dns-stats
Collector Project

Sara Dickinson Sinodun

OARC Spring Workshop 2016

dns-stats

- “dns-stats” is a collaborative effort to produce Open Source software for DNS traffic collection and statistics analysis (dns-stats.org)

- May already know of it from Hedgehog presenter
  - Used by ICANN (2.1.0b packages available)

- Who is involved ?
  - ICANN
  - CZ.NIC
  - Sinodun

Would like to hear from other interested parties!

DNS Statistics

- **Previously….** Full PCAPs or DSC (OARC).

- **Today:** Other DNS Traffic Analysis software is available… not always a good fit or free!

- **Next for dns-stats:** New DNS traffic collector to enable detailed traffic analysis

Collector Features

- Packet capture for 2 use cases:
  - ‘dedicated capture server’ (port mirroring)
  - ‘hosted name server instance’ (resource constrained)

- Multiple output formats produced by collector (Work in Progress)
  - **PCAPs (paired)** for replay
  - **Compressed DNS format** for analysis
  - **DSC XML** for overview

Upload might normally be XML only,
with periodic or on-demand retrieval of detailed data

Collector Status

- Prototyping collector (C, libtrace)
  - Packet pairing algorithm
- Investigating data formats (PCAP-NG, CBOR, …)
- Target: Start some testing by mid 2016
- Ubuntu and FreeBSD

Next Steps

- Ongoing work on collector
- Future work on consuming detailed data and performing analysis centrally
- Code will be release Open Source, most likely under GPL v3 license
- If you are interested contact us!

terry.manderson@icann.org
ondrej.sury@nic.cz
sara@sinodun.com
dns-stats-users@dns-stats.org