Connect. Communicate. Collaborate

A Quantitative Cross Comparative Analysis of Tools for Anamoly Detection

Wayne Routly

DANTE

Riga, 20th Jan. 2008

Quite obviously….

- For a small organization, doing a quantitative cross comparison of commercial tools for network security is **lengthy** and **difficult**

Connect. Communicate. Collaborate

Moving on…

1. The Problem
2. The Tools
3. What Are We Looking For?
4. The Process
5. The RESULTS!!!
6. In Conclusion

GÉANT2

DANTE

Connect. Communicate. Collaborate

The Problem….

1. …. A Transit Network
2. +/- 10 Million Speaking Hosts Per Day
3. 10Gbps Links
4. Unusual Traffic
    1. Large FTP Transfers
    2. Legitimate SSH & DNS Traffic
5. Intercontinental Peerings

The Difficult Part….

- You must give the tools the same data
- You must understand different tool terminology
- You must tune the tools to give “similar” results
  - And you’ll never get them to see exactly the same things…
- You must not just trust the tool results, but verify them with other means
  - Raw NetFlow analysis via NfSen, exchange of evidence with friendly CERTs
- You must work out your success criteria

Lengthy…very lengthy

- It took us **more than one year**
- Preparation: 6-7 months
  - Shortlist vendors, get in touch with them, convince them to engage in a *comparative* trial with no upfront commitment, make them spell out a price figure even before the trial, set up the legal bit, get the boxes delivered, installed and configured
  - One (established) vendor pulled out (we remained with 3)
- Tool learning curve and tuning: 3-4 months
- Comparative testing: 1 month
- Result analysis and reporting: 1 month

Connect. Communicate. Collaborate

What if you can't afford all that?

1. You decide on the basis of vendor's visits (cool! ☺)
2. You buy the cheapest, or the more expensive, but not what you need (cool! ☺)
3. You buy what others have bought, for their own network and needs (cool! ☺)
4. You don't buy at all (cool! ☺)

- We're showing some results, today, but we don't want you to convince to buy either or the two (best performing tools) we tested
- But we'd very much like to discuss how small CERTs could share these experiences (**and that'd be really cool!** ☺)

The Good Stuff…the Tools

- StealthWatch – Lancope
  - Per Host Behavioral Analysis
  - Requires 1 Point to be Defined
  - Normally Found in Campus Networks
- Netreflex - Guavus
  - Fuses BGP & ISIS Data
  - Creates a 18 x 18 Router Matrix

Connect. Communicate. Collaborate

The Process…

- 13 days of cross comparative testing (balancing MM - WR)
- 1066 Investigated anomalies, results precision bounds estimated
- 14 Anomoly Types
- Analyzed raw netflow using nfsen
- Certain Events forwarded to CERTS for Confirmation

