Techniques for visualizing network hygiene

Tarik El Yassem

Introduction

For Release: 06/04/2009

FTC Shuts Down Notorious Rogue Internet Service Provider, 3FN Service Specializes in Hosting Spam-Spewing Botnets, Phishing Web sites, Child Pornography, and Other Illegal, Malicious Web Content

● **8 februari 2012**, 18:11

KPN slachtoffer van computerhack

De CEO van KPN, Eelco Blok, tijdens een aandeelhoudersvergadering in april vorig jaar. Foto NRC / Roel Rozenburg

BINNENLAND KPN is vorige maand slachtoffer geworden van een geslaagde hackaanval. Dat heeft het bedrijf vanmiddag gemeld. De hacker(s) slaagden erin toegang te krijgen tot servers met klantgegevens van particulieren en bedrijven zoals adressen, telefoonnummers en bankrekeningnummers.

door Pim van den Dool

Introduction: problem

- What's going on in that network?
- Too much to look for
- Many different information feeds
- Big data sets
- Hard to get an overview
- Incident driven
- Difficult to communicate

Theory: research question

What techniques can be used to visualize network hygiene?

- *That network has urgent security issues*
- *This threat occurs on those systems*
- *This customer keeps misbehaving*
- *Security has improved in this part of the network*

Data


vulnerabilities
botnets
firewalls
IDS
open resolvers
misconfigurations
notice-and-takedown
denial-of-service
AS
netblock
phishing
IP addresses
spam
honeypots

