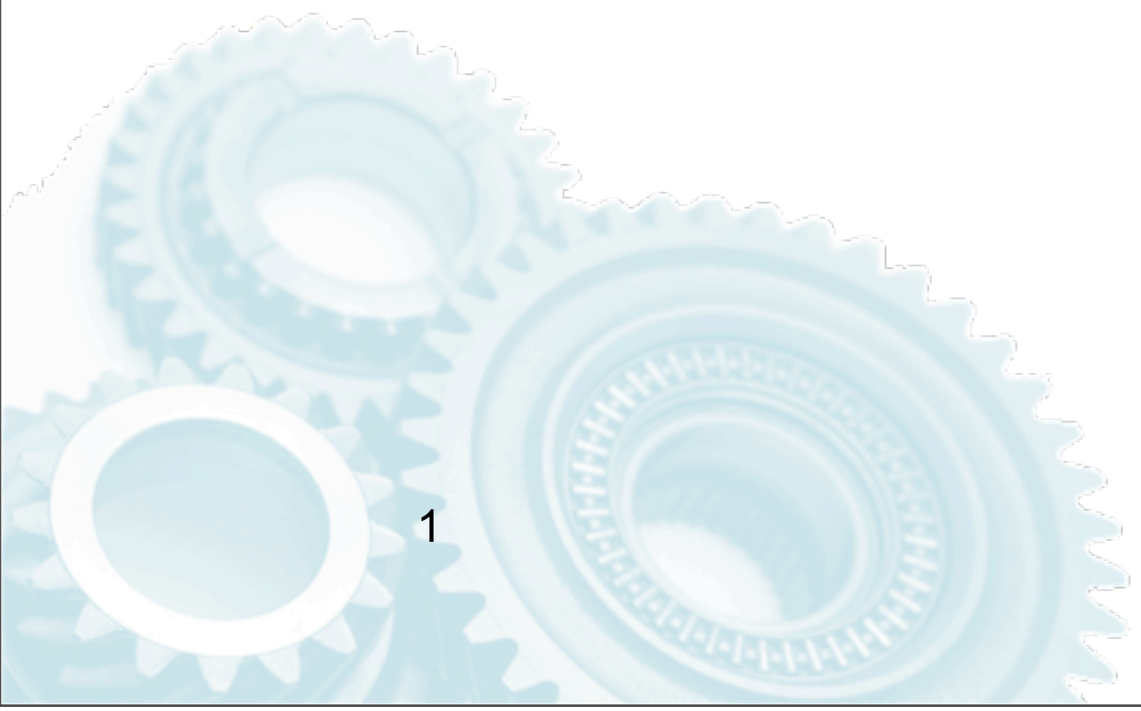
DNS Pasivo/DNSDB

ISC



DNS Pasivo y DNSDB

- DNS Pasivo
  - –ejemplos
- SIE
- dnsqr
- DNSDB

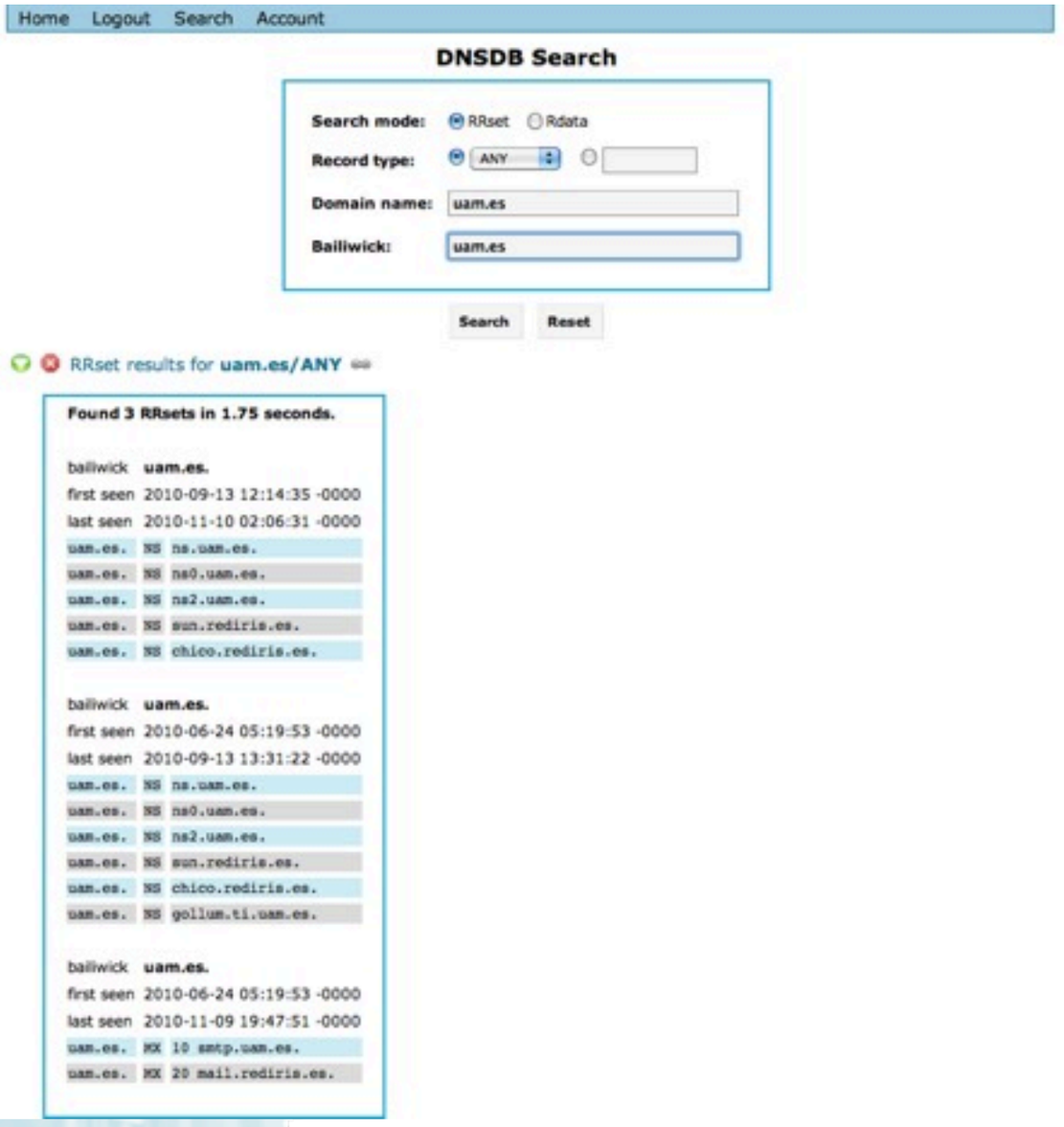
DNS Pasivo / Passive DNS

- Inventado por Florian Weimer en 2004
- Se capturan mensajes de DNS entre servidores
  - no entre usuario y servidor
  - captura por sensores distribuidos
  - enviados a puntos de analisis
- la información procesada se guarda en una base de datos

DNS Pasivo

- Florian Weimer - dnslogger (2004-) en BFK.de (antes en RUS-CERT)
- Bojan Zdrnja dnsparse (2006-)
- SIE en ISC (2007-)

ISC DNSDB


Home Logout Search Account
DNSDB Search
Search mode: RRset Rdata
Record type: ANY
Domain name: uam.es
Bailiwick: uam.es
Search Reset
RRset results for uam.es/ANY
Found 3 RRsets in 1.75 seconds.
bailiwick uam.es.
first seen 2010-09-13 12:14:35 -0000
last seen 2010-11-10 02:06:31 -0000
uam.es. NS ns.uam.es.
uam.es. NS ns0.uam.es.
uam.es. NS ns2.uam.es.
uam.es. NS sun.rediris.es.
uam.es. NS chico.rediris.es.
bailiwick uam.es.
first seen 2010-06-24 05:19:53 -0000
last seen 2010-09-13 13:31:22 -0000
uam.es. NS ns.uam.es.
uam.es. NS ns0.uam.es.
uam.es. NS ns2.uam.es.
uam.es. NS sun.rediris.es.
uam.es. NS chico.rediris.es.
uam.es. NS gollum.ti.uam.es.
bailiwick uam.es.
first seen 2010-06-24 05:19:53 -0000
last seen 2010-11-09 19:47:51 -0000
uam.es. MX 10 smtp.uam.es.
uam.es. MX 20 mail.rediris.es.

