

# Tracking global wide configuration errors

**Jérôme François, Radu State, Olivier Festor**

**Madynes**

**Email : [state@loria.fr](mailto:state@loria.fr)**

**LORIA-INRIA  
France**

**MADYNES**

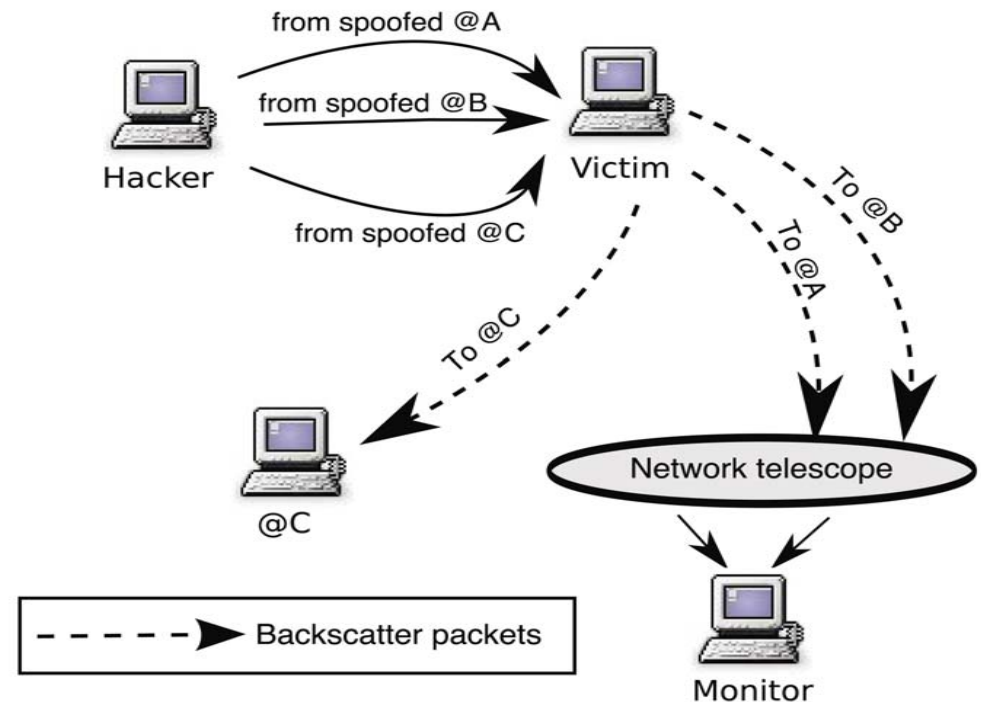
# Outline

- Introduction
  - Network Telescope
  - Honeypots and honeynets
- Research challenges
- Contributions
  - Intersection graphs: method and applications
  - Configuration errors analysis
  - Security policy changes
- Conclusions

Note : (Some graphics have been made from images of the Wikicommons project )

# Network Telescopes

- Unused IP addresses monitoring (a subnetwork)
- CAIDA project: size /8
- Few days per month
- Backscatter packets
  - Denial of service
  - Hide the identity
  - Pass through the firewalls
  - Mirrored attack
  - **More than 2 milliards of packets from may to december 2004**



V. Yegneswaran, P. Barford, and D. Plonka, "The design and use of internet sinks for network abuse monitoring," 2004.

D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," 2006.

