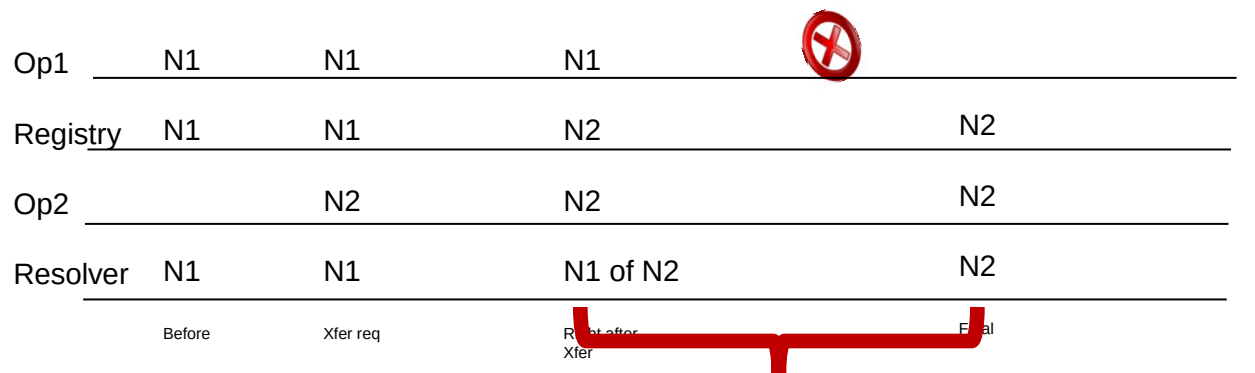
- Eindgebruiker controle
  - Is pietje puk wel pietje puk ?
  - Is pietje puk wel eigenaar van dit domein
  - KVK inschrijving, paspoort etc.
- Vertrouwen
  - CA controleert certificaat en kan revoken
  - Hoe betere controle, hoe beter de CA in aanzien
- Legacy browser support
  - Oudere browsers doen geen DANE

Voorwaarden DANE

- Domein moet DNSSEC doen
- Validating resolver moet DNSSEC ondersteunen
- Geen DNSSEC outages, dan werkt https niet meer
- Nog meer diensten op basis van DNSSEC op stapel?
- Bij veranderingen aan domein moet DNSSEC blijven werken

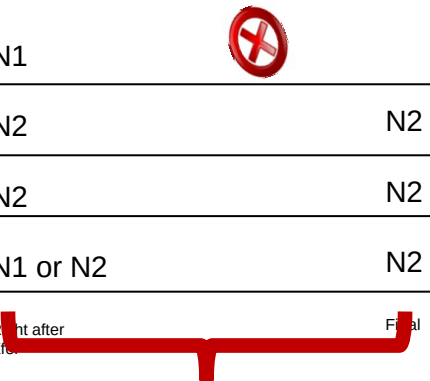
DNSSEC secure verhuizen

Transfers in (no DNSSEC) DNS



Waarom is er een probleem ?

Op1	N1	N1	N1	
Reg	N1	N1	N2	N2
Op2		N2	N2	N2
Res	N1	N1	N1 or N2	N2
	Before	Xfer req	Right after Xfer	Final



Als er slechts 1 sleutel is, is er slechts 1 van de 2 antwoorden geldig

Oplossing

Op1	N1	N1	N1	
Reg	N1	N1	N2	N2
Op2		N2	N2	N2
Res	N1	N1	N1 of N2	N2
	Before	Xfer req	R[illegible] after Xfer	F[illegible]al

