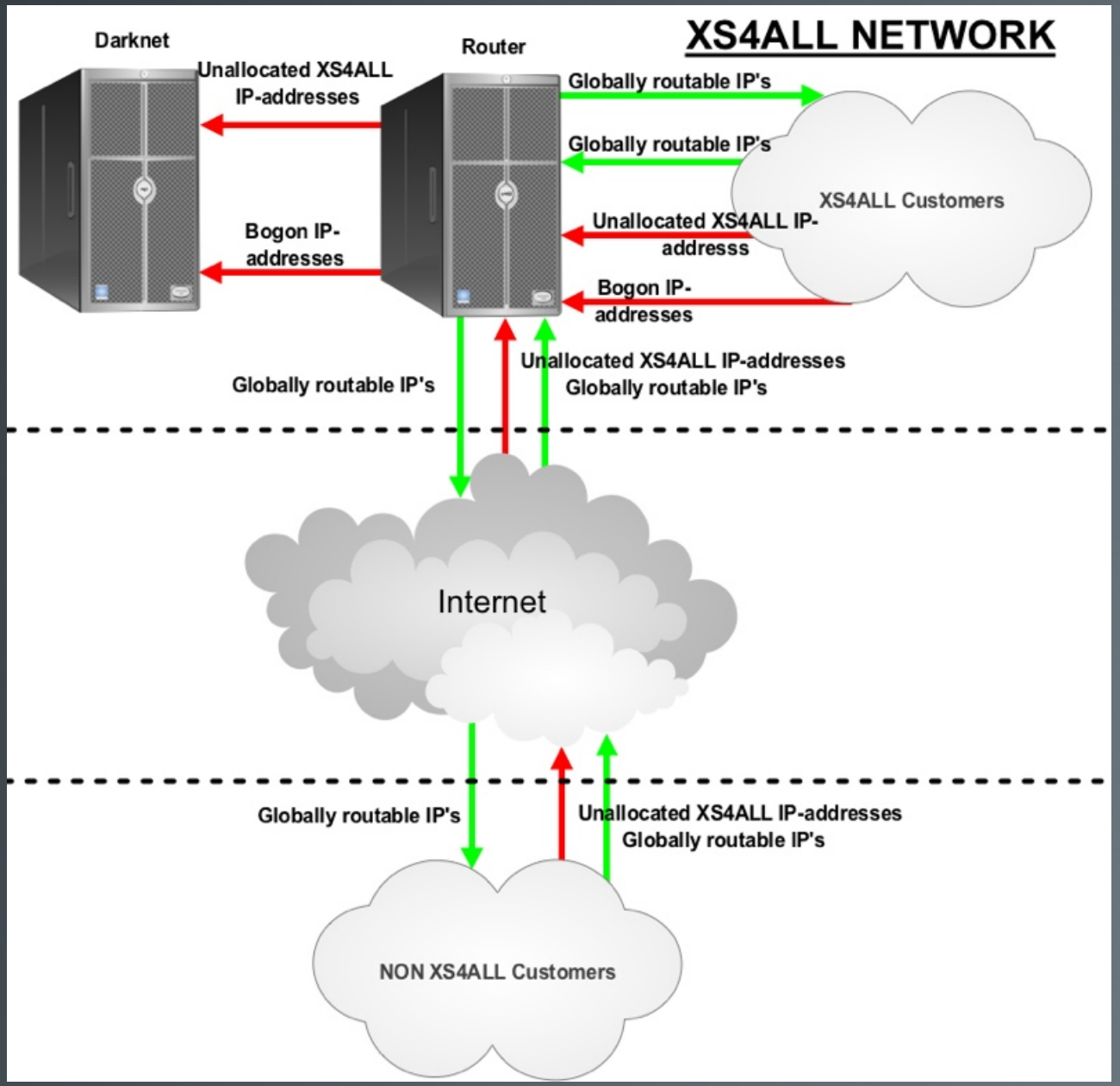

PROJECT
DARKLIGHT

Overview

- XS4ALL Darknet
- Research question
- Argus
- Research
  - Results
  - Zero day warning system
  - Internet Security Index
- Conclusion
  - Future work