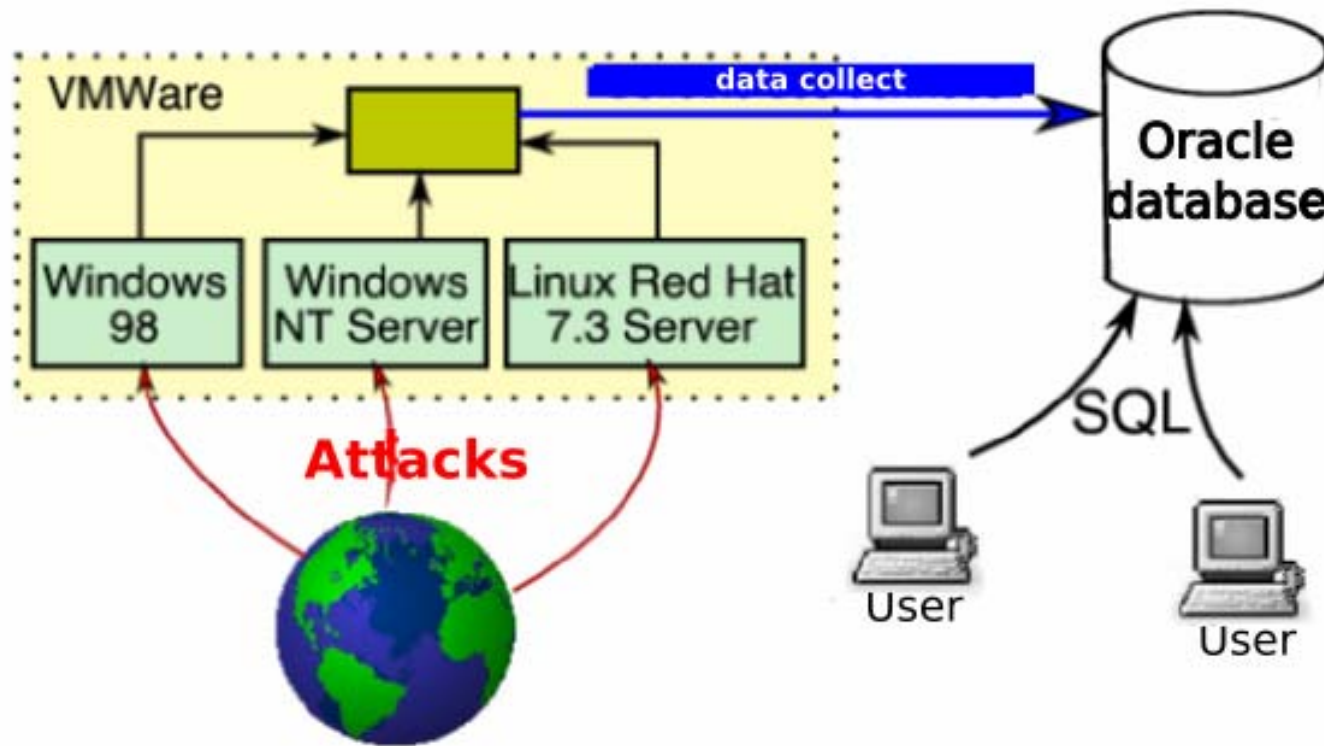
K. E. Giles, D. J. Marchette, and C. E. Priebe, "On the spectral analysis of backscatter data," 2004.

C. Shannon, D. Moore, and E. Aben, "The caida backscatter-2004-2005 dataset - may 2004 - november 2005"

# Honeytrap and Honeytrap

Leurre.com project: data for all days (11 millions of packets from may to december 2004)

43 platforms worldwide



*F. Pouget and T. Holz, "A pointillist approach for comparing honeypots," 2005.*

*F. Pouget, M. Dacier, and H. Debar, "Attack processes found on the Internet," 2004.*

*F. Pouget and M. Dacier, "Honeytrap-based forensics," 2004.*

# Research challenges

## Comparison of honeynets and telescopes

- Kind of analysis
- Results

## Use of a generic method

- For honeynets and telescopes
- Analyze aggregated data and track temporal evolution