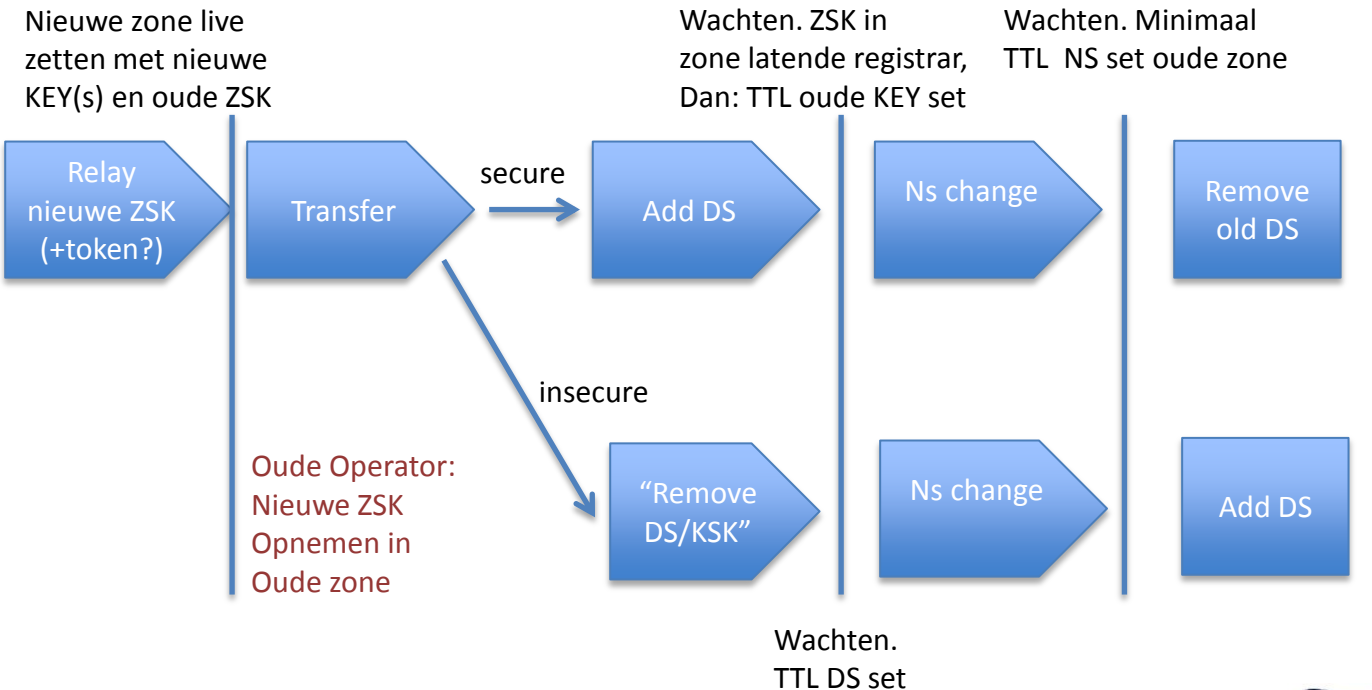
Beide versies zijn geldig met DNSSEC als:

-nieuwe zone gesigned is met oude private key

-de oude zone de nieuwe public key bevat

Uitdaging

- Losing DNS-operator moet nieuwe ZSK ontvangen.
- Er bestaat geen direct communicatiekanaal
- Losing DNS-operator moet ZSK opnemen in zone.
- Moet eenvoudig te automatiseren zijn.
- Verschillen in TTL's en wachttijden.
- Gaining operator in control.
- Beschreven in draft-koch-dnsop-dnssec-operator-change



- Geen checks vanuit SIDN
- U vraagt, wij draaien

Impact Secure verhuizen

- Oude operator
  - Ontvangt ZSK van registry in EPP queue registrar
  - Zet ZSK in zone en signeert opnieuw
  - Volledig automatiseerbaar
- Nieuwe operator
  - 1 extra stap voor de transfer (ZSK relay)
  - Controleer of ZSK in oude zone staat voor/na transfer
  - Maak zelf keuze hoe lang wachten voor secure/insecure traject
  - Inbouwen standaard timers of query oude zone
  - 1 extra stap na de verhuizing (remove old DS)

Discussie: Technische eisen .nl domeinnamen

6i. De TTL-waarde van het DNSKEY record van een zone mag maximaal 172800 (2 dagen) bedragen. Dit om te voorkomen dat bij wijziging van de operator van een zone te lang moet worden gewacht voordat het nieuwe key materiaal is gepropageerd, en de zone als het ware wordt gegijzeld door de latende operator.