- Darknets
- Traffic to the XS4ALL darknet
  - For everyone
    - Not used XS4ALL space
  - For XS4ALL customers
    - Not used XS4ALL space
    - Bogon IP's
- Argus
- No response

XS4ALL Darknet



Research question

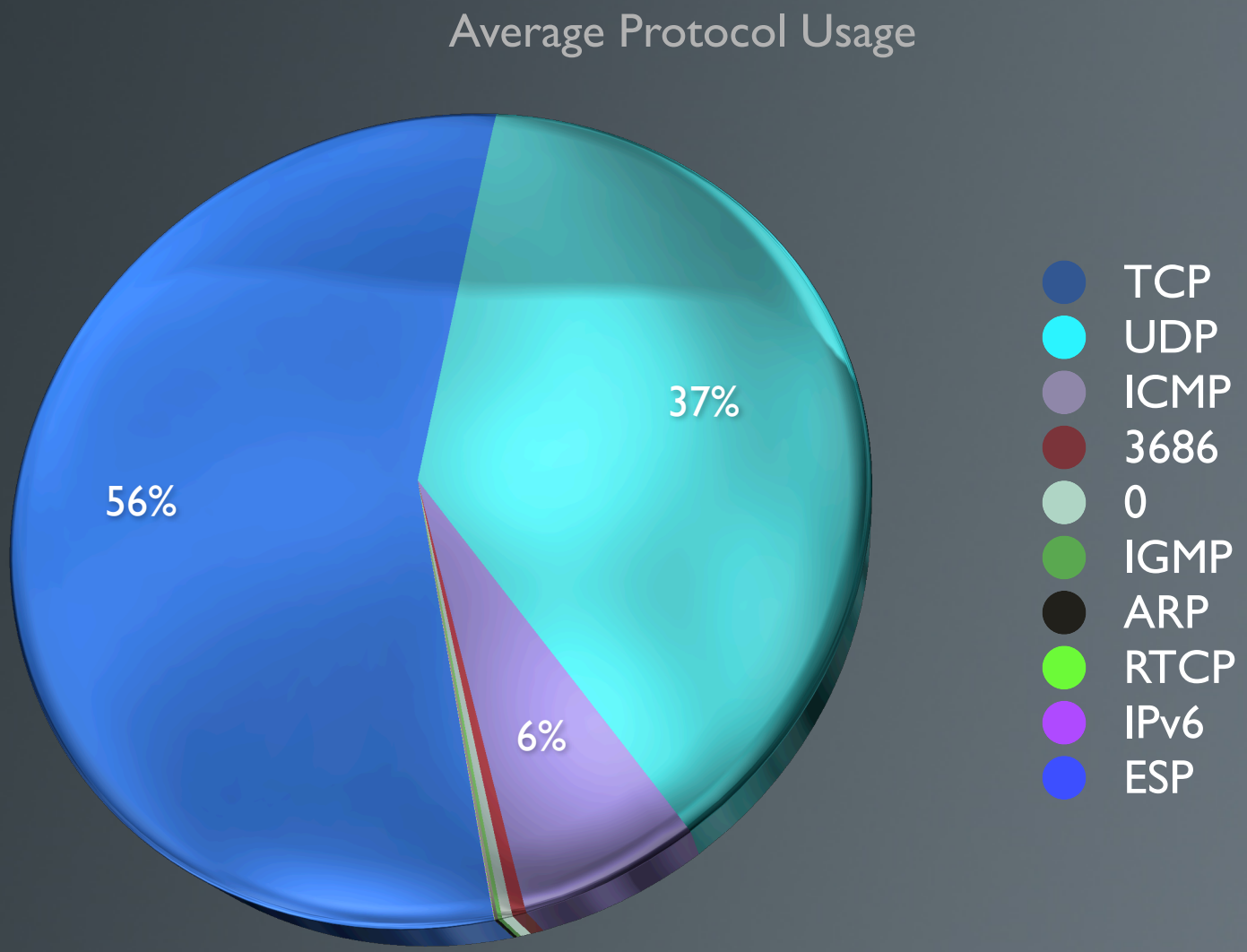
"What information can be gained from the captured XS4ALL Darknet streams, and could it be used as a zero day warning system?"