## Configurations errors analysis

- Firewalls and routers configurations

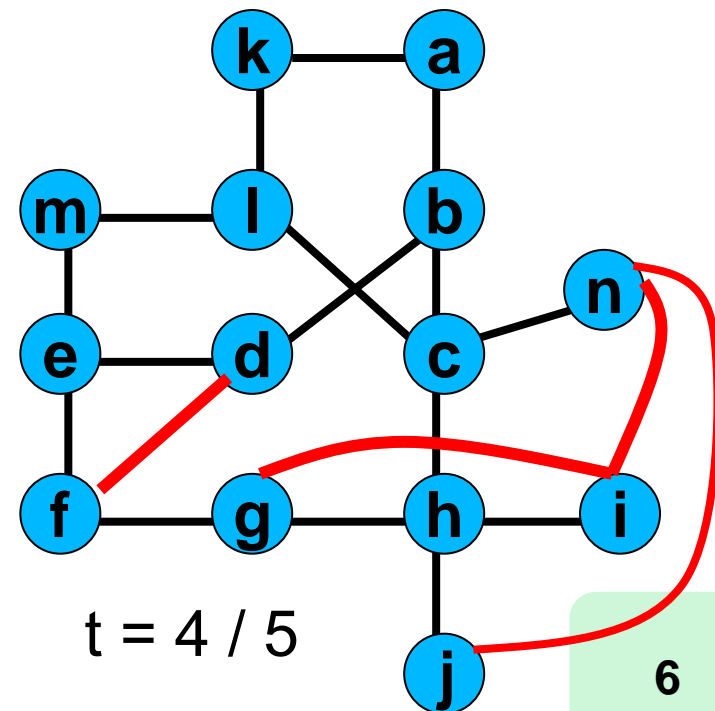
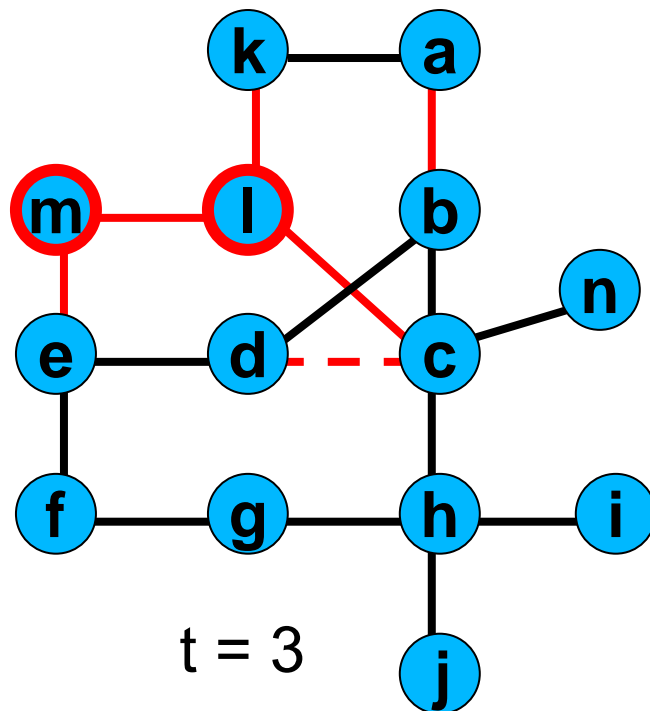
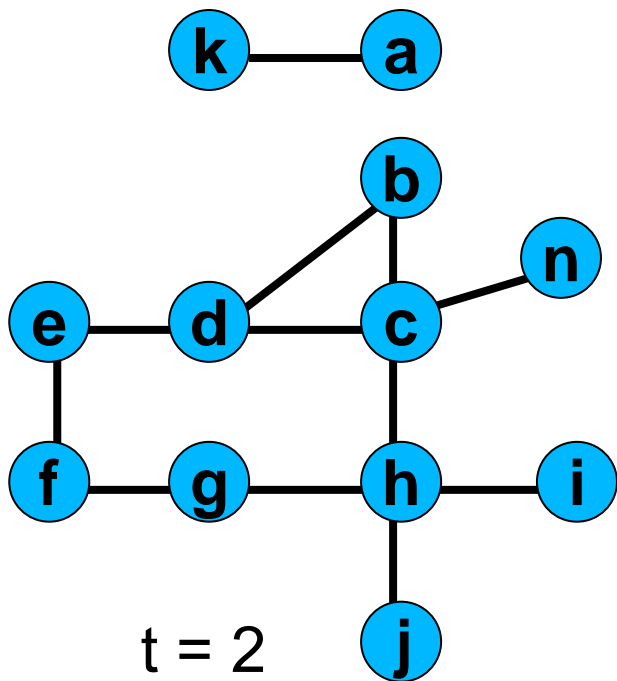
## Security policy modifications

# Centrality in a graph at a time moment

Detect topology changes  $\rightarrow$  variations of the maximal centrality (Locality)

$\psi_k(v) = \#edges \text{ of the subgraph of the } k \text{ nearest neighbors of } v$

$$M_k = \max_{v \in \text{vertices}} \psi_k(v)$$



# Tracking topology changes

Topology changes  $\rightarrow$  variations of the maximal centrality (Locality)