Rate limiting DNS amplification attacks

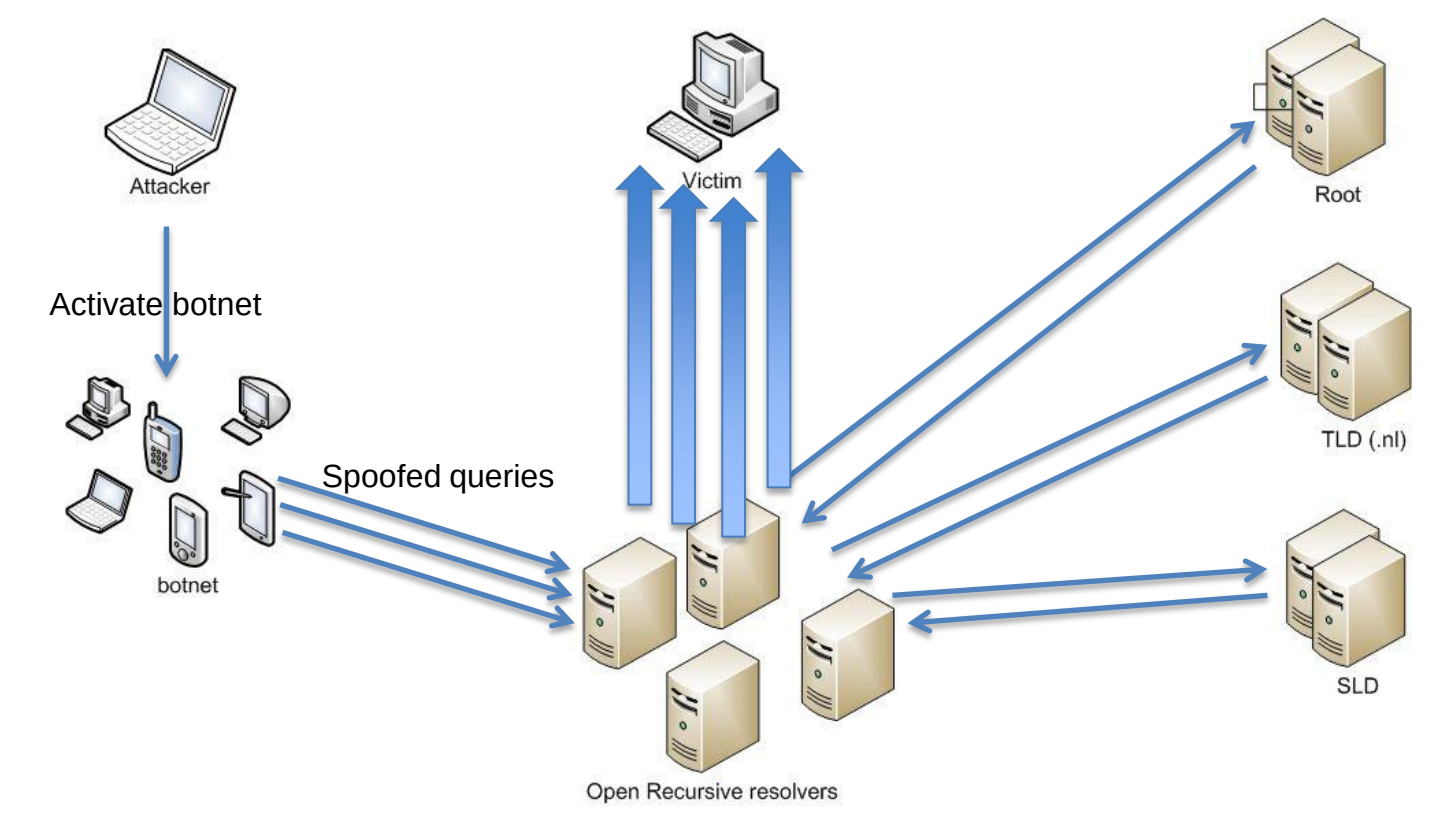
DNSSEC abuse

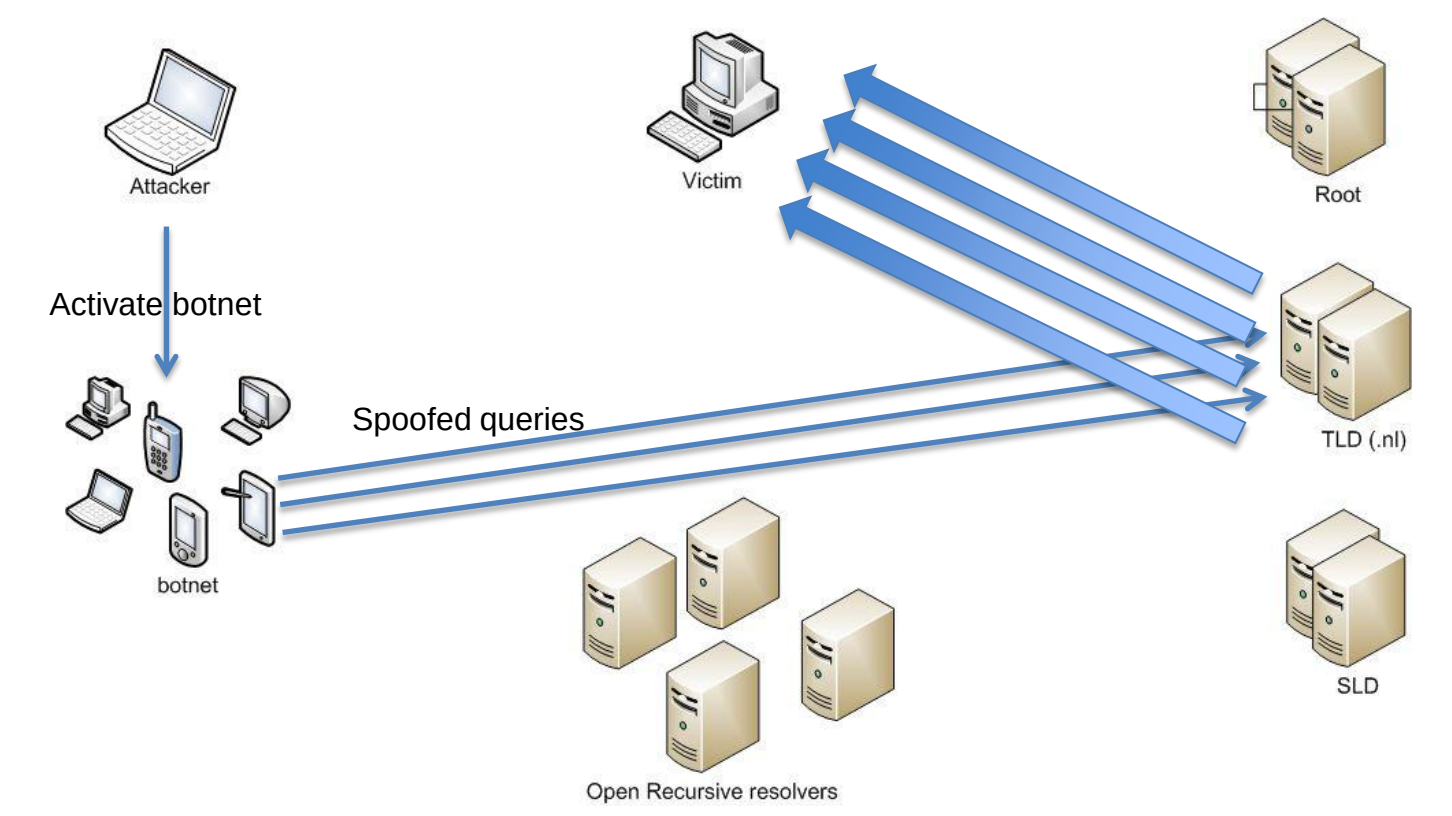
- ANY antwoorden zijn groot:

```
; <<>> DiG 9.8.1-P1 <<>> @ns1.dns.nl nl any
;; MSG SIZE  rcvd: 1940
```