Argus

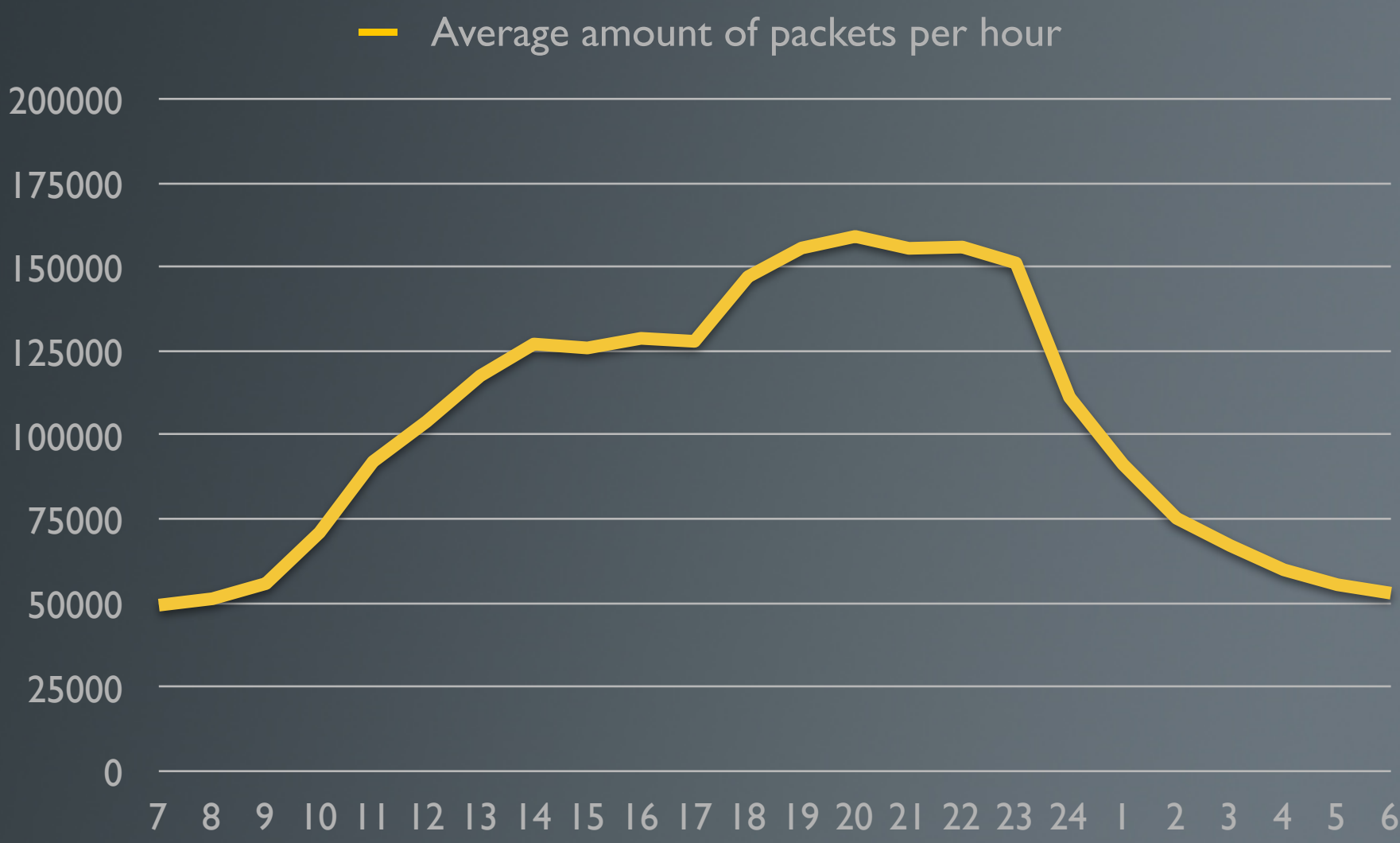
- Real time flow monitor
- Fields
  - Source and destination IP address
  - Source and destination port
  - Type protocol
  - Start time
- UDP first 712 bytes payload
- 4 Months of data
- Argus tools

