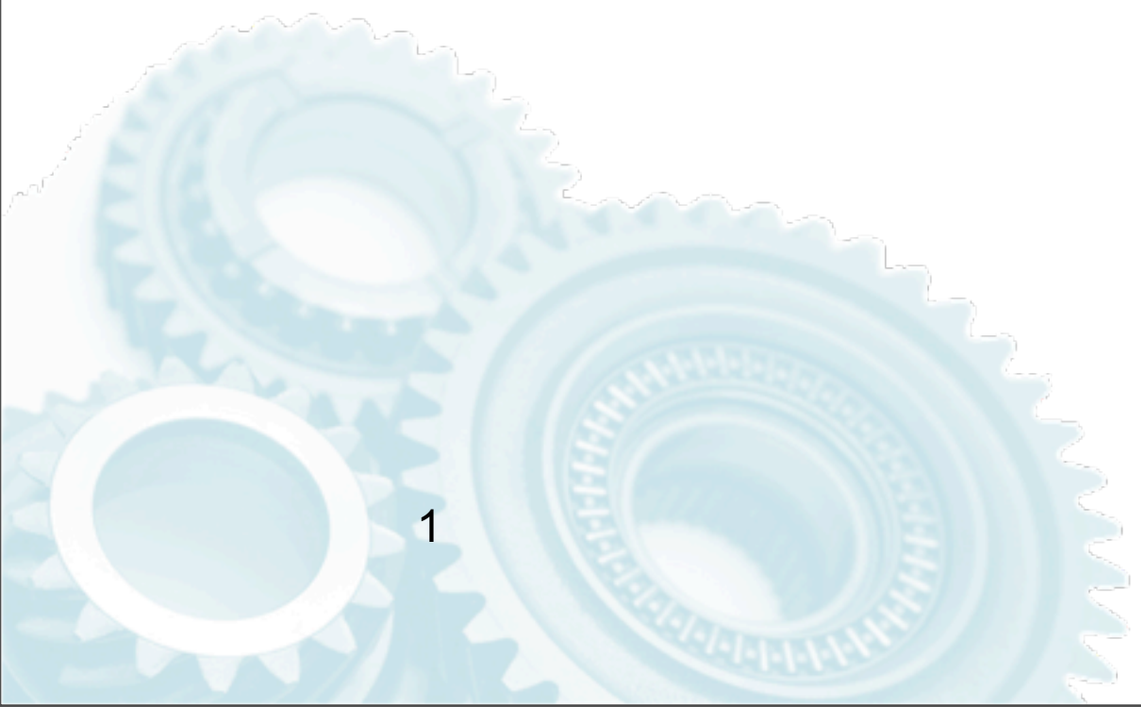
Passive DNS/DNSDB

ISC



Passive DNS & DNSDB

- PassiveDNS
  - –examples
- SIE
- dnsqr
- DNSDB

Passive DNS

- Idea by Florian Weimer in 2004
- Capture DNS messages between servers
  - not between user (stub) and server
  - distributed sensors for data capture
  - Data forwarded for analysis at SIE sites
- Processed data is stored in a Database

Passive DNS history

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

ISC Security Information Exchange (SIE)

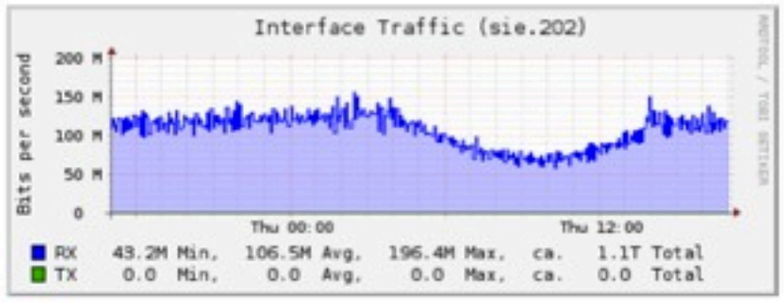
- Distribution network for several types of security information
  - one type is Passive DNS
- Sensor operators upload data to SIE
- Data is replayed onto private VLANs where the analysis machines are
- Messages flow in NMSG format

Passive DNS channel

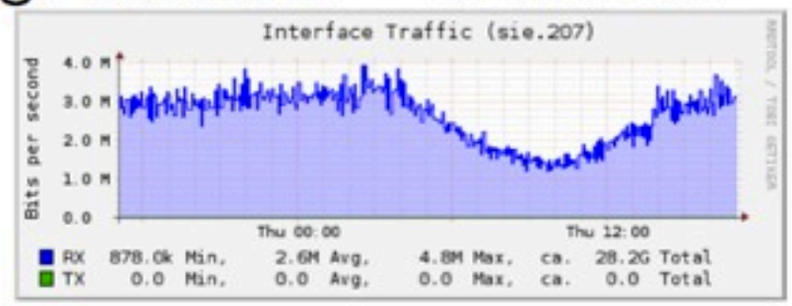
- raw Passive DNS channel on a dedicated VLAN
  - each "channel" at SIE is a VLAN
- Some estimates for yearly data collection
  - 0.98 trillion DNS response messages per year.
  - 2.6 trillion RRsets per year.
  - 140 terabytes of uploads per year.

Passive DNS channel

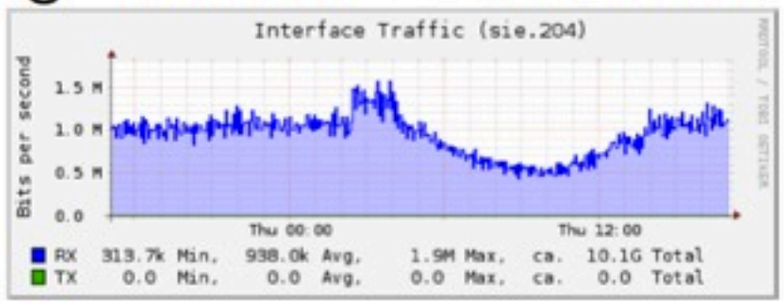
Raw passive DNS – VLAN 202 – 100 Mbps.



First stage reduction – VLAN 207 – 3 Mbps.



Second stage reduction – VLAN 204 – 1 Mbps.



dnsqr

- messages module for libnmsg designed for passive DNS capture
- captures, with optional filters, and generates messages in NMSG format
- also does IP level re-assembly so you don’t have to

sie-dns-sensor & sie-scripts

- sie-dns-sensor. executable to aid in setting up sensors on Linux (deb/rpm)
- sie-scripts, scripts and support for FreeBSD
- ftp://ftp.isc.org/isc/nmsg/misc/

DNSDB

- DB to store DNS records
  - loads data from Passive DNS and zone files
  - uses Apache Cassandra
    - very fast sequential writes
    - key-value maps well to DNS data
  - RESTful HTTP Interface

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"}

Demo...

https://dnsdb.isc.org