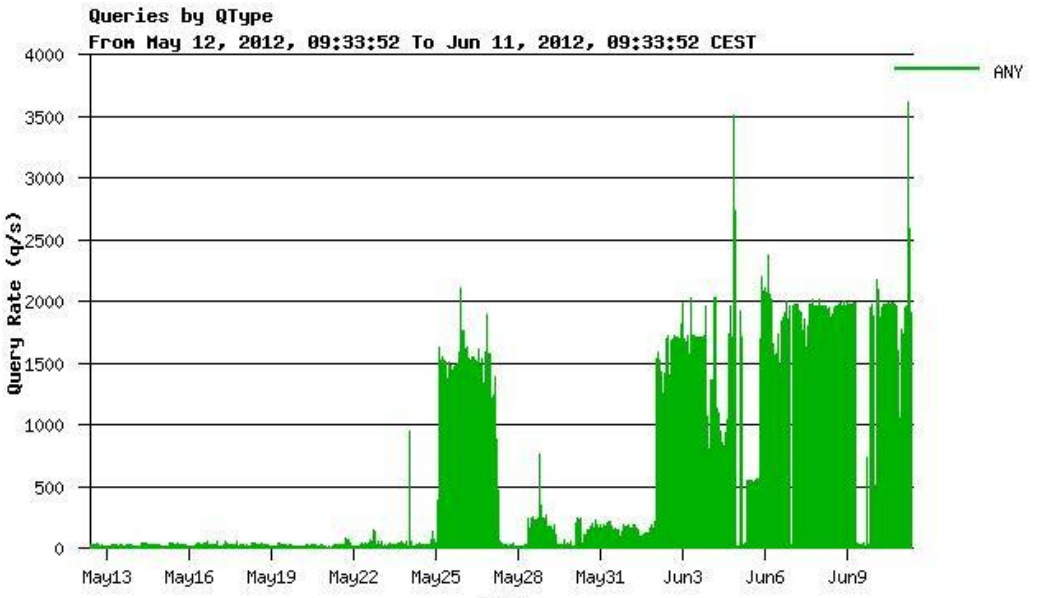
- DNSSEC maakt ze nog groter, en niet enkel bij ANY

- Sinds mei 2012 groot ingezet bij DDOS aanvallen


Attacker
Activate botnet
botnet
Spoofed queries
Victim
Root
TLD (.nl)
SLD
Open Recursive resolvers


Attacker
Activate botnet
botnet
Spoofed queries
Victim
Root
TLD (.nl)
SLD
Open Recursive resolvers

Rare ANY queries



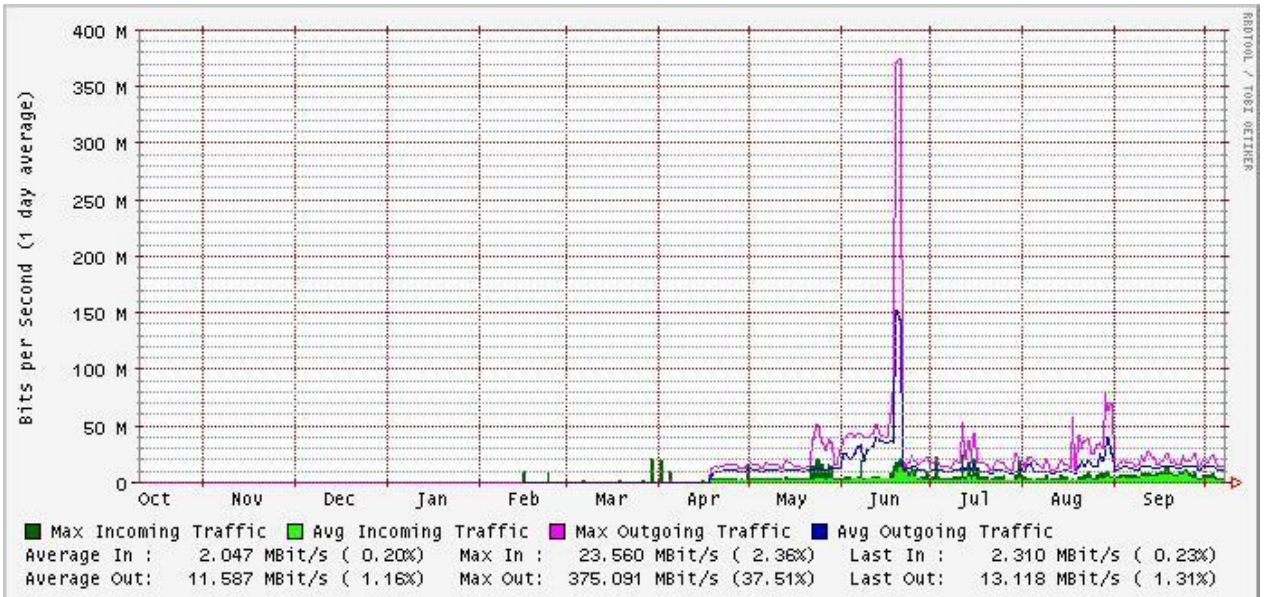
Overleg met andere TLD's/OARC/DNS-community