- Port scans
- IP scans
- IP patterns
- Port patterns
- Time patterns

Research - Protocol usage

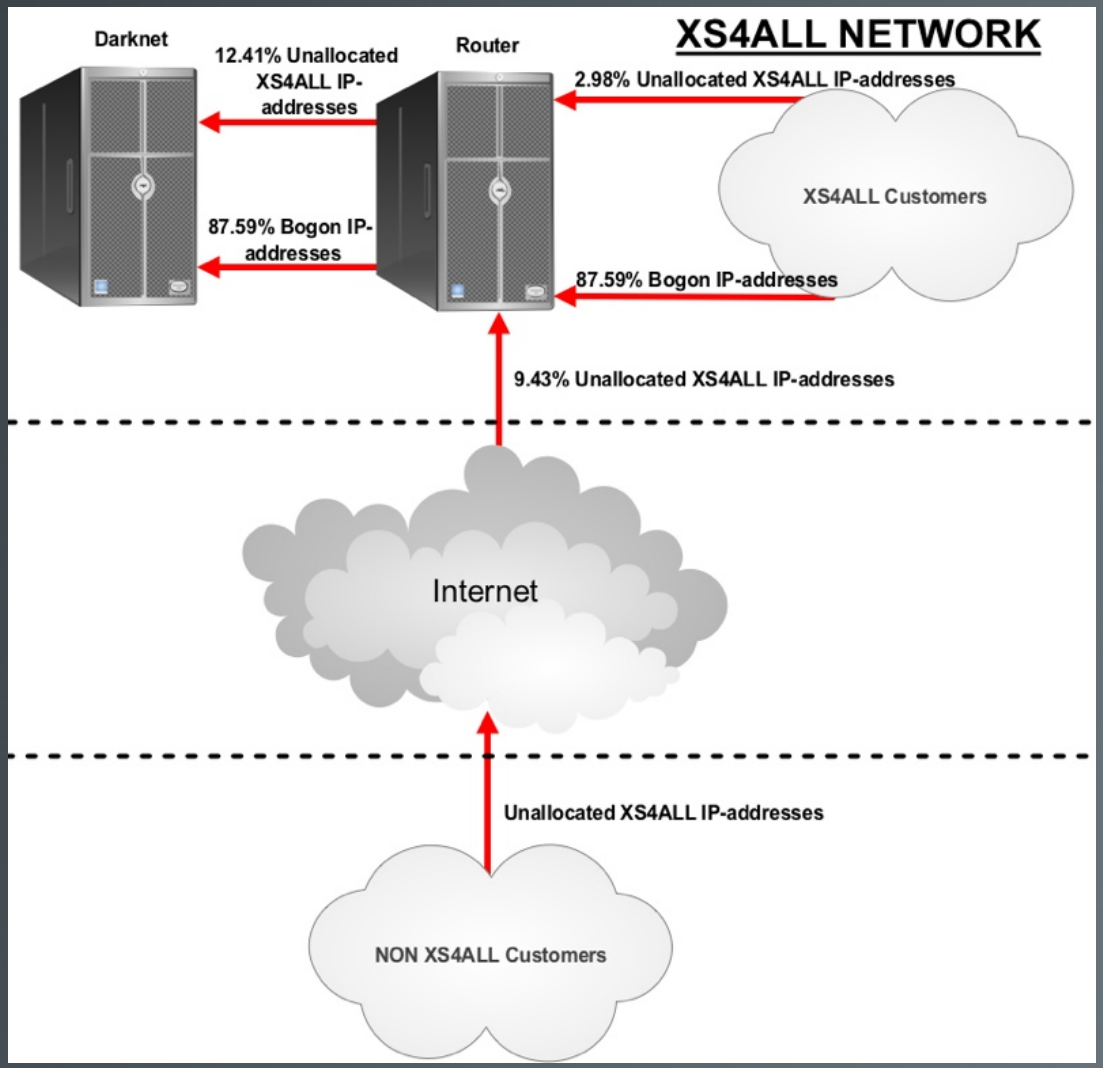


Research - Time pattern