GEANT2

DANTE

Connect. Communicate. Collaborate

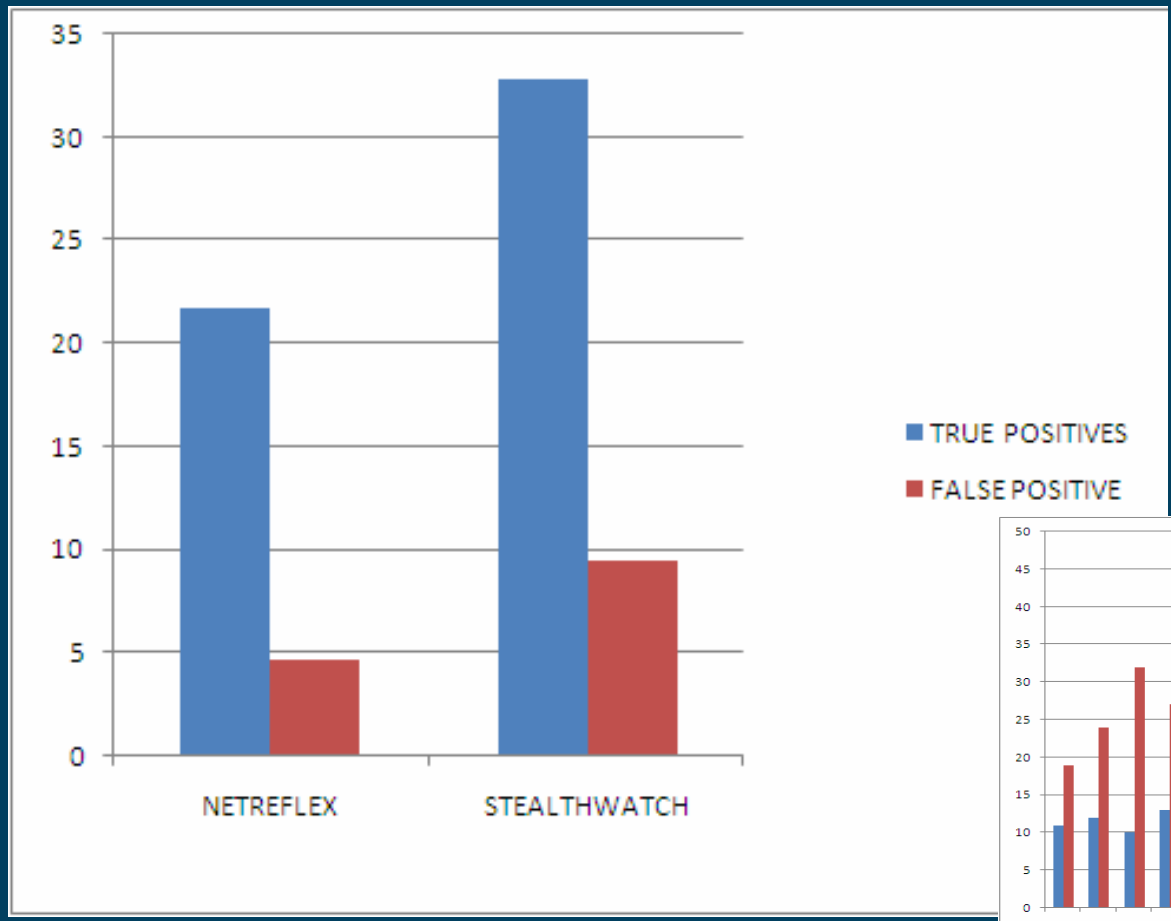
THE RESULTS

GÉANT2

DANTE

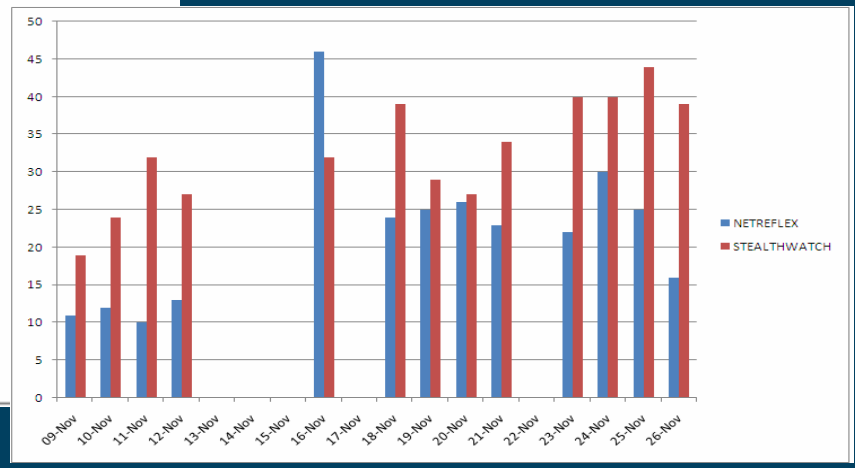
Connect. Communicate. Collaborate

True and False Positives



SW 32.8 anomalies per day, followed by NetReflex (21.7)