- Zeer duidelijke fingerprint:
  - Query voor "TLD" ANY
  - Per TLD slechts 1 of enkele servers aangevallen
  - UDP payload size 9000 hard gezet
  - 25 identieke pakketten per 200-300 microseconde
  - Source IP gebruikt altijd hetzelfde query ID
  - 1 of Enkele victims met colateral damage
  - Overleg met IXes loopt dood vanwege onvoldoende monitoring

Wat te doen ?

- Eerste prioriteit: beschermen .nl: kan het kwaad?
- .nl wordt niet aangevallen, maar iemand anders.
- Met misbruik van onze capaciteit.
- Uitgaand verkeer naar slachtoffer: 350 Mbs per NS !!
- Andere TLD's/DNS-operators rapporteren exact dezelfde aanval (en slachtoffer), dus in totaal nog meer.
- SIDN wil niet medeplichtig zijn aan aanval.
- Besluit te filteren in juni niet lichtzinnig genomen.

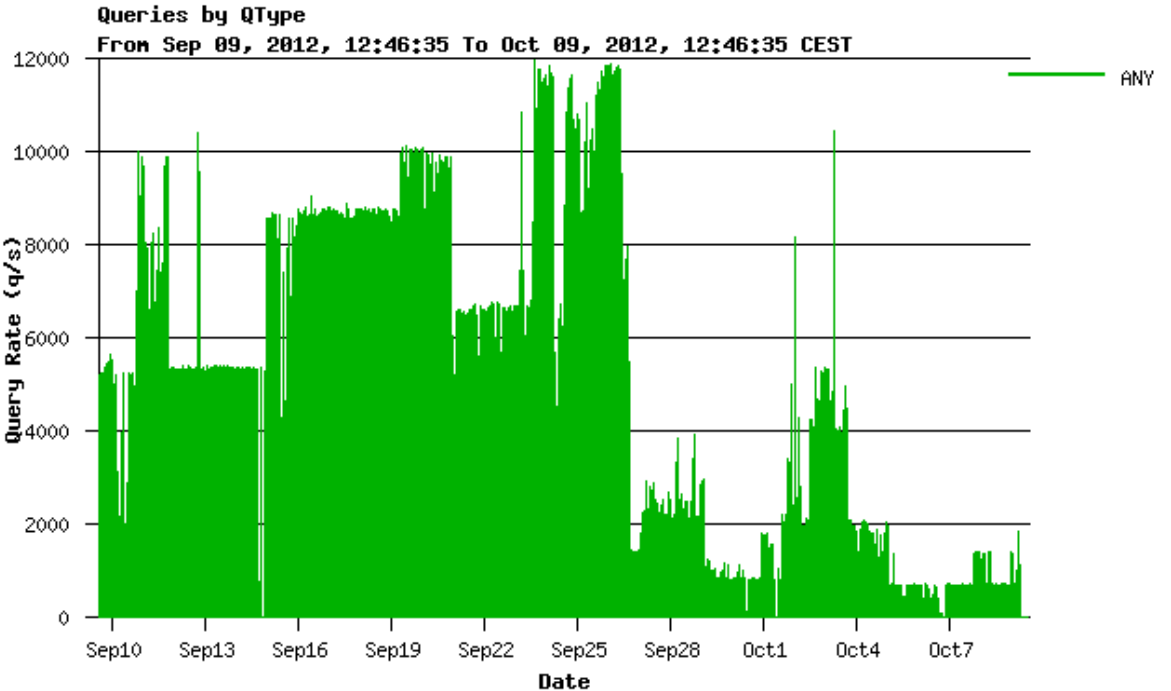
Traffic


Bits per Second (1 day average)
400 M
350 M
300 M
250 M
200 M
150 M
100 M
50 M