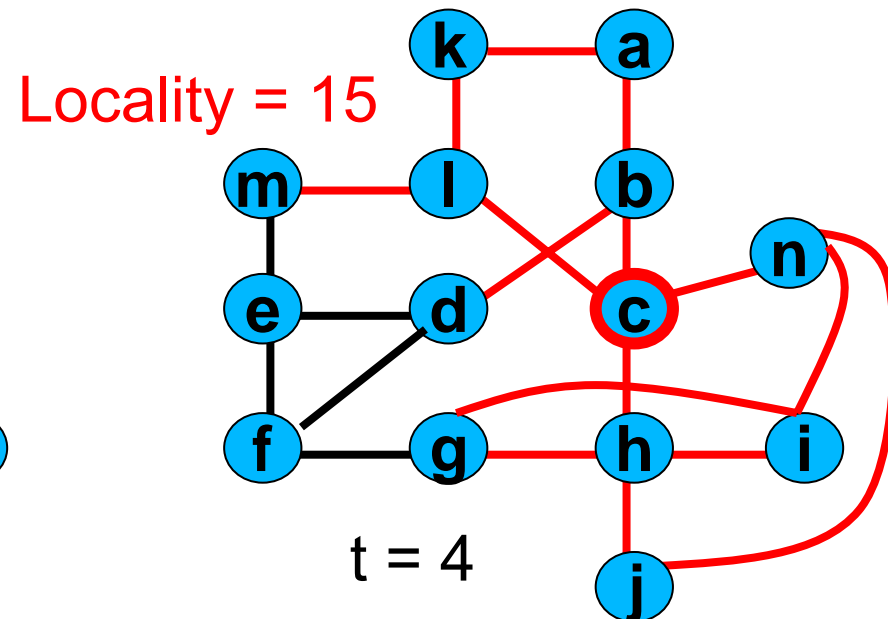
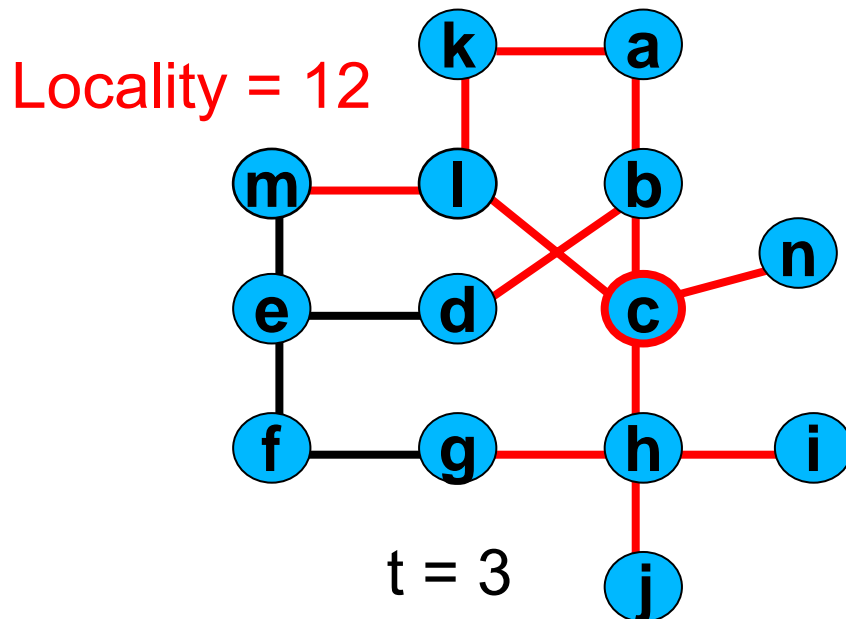
Centrality uses a sliding window mechanism

$$\tilde{\psi}_{k,t}(v) = \frac{(\psi_{k,t}(v) - \hat{\mu}_{k,t,\tau}(v))}{\max(\hat{\sigma}_{k,t,\tau}(v), 1)}$$

$$\hat{\mu}_{k,t,\tau}(v) = \frac{1}{\tau} * \sum_{t'=t-\tau}^{t-1} \psi_{k,t'}(v)$$

$$\hat{\sigma}_{k,t,\tau}(v) = \frac{1}{\tau - 1} \sum_{t'=t-\tau}^{t-1} (\psi_{k,t'}(v) - \hat{\mu}_{k,t,\tau}(v))^2$$