Data

Security state

- Vulnerabilities
- Abuse, NTD

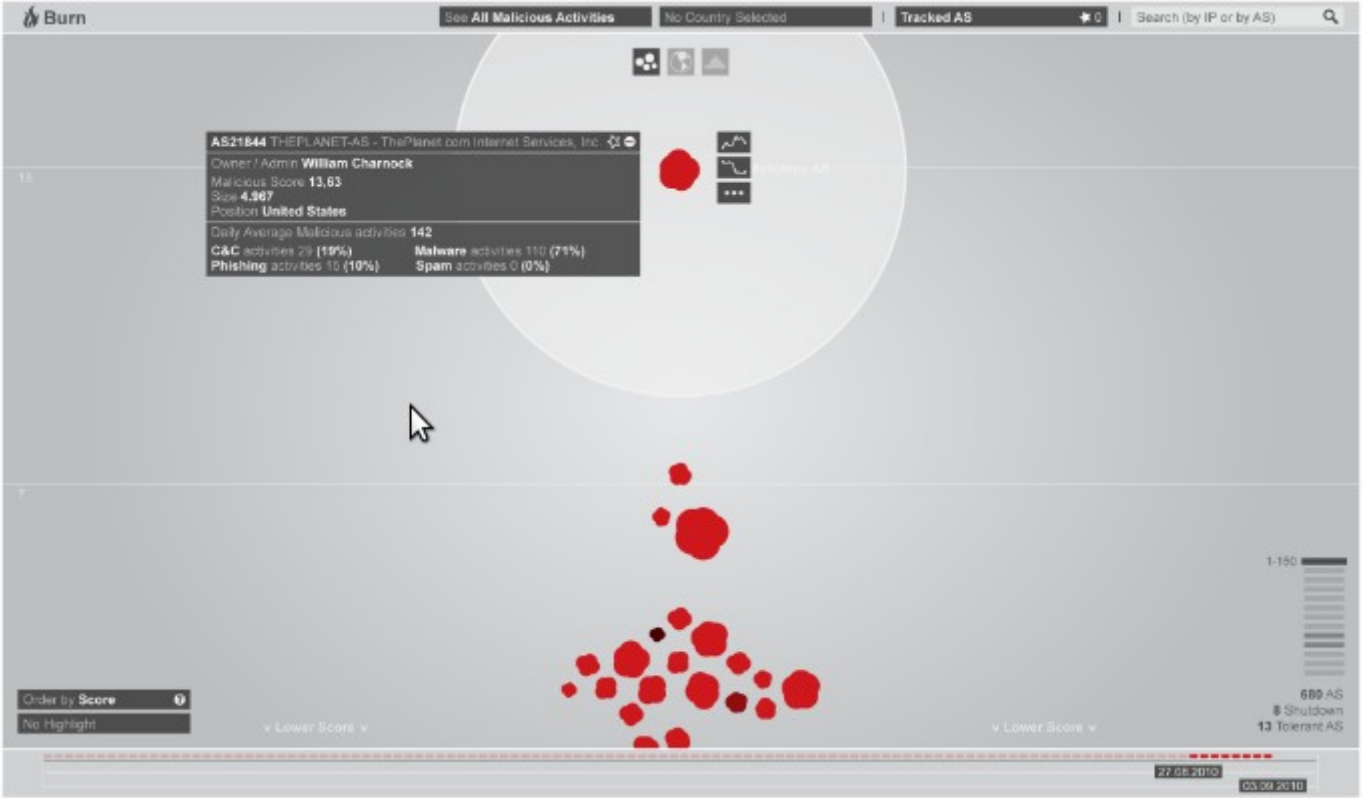
Communication

- IDS, firewalls, honeypots...

Networks

- AS's, netblocks, IP's

Visualization



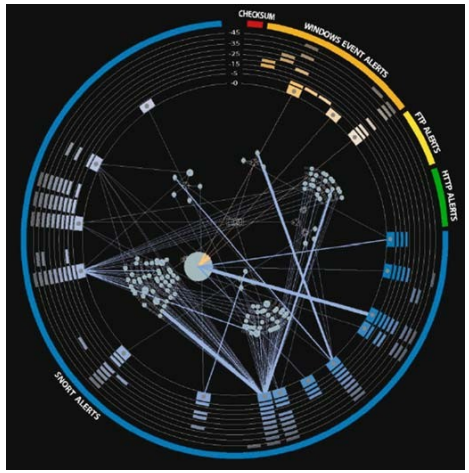
Bearing unkown rogue networks

Roveta et al. (vizsec**2011**)