0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Max Incoming Traffic
Avg Incoming Traffic
Max Outgoing Traffic
Avg Outgoing Traffic
Average In : 2.047 MBit/s (0.20%)
Max In : 23.560 MBit/s (2.36%)
Last In : 2.310 MBit/s (0.23%)
Average Out: 11.587 MBit/s (1.16%)
Max Out: 375.091 MBit/s (37.51%)
Last Out: 13.118 MBit/s (1.31%)
RRDTOOL / TOBI OETIKER

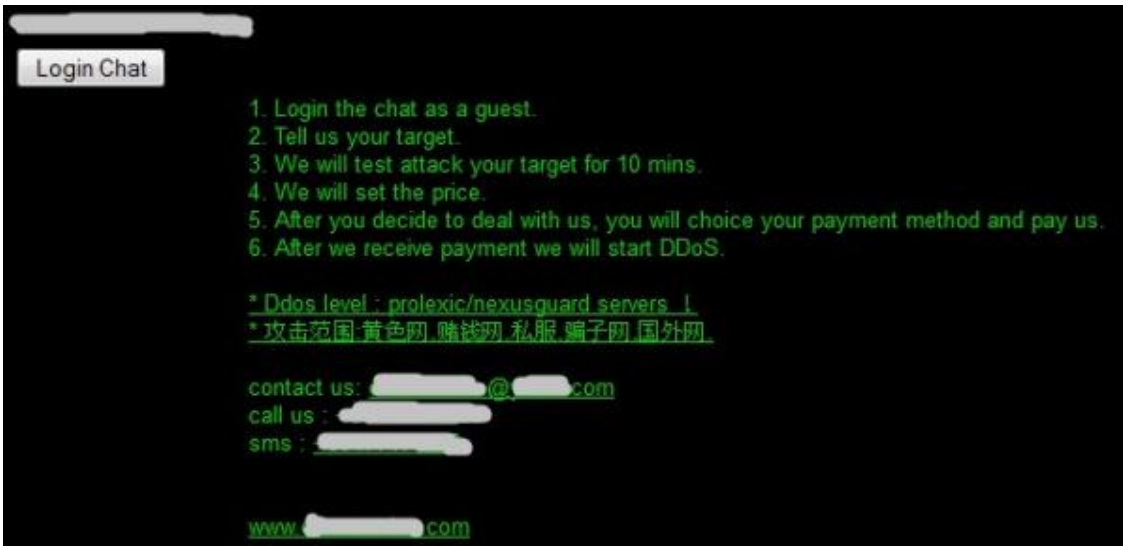
Filtermethode

- Python script van Stephane Bortzmeyer
- IPtables ratelimiter
- Alle identieke ANY queries meer dan 20/seconde worden niet meer aangeboden aan nameserver, en dus ook niet meer beantwoord.
- We meten binnenkomende queries op IF, dus we zien ze nog wel binnenkomen in onze monitoring/logs

- Ook andere filtermethodes (BIND patch)


Queries by QType
From Sep 09, 2012, 12:46:35 To Oct 09, 2012, 12:46:35 CEST
ANY
Query Rate (q/s)
12000
10000
8000
6000
4000
2000
0
Sep10
Sep13
Sep16
Sep19
Sep22
Sep25
Sep28
Oct1
Oct4
Oct7
Date

Waar komt het vandaan ?