Number of false positives is 28% in SW, 21% in NetReflex

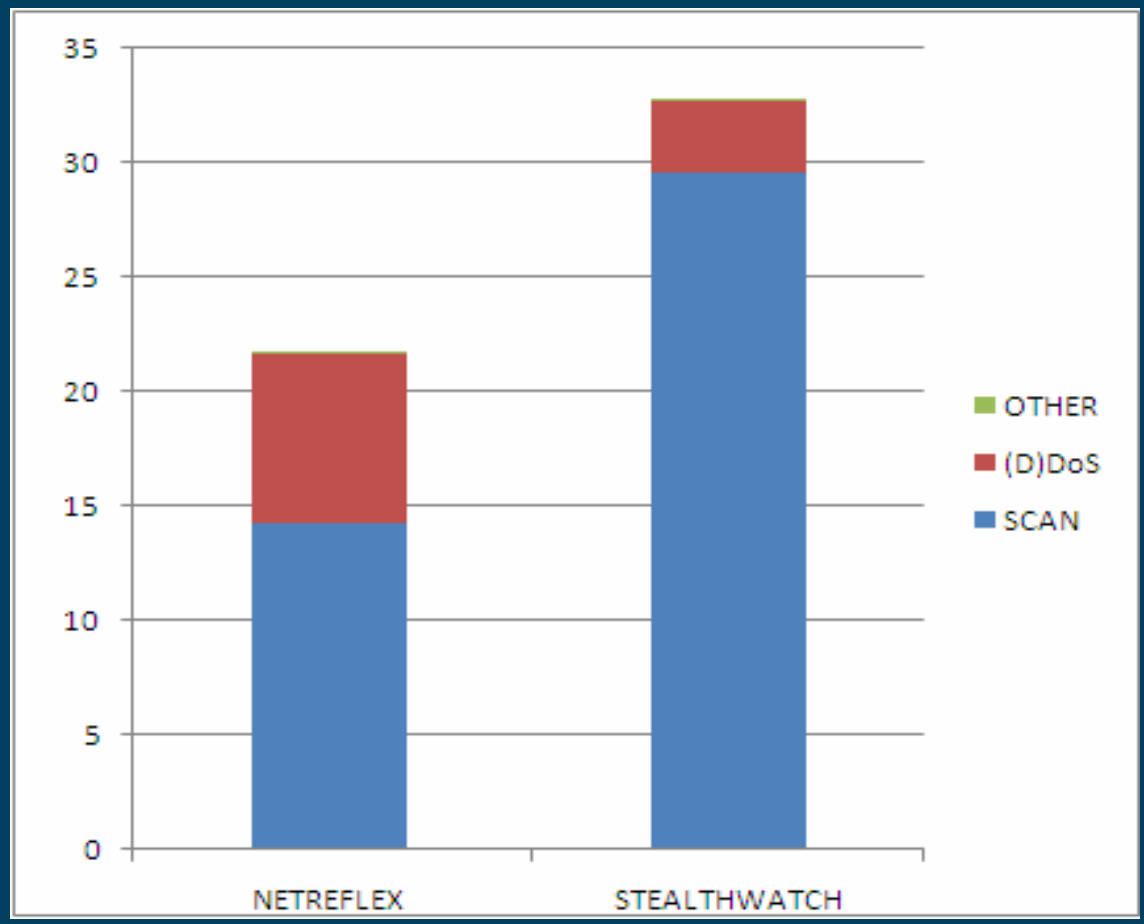


GÉANT2

DANTE

Type of Anomolies

- Scan vs DoS
- Other?
- No. of Anomolies Per Tool



Scan types

Connect. Communicate. Collaborate

	StealthWatch	NetReflex
Port scans (all ports)	Rare	Some
Ports 135, 139, 445 (windows file sharing)	A lot	- (*)
Port 22 (ssh)	A lot	A lot
Port 23 (telnet)	Some	-
Port 53 (DNS) Port 80 (Http) Port 1433 (SQL)	- Rare Rare	Some - - (*)
ICMP scans (ping)	Some	-