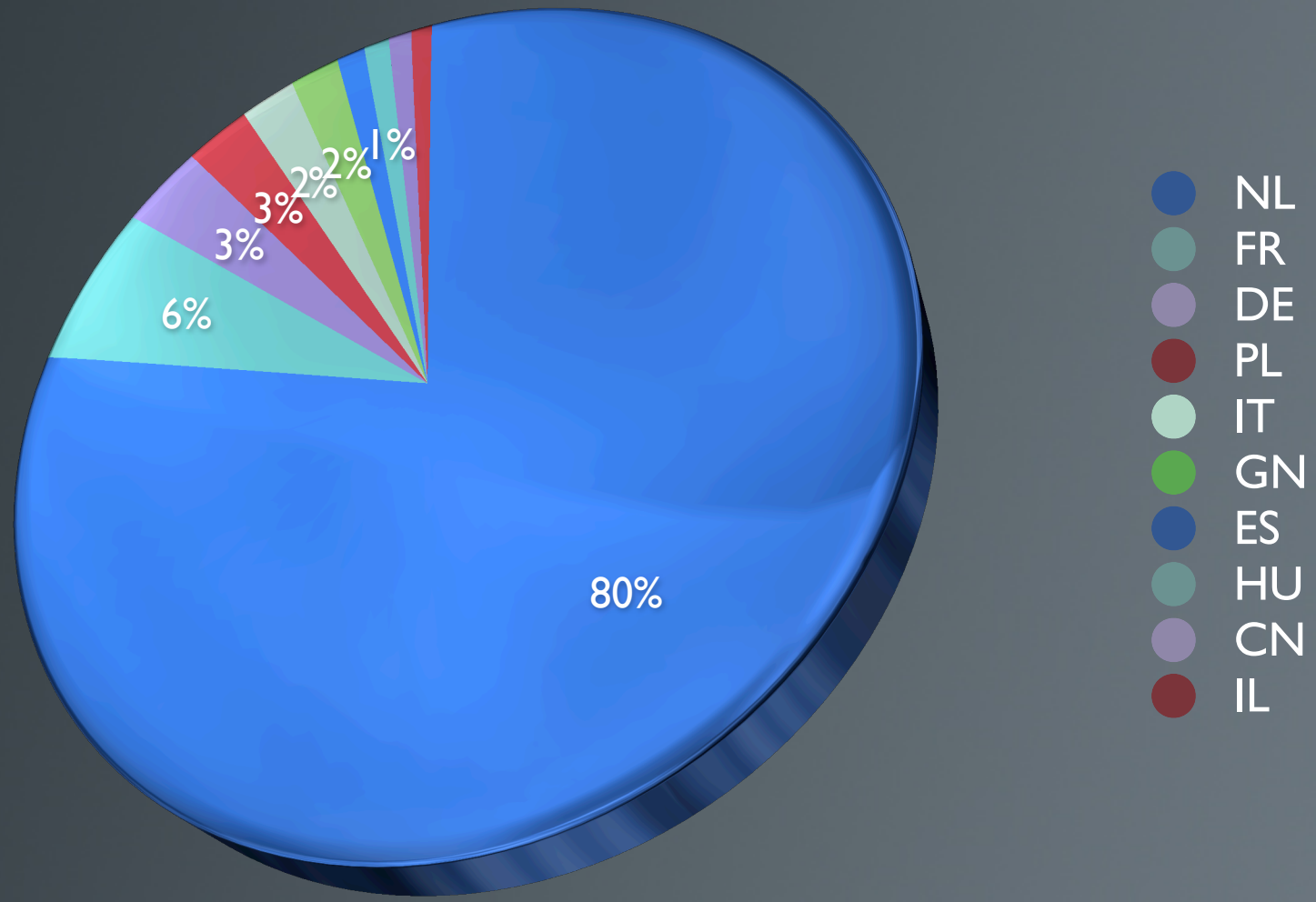
- Why
  - Misconfiguration
  - Viruses, worms and malware
  - Scans
- From where
  - Countries
  - Customers
  - Non customers