ISC Security Information Exchange (SIE)

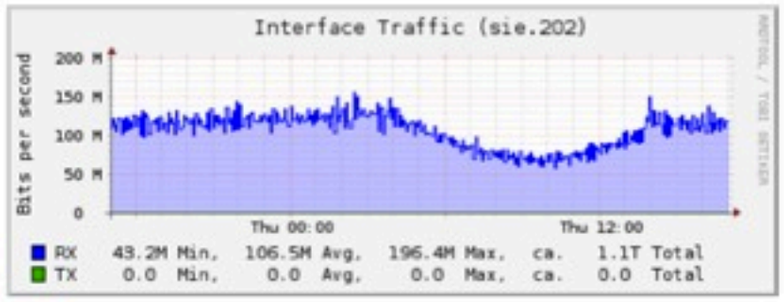
- Red de distribución para diversos tipos de información de seguridad
  - un tipo es DNS Pasivo
- Los operadores de sensores suben datos al SIE
- Los datos se emiten a VLANs privadas donde están las máquinas de análisis
- Los mensajes fluyen el formato NMSG

Canal de DNS Pasivo

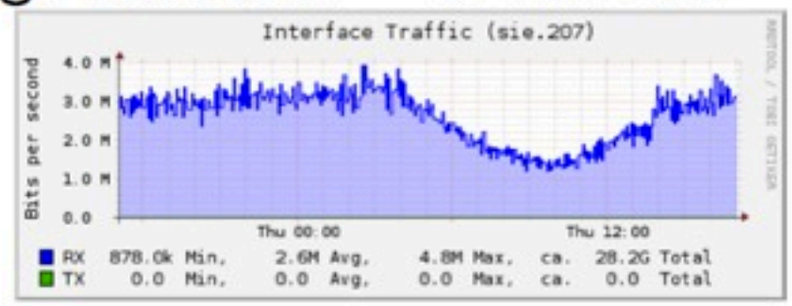
- Canal de DNS Pasivo “raw” en VLAN dedicada
  - cada “canal” es una VLAN
- Estimación a un año de datos recogidos
  - 0.98 trillion DNS response messages per year.
  - 2.6 trillion RRsets per year.
  - 140 terabytes of uploads per year.

Canal de DNS Pasivo

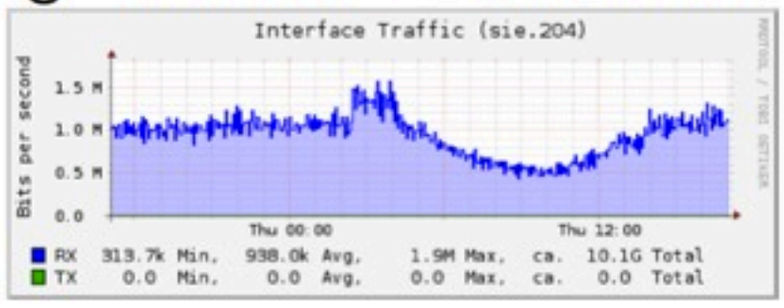
Raw passive DNS – VLAN 202 – 100 Mbps.



First stage reduction – VLAN 207 – 3 Mbps.



Second stage reduction – VLAN 204 – 1 Mbps.



dnsqr

- módulo de mensajes para libnmsg diseñado para captura de DNS Pasivo
- captura, con filtros opcionales, y genera mensajes en formato NMSG
- se encarga de re-ensamblar los paquetes IP para recomponer cada mensaje

sie-dns-sensor & sie-scripts

- sie-dns-sensor. ejecutable para ayudar a montar sensores en Linux (deb/rpm)
- sie-scripts, scripts y soporte para FreeBSD
- ftp://ftp.isc.org/isc/nmsg/misc/