GEANT2

DANTE

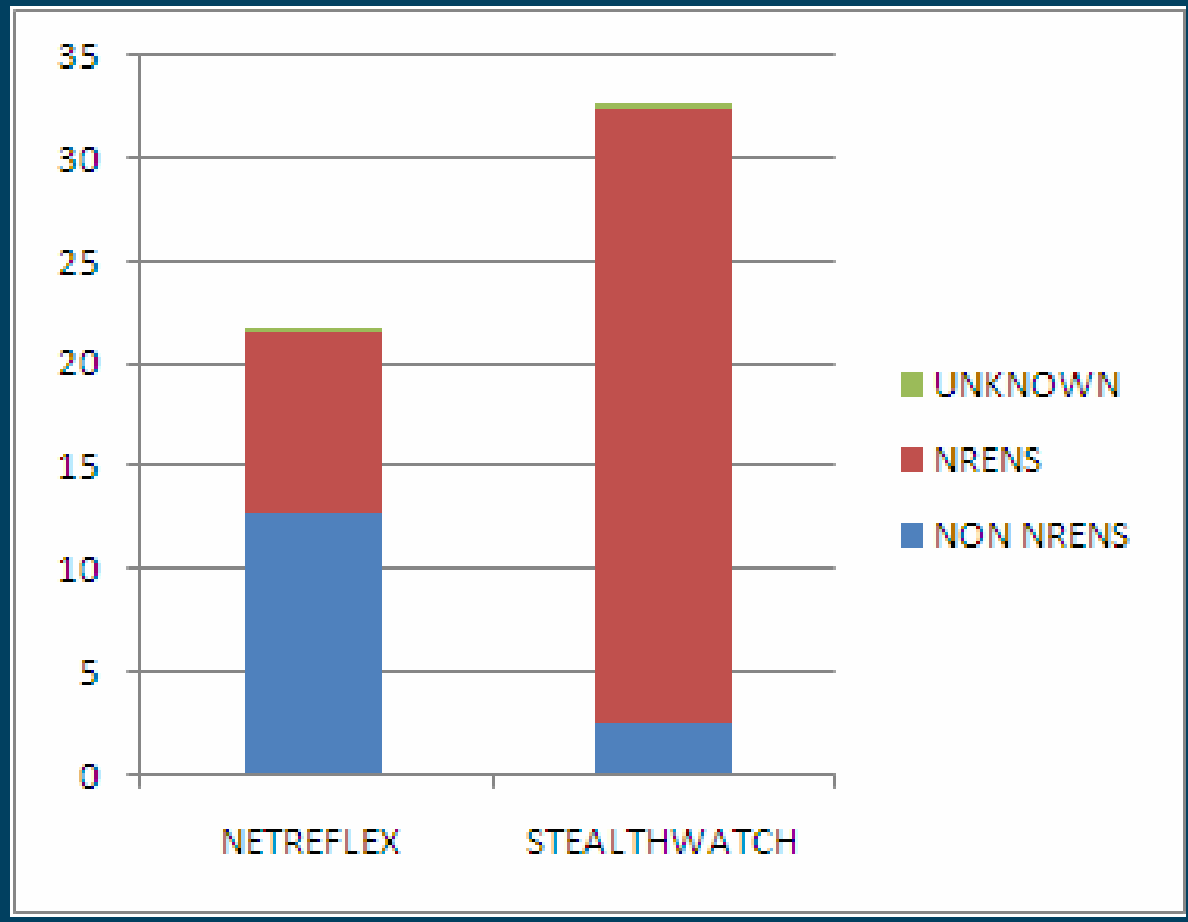
Connect. Communicate. Collaborate

(D)DoS types

	StealthWatch	NetReflex
UDP (small packets)	Rare	A lot
TCP (syn floods)	Rare	Some
ICMP floods (large packets)	Rare	-