$$\tilde{M}_{k,t} = \max_{v \in \text{vertices}} \tilde{\psi}_{k,t}(v)$$



# Intersection graphs

## Source IP addresses analysis

### Goal

- Detect if probes / subnetworks detect a larger panel of source IP addresses

### Honeynet

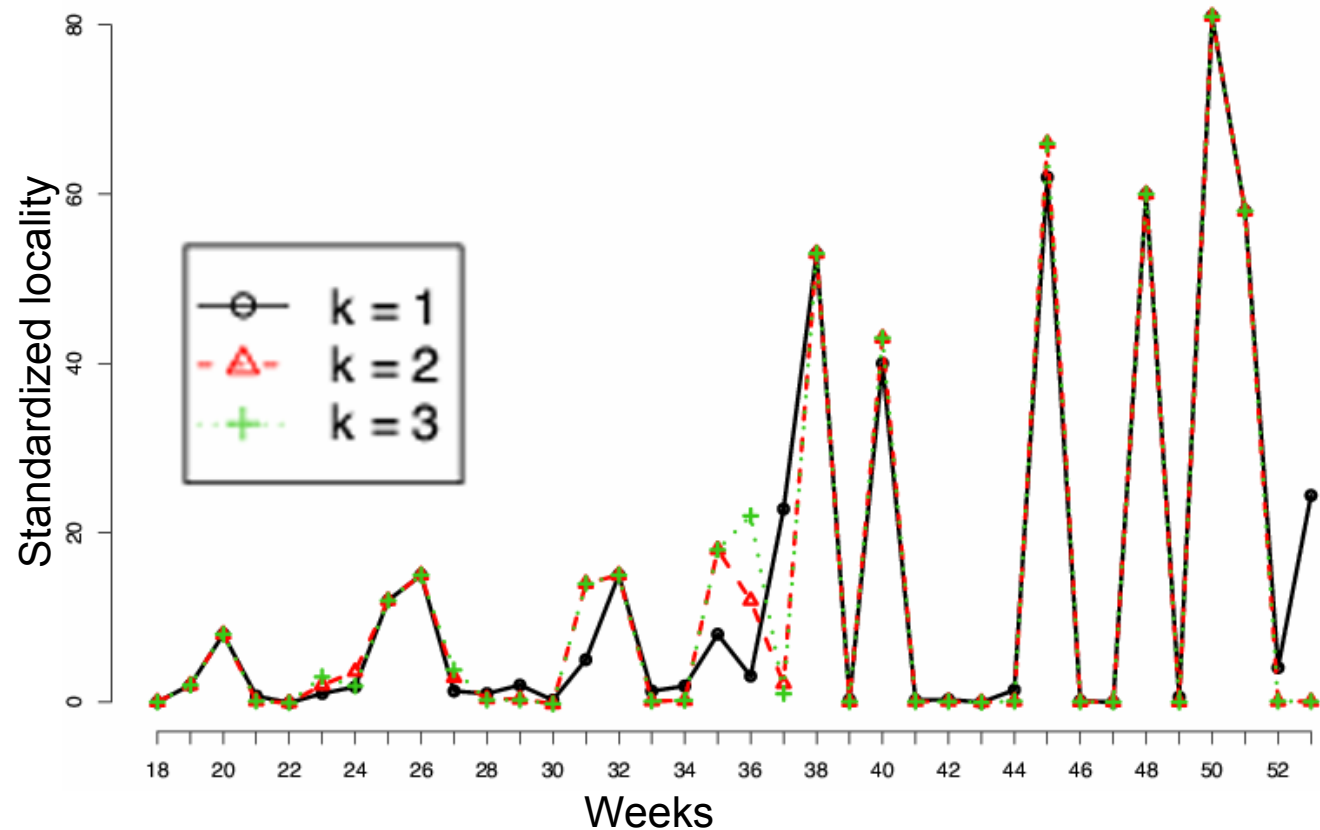
- From may to december 2004, per weeks (11 millions of packets – 1,8 GB)
- Per platform (3 destination IP addresses)

Modeling: 2 platforms (vertices) are linked if the common addresses  $<$  threshold

# Intersection graphs IP source addresses

## Honeynet

- Standardized locality (threshold = 0,25%,  $\tau = 5$ )