Steeds geavanceerder….

Dit gaat jullie ook overkomen

- TLD’s/Root hebben veel infrastructuur -> veel bandbreedte beschikbaar -> goede reflector for bad guys ☹
- Andere SLD’s met veel infrastructuur ook al doelwit.
- De meeste TLD’s, root servers worden nu gefilterd zodra er een aanval komt.

- Grote DNS hosters zijn het volgende slachtoffer.

Wat moet er echt gebeuren

- Rate limiting op nameservers is een tijdelijke pleister
- Er zijn aanvallen te bedenken die veel moeilijker te filteren zijn zonder regulier verkeer aan te tasten.

- Stop spoofing (BCP38, Lees RFC 2827)
- Stop open resolvers (Test je eigen netwerk)
- Stop Botnets (Hoe?)

DNS abuse rapportage/onderzoek

Vraagjes

- Hoe monitoren jullie netwerk verkeer?
- Hoe analyseren jullie DNS verkeer?
- Wanneer gaan er bij jullie alarmbellen rinkelen?
- Welke fora/mailinglists/communities hou je bij?
- Met wie overleg je als je een probleem hebt buiten je eigen netwerk?
- En wie helpt je dan ?

Tools

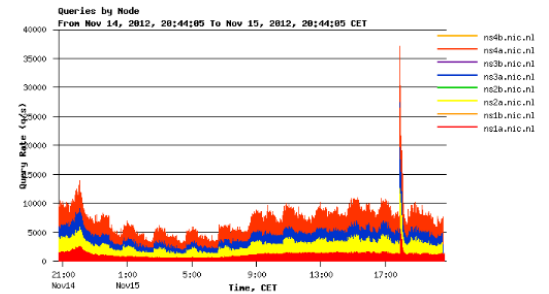
- DSC (DNS Statistics Collector)
- PacketQ
- DNS2DB
- Wireshark

Tools: DSC

Servers/Nodes
- nl
  - ns1a.nic.nl
  - ns1b.nic.nl
  - ns2a.nic.nl
  - ns2b.nic.nl
  - ns3a.nic.nl
  - ns3b.nic.nl
  - ns4a.nic.nl
  - ns4b.nic.nl
- anycloud
- nl-zonexfer

Plots
- By Node
- Qtypes
- Rcodes
- Classification
- Client Geography
- TLDs
- 2nd Level Domains
- 3rd Level Domains
- Rcodes by Client Address
- Popular Names
- IPv6 root abusers
- Opcodes
- Query Attributes
- CHAOS
- IP Version
- DNS Transport
- IP Protocols
- Qname Length
- Reply Lengths
- Source Ports
- Priming Queries
- Priming Responses

Time Scale
- 1hour
- 4hour
- 1day
- 1week
- 1month



The **Queries by Node** plot shows the amount of queries coming from each node in the server cluster. If you would like to see the traffic for a single node, select the node name in the Servers/Nodes menu on the left.

Note that the *By Node* option disappears from the Plots list when you are viewing the data for a single node. It reappears if you click on the Server name in the Servers/Nodes menu.

Y-Axis
- Query Rate (q/s)
- Percent of Queries

Help

- Bind/NSD/PowerDNS user mailinglists
- RIPE DNS WG
- IETF DNSOP WG
- DNS OARC

DNS-OARC

Domain Name System Operations Analysis and Research Center

- Not for profit, membership, NDA, data sharing
- Root servers, TLD's, DNS Vendors, ISP's, DNS operators
- Besloten incident reporting, members only mailinglist
- DITL: Day In The Life (of the Internet)
- Maar ook: openbare workshops
- Openbare services
- Zie http://www.dns-oarc.net

DNS-OARC

Domain Name System Operations Analysis and Research Center

Discussie:

- Waar hebben jullie behoefte aan?
- Wanneer zouden jullie lid worden van een CERT?
- Wat zouden jullie (kunnen) bijdragen?
- Wat zouden jullie er voor over hebben?
- Is jullie data belangrijk voor anderen?

Vragen ?

antoin.verschuren@sidn.nl

www.sidnlabs.nl