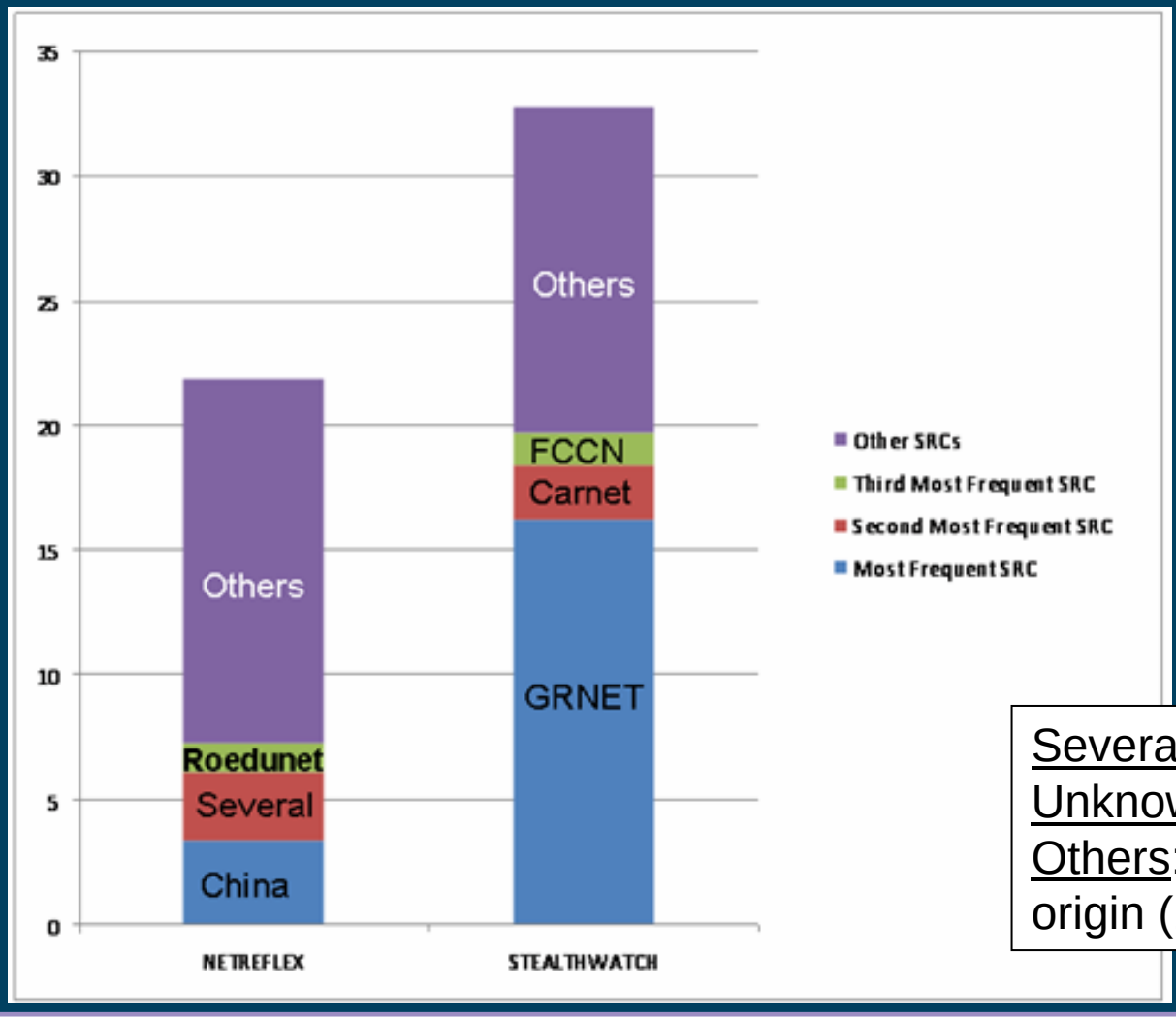
Origin of Anomalies (1/2)

- Stealthwatch & NRENS
- Unknown?
- Netreflex Balanced



Origin of Anomalies (2/2)

Connect. Communicate. Collaborate



- DWS Clients =GRNET
- Several?
- International SRC's versus NRENs?