**Peaks = topology  
changes**

**6 central platforms =  
necessary platforms**

# Intersection graphs

## Source IP addresses

### Telescope

- From August 26 to 31, per hour (460 millions of packets – 24,1 GB)
- By /16 subnetwork

Modeling : 2 subnetworks (vertices) are linked if common source IP addresses  $< 5\%$

→ Locality = 0 all time except at the beginning

$5\% \gg 0,25\%$  → much higher redundancy than the honeypot

# Intersection graphs

## Source ports analysis

### Objective

- Detect if probes / networks see a larger panel of open source ports (SYN + ACK)

### Honeynet

- By platform (3 destination IP addresses)

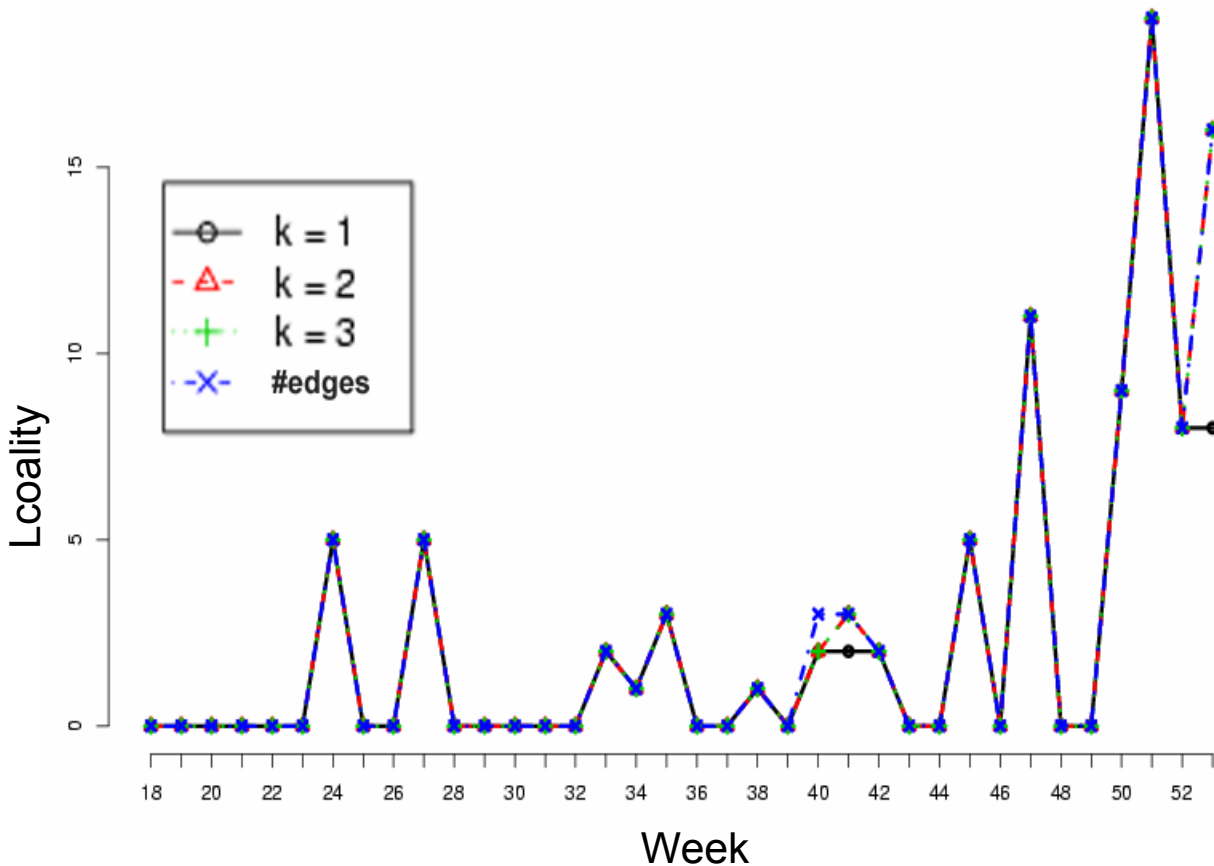
Modeling : 2 platforms (vertices) linked if common open source ports  $<$  threshold

# Intersection graphs

## Source port analysis

### Honeynet

- Maximal locality (threshold = 10 %)



few vertices  $\rightarrow$  the platforms detect the same ports