Current visualisations

- NICT daedalus

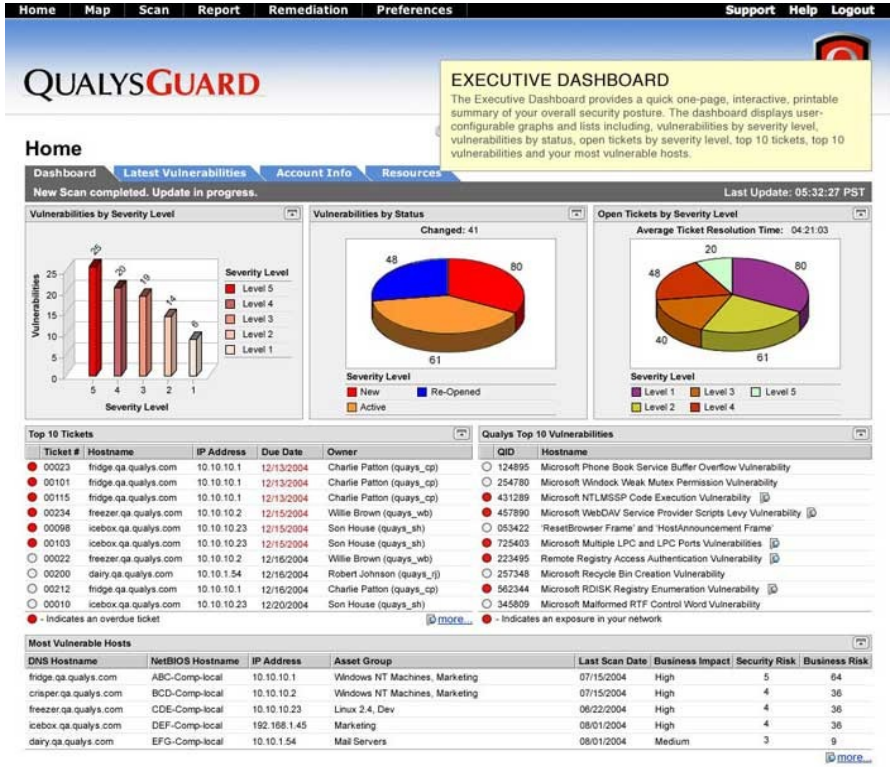
- VisAlert



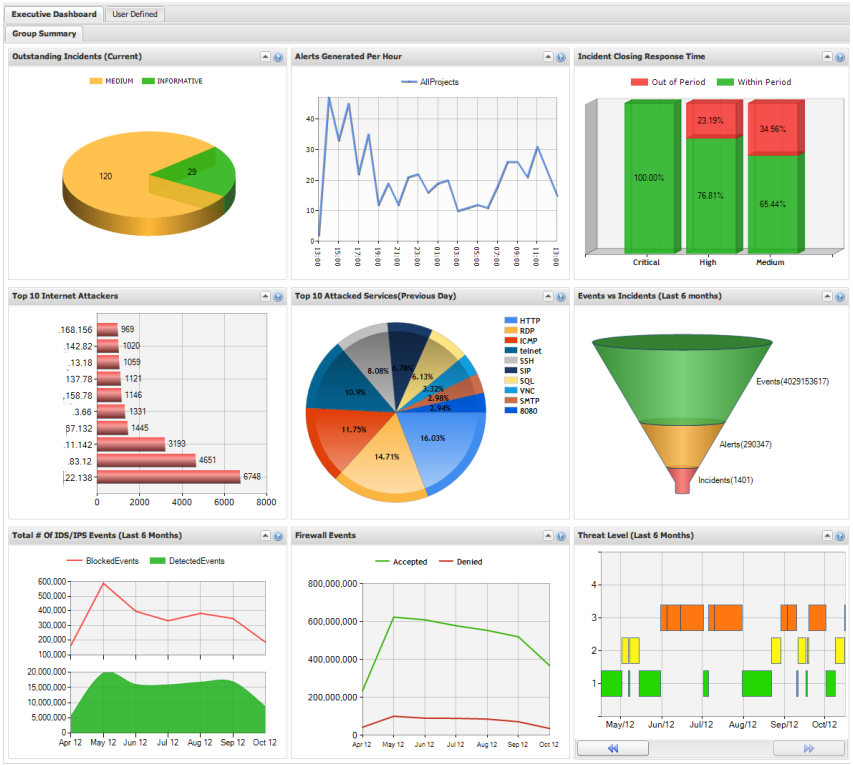
- Shadowserver

- Clockview

Current dashboards



http://www.qualys.com/



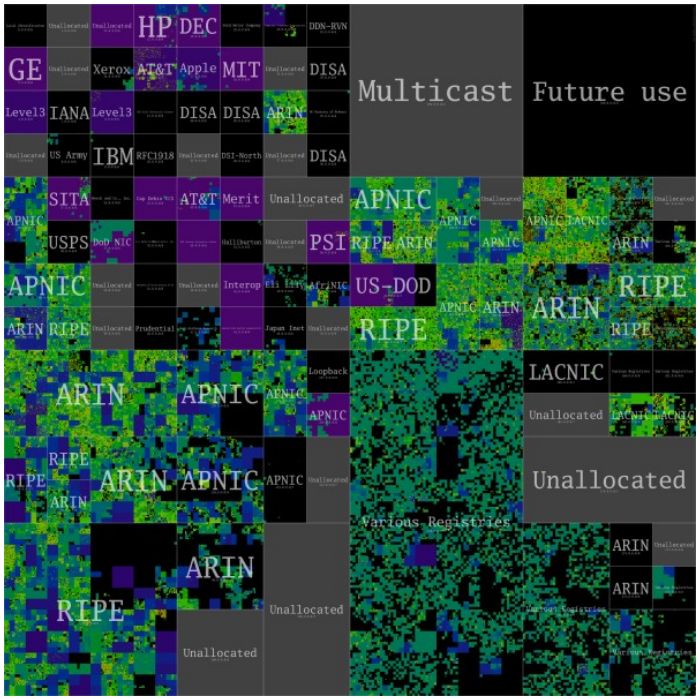
http://www.odysseyconsultants.com

Shortcomings

- Too abstract
- Too much detail
- Too complex
- Geographical visualization not actionable
- No network overview
- Limited or no interaction