Research - Traffic streams



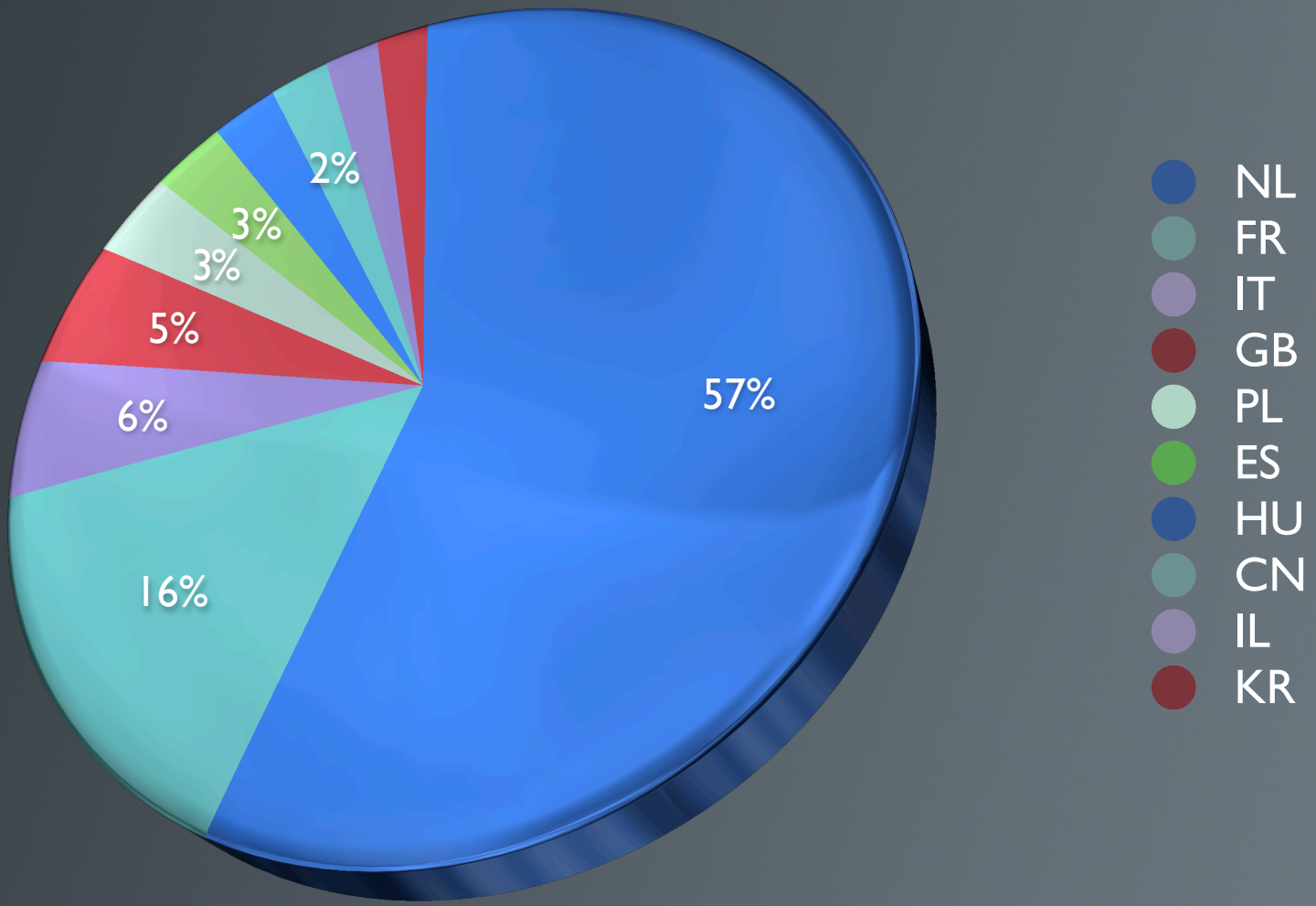
Research - Country origin

Country origin of traffic to not used XS4ALL space



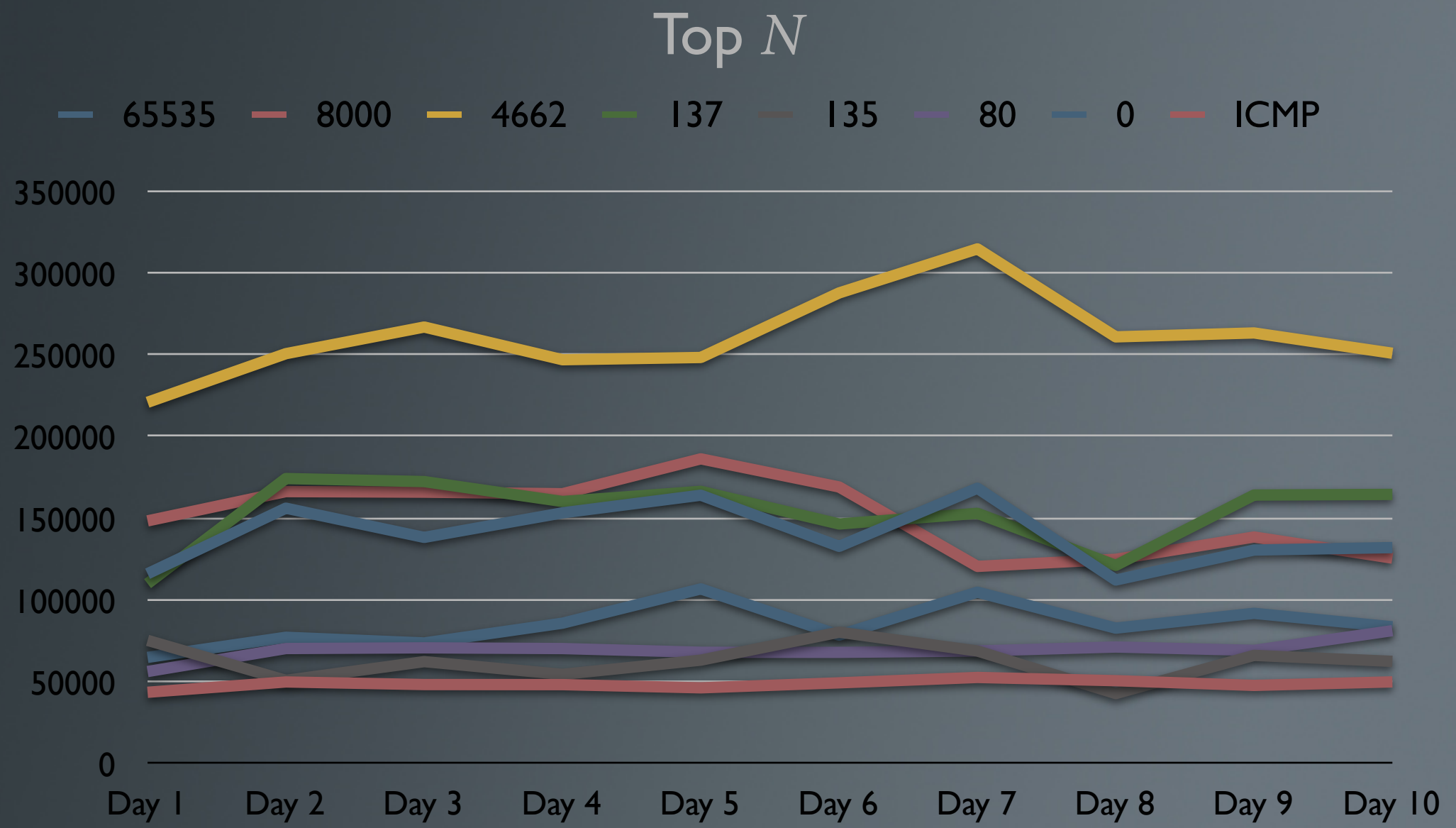
Research - Country origin

Country origin of traffic to not used XS4ALL space, without XS4ALL customers



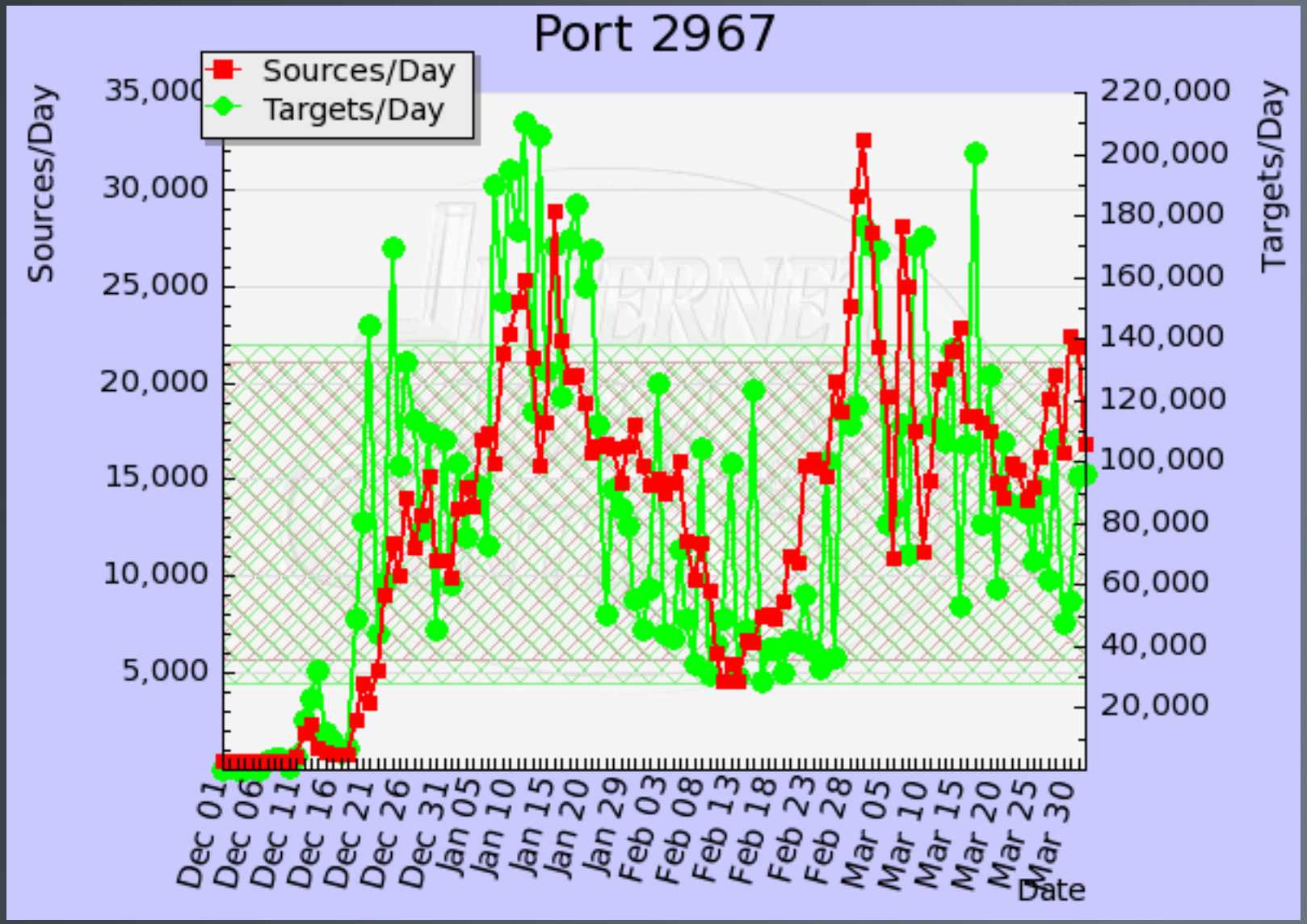
- Top N
- Baseline
- Trends

Research - Port analysis



Research - Port trends

The coming of the SAV worm



Research - Port trend analysis

- Trends calculation with baseline
- Effective to detect upcoming popularity of ports
- Important to define minimum port frequency
- Otherwise:

62.50% - Portnumber: 12149 - Port amount: 13 - Overallaverage: 8
40.00% - Portnumber: 12186 - Port amount: 7 - Overallaverage: 5
34.21% - Portnumber: 12183 - Port amount: 51 - Overallaverage: 38
25.00% - Portnumber: 12165 - Port amount: 10 - Overallaverage: 8
18.52% - Portnumber: 12210 - Port amount: 32 - Overallaverage: 27
18.18% - Portnumber: 12204 - Port amount: 13 - Overallaverage: 11
16.67% - Portnumber: 12188 - Port amount: 7 - Overallaverage: 6

Zero day warning system

- Identify and notify upcoming threats in an early stage
- Trend analysis of darknet data
- Top N analysis

- Total amount
- Rapid increase
- Port rating
- IP rating

Conclusion

- IP origin, country of IP address
- Protocol usage
- Time patterns
- Port patterns

- Zero day warning day
  - Trend analysis
  - Top N

Future work

- Cooperate with Dshield / Internet Storm Center
- Build zero day warning system
- Build internet security index
- Build abuse messages system

Questions