Internet-Sicherheit fördern – kritische Infrastrukturen schützen.

CSIRT Meeting
2011 - Barcelona
passive DNS: Idea to capture the DNS answers and give them a timestamp.

Privacy -> omit src IPs (of client)!

CERT.at + UniWien implemented a pDNS server: nmsg + C code + postgresql 9.0.2

Optimized for speed! (~ 20 msec for a complex answer).

Can go through CIDR network ranges

webinterface

whois interface is 100% compatible with BFK pDNS.

Looking for sensors!
Privacy Aware?

- Yes! We are super careful about this
- We capture outside of the DNS recursor
- We want more sensors to mix the results
  -> can not associate data with a specific sensor
ReSTful interface

search + source

ISC is coming now

Answer + links

open source intelligence tools on the Web

Time info
Scalability

- Last time (Istanbul) we mentioned scalability problems.
- Solved!
- Postgres needed to be tuned a lot!
- New server with 35 GB RAM, 12 cores

60 mil. rows and growing linearly
Agreement

• Have to sign NDA:
  • Data must not be sold,
  • Data must not be given away to third parties except for incident handling purposes

• Access only for CERTs
• Database stays in the EU!

• We need big recursive DNS servers as sensors! (Universities, ISPs).
Contact:

team@cert.at

Thanks!