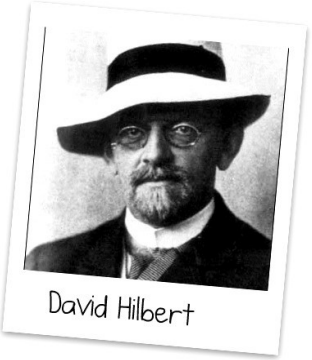
Visualizing network maps

Randall Munroe (XKCD), **2006**

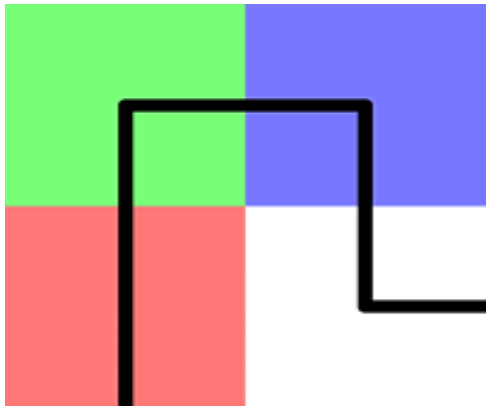


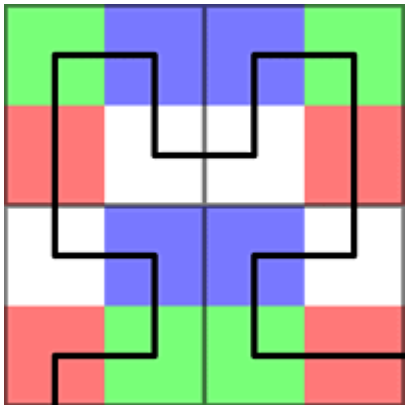
Caida.org

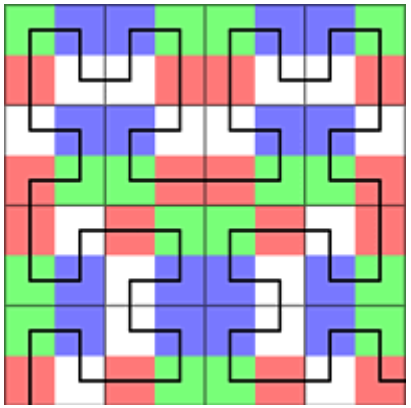
Hilbert curve



- A space filling curve
- Preserves locality



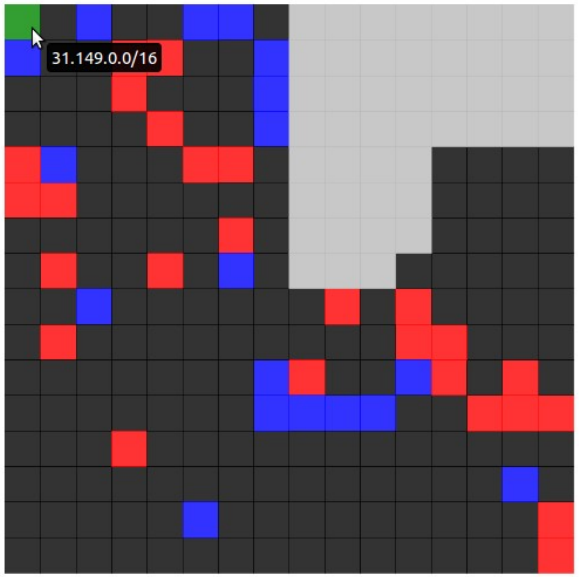


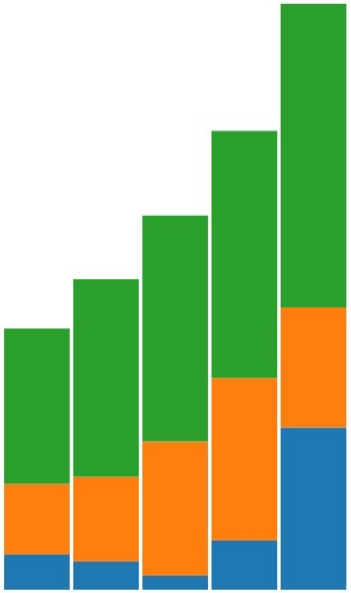


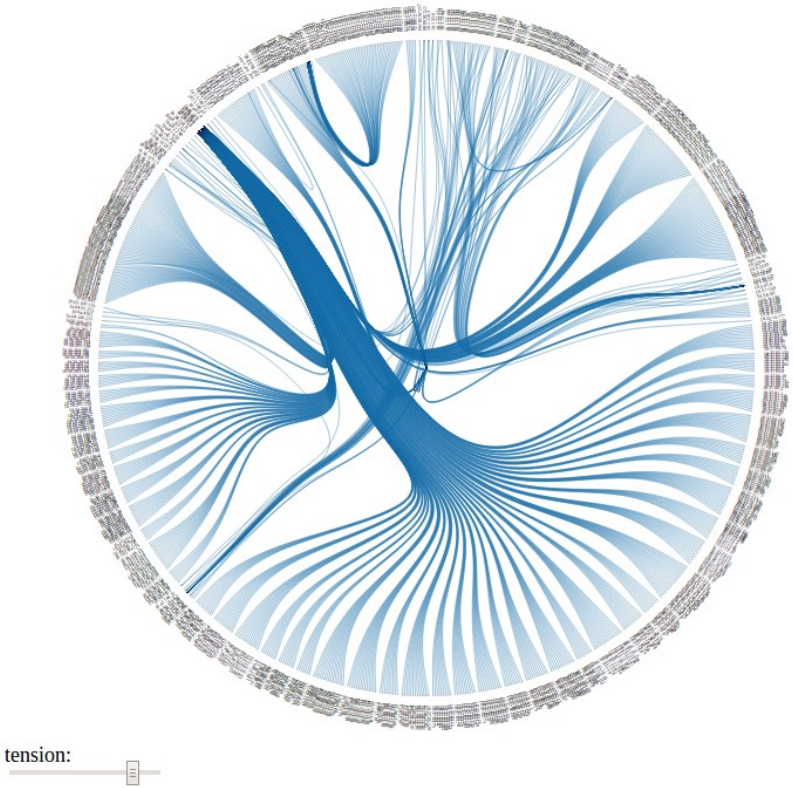
Hilbert curve visualization

- Can we actually use this for something else then an Internet map of /8's?
- CIDR?
- IPv6?
- Is it feasible to use in an interactive dashboard?