DNSDB

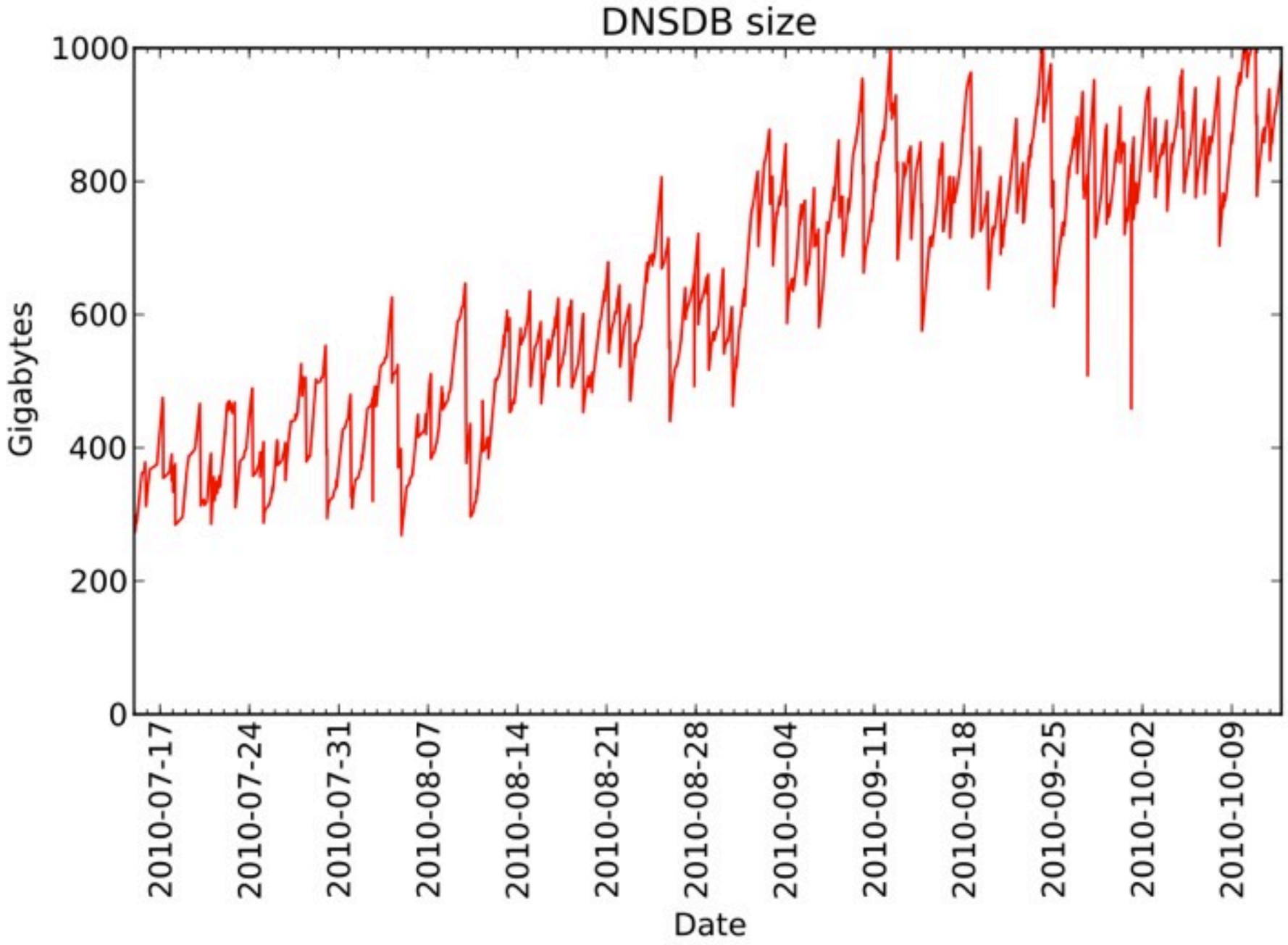
- base de datos para guardar registros de DNS
  - carga datos de DNS Pasivo y de ficheros de zona
  - usa Apache Cassandra como base de datos
    - muy rápida para escritura secuencial
    - key-value se corresponde bien con datos de DNS
  - Interfaz HTTP con REST

API DNSDB

$ DNSDB_FORMAT=json isc-dnsdb-query rdata ip 192.0.32.10 l sort

{"rrtype": "A", "rrname": "example.com.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.edu.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.net.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.org.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "mal1.gbs-clan.de.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "mail2.gbs-clan.de.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "scribble.co.uk.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.com.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.edu.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.net.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.org.", "rdata": "192.0.32.10"}

Crecimient de DNSDB



Demo...

https://dnsdb.isc.org