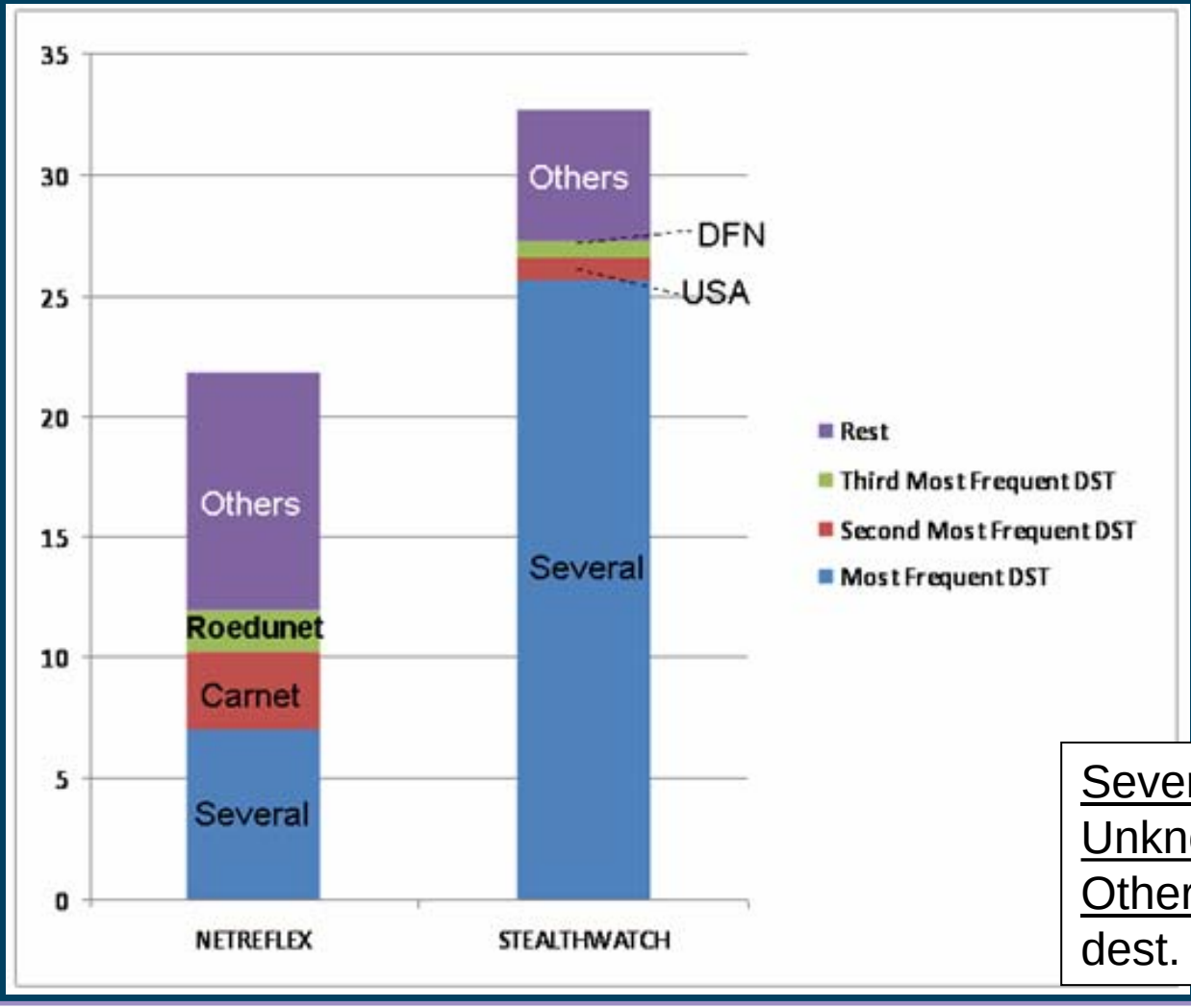
Several: multipoint origin
Unknown: could not track origin
Others: 1 single, identified origin (but not within top 3)

GEANT2

DANTE

Destination of Anomalies

Connect. Communicate. Collaborate



- SW, Scans & NRENS
- NR versus SW

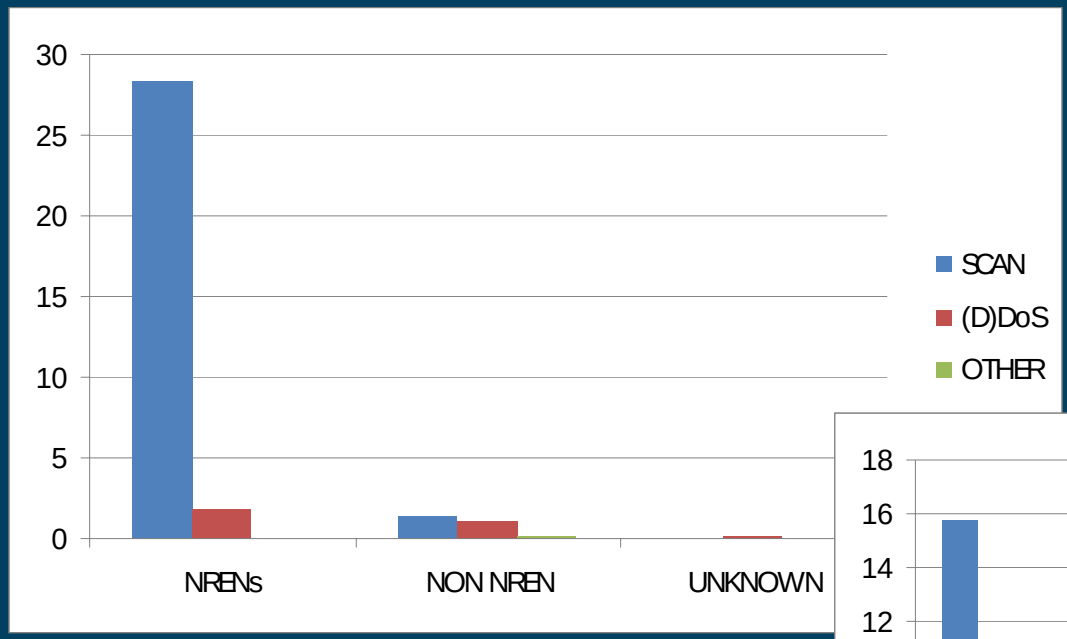
Several: multipoint dest.
Unknown: could not track dest.
Others: 1 single, identified dest. (but not within top 3)

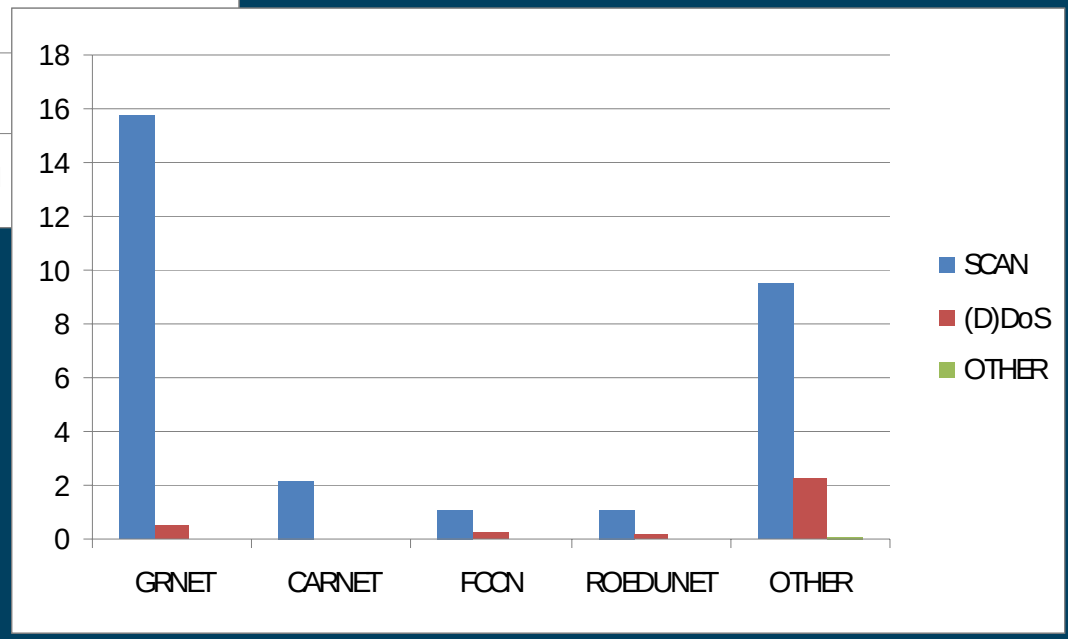
GEANT2

DANTE

Origin and type: SealthWatch

Connect. Communicate. Collaborate





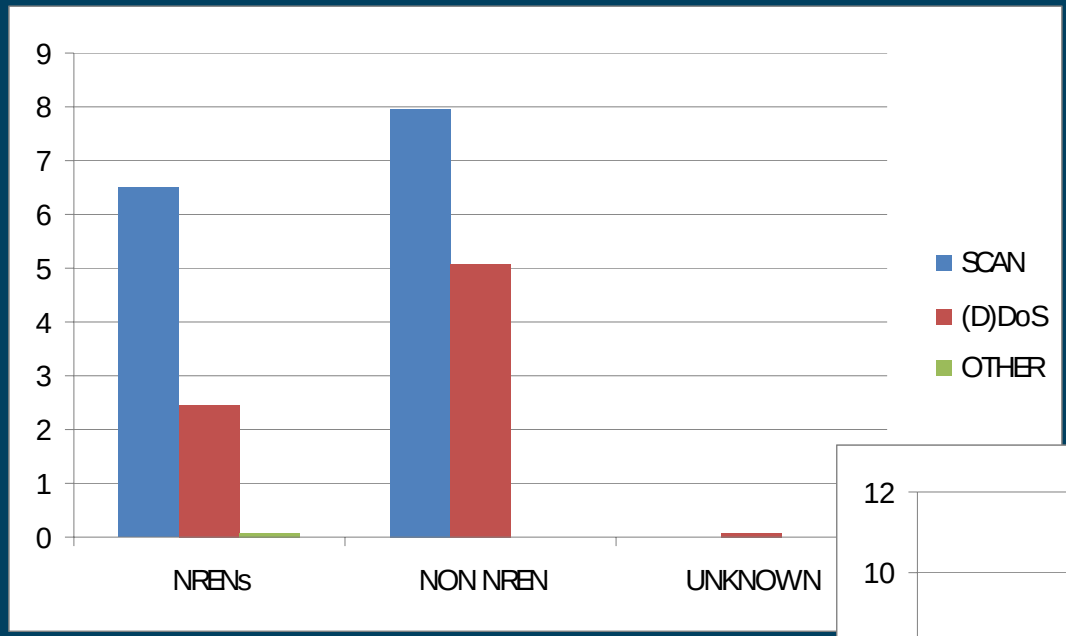
- SCANS Feature Prodominatly
- Primarily NRENS as SRCs

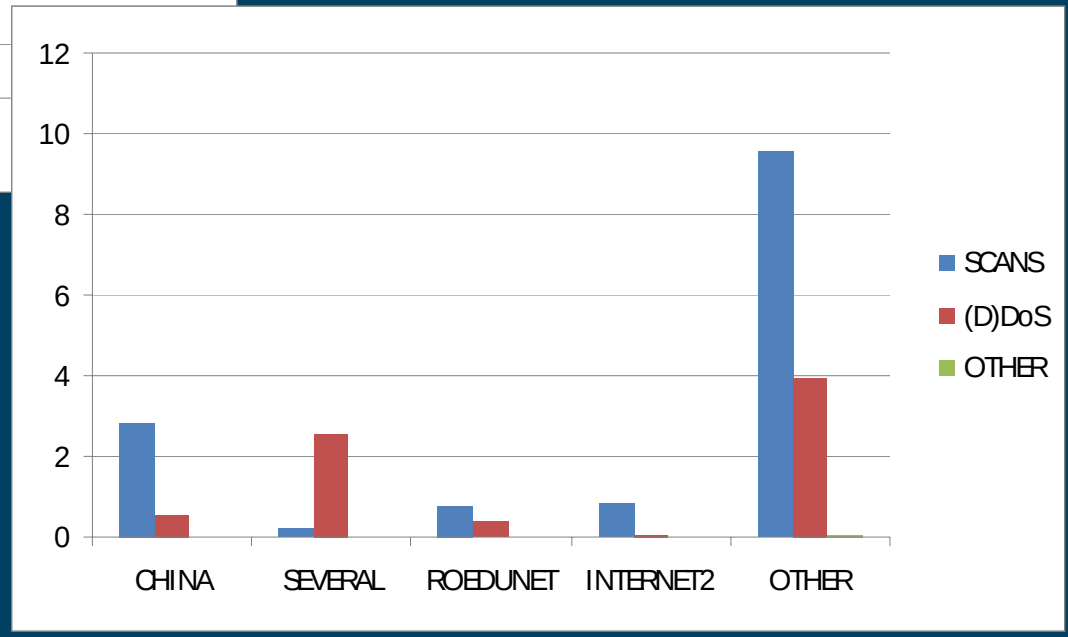
GEANT2

DANTE

Origin and type: NetReflex

Connect. Communicate. Collaborate





- Fair Anomaly Type Distribution
- Dispersion of NREN & Non NREN SRCs

GÉANT2

DANTE

In Conclusion

- Aquired Anomaly Detection Tools To Trial
- Installed, Configured, Tweaked….and Tweaked Again
- Captured & Investigated over 1000 events in 13 days
- Cross-compared results amongts all tools and validated results
- …..and the descision is ??????

Connect. Communicate. Collaborate

Questions?

THANK-YOU

GÉANT2

DANTE