Demo



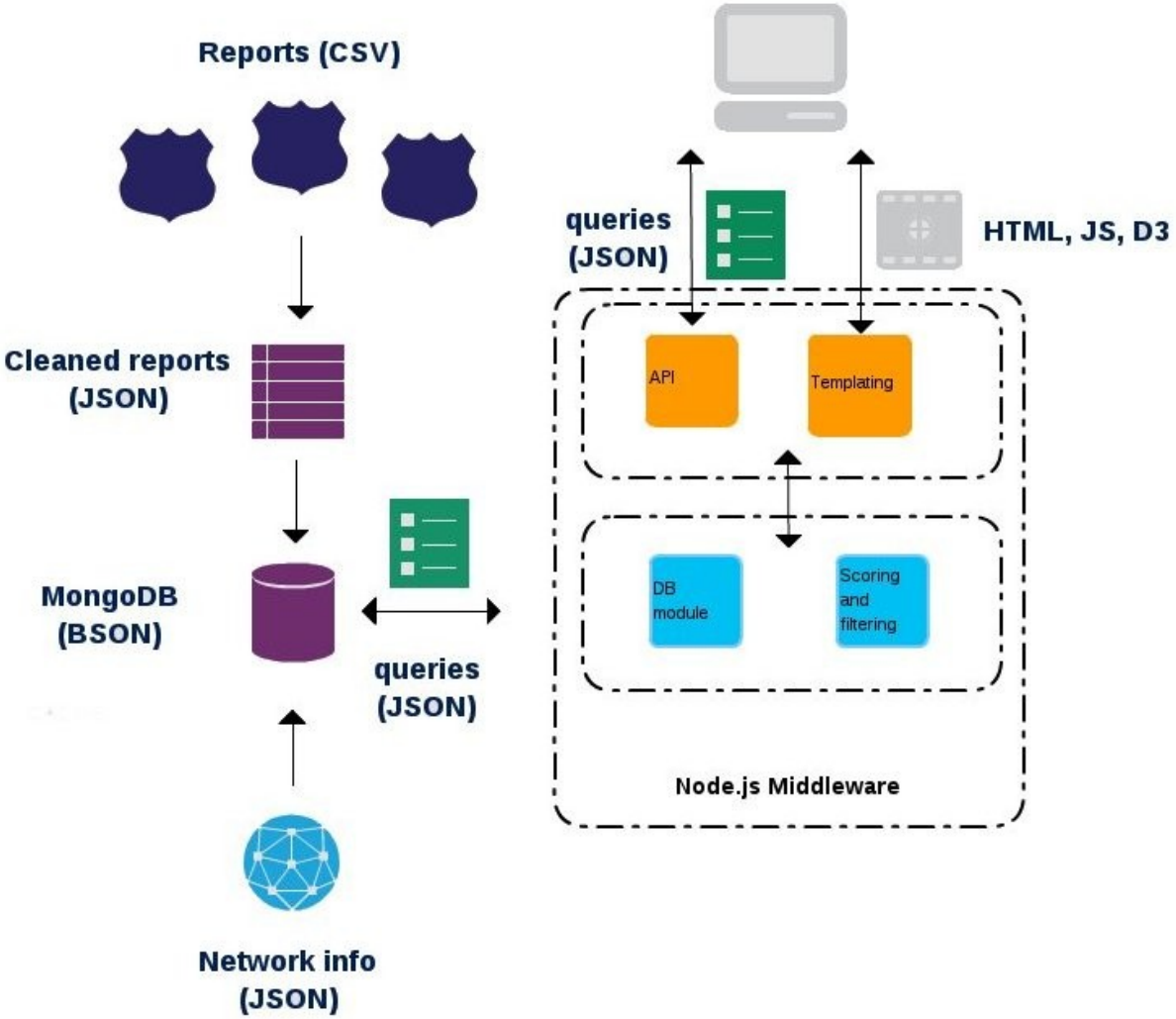




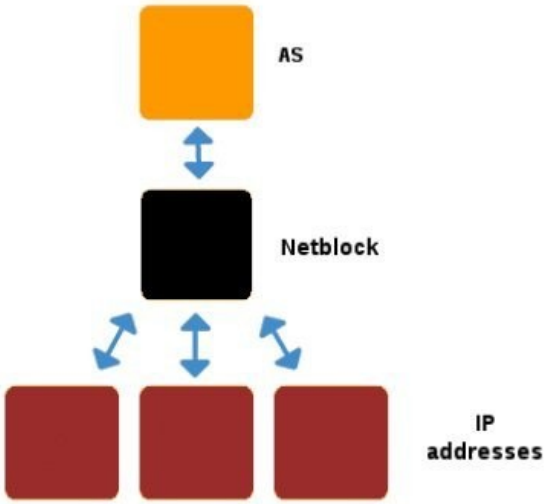
Hilbert curve implementation

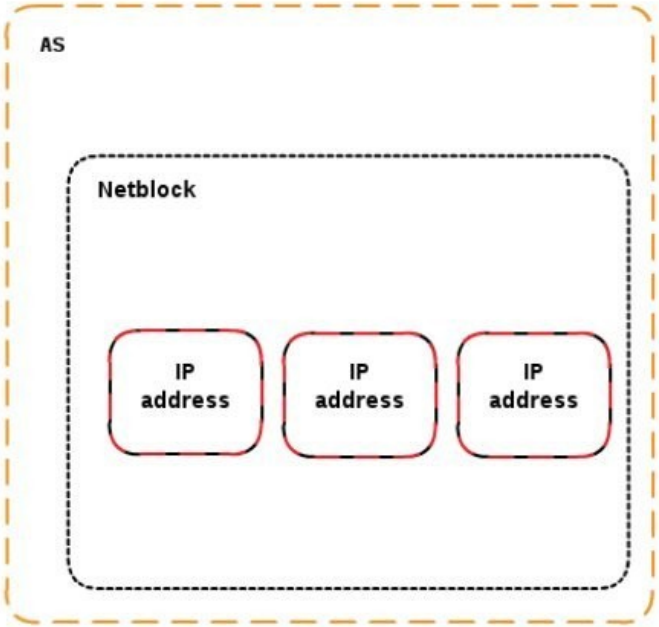
- Different depth for AS/Netblocks/IP's
- Not one same netblock size
- Level >7: 
- Higher level = too many tiny specs
- Issue for some CIDR ranges and IPv6
  - IPv4 > /18
  - IPv6
    - /48 as 256 /56's
    - /56 as 256 /64's
- Filter: IP's with no data, risk level

Architecture



MongoDB schema





Referencing or embedding

Conclusions

- Flexible and scalable architecture
- Hilbert curve useful
  - Aggregation
  - Filtering
  - Browser limitations
  - Can work for IPv6
  - Combine with statistics and traffic viz

- Poc, work in progress. Looks promising.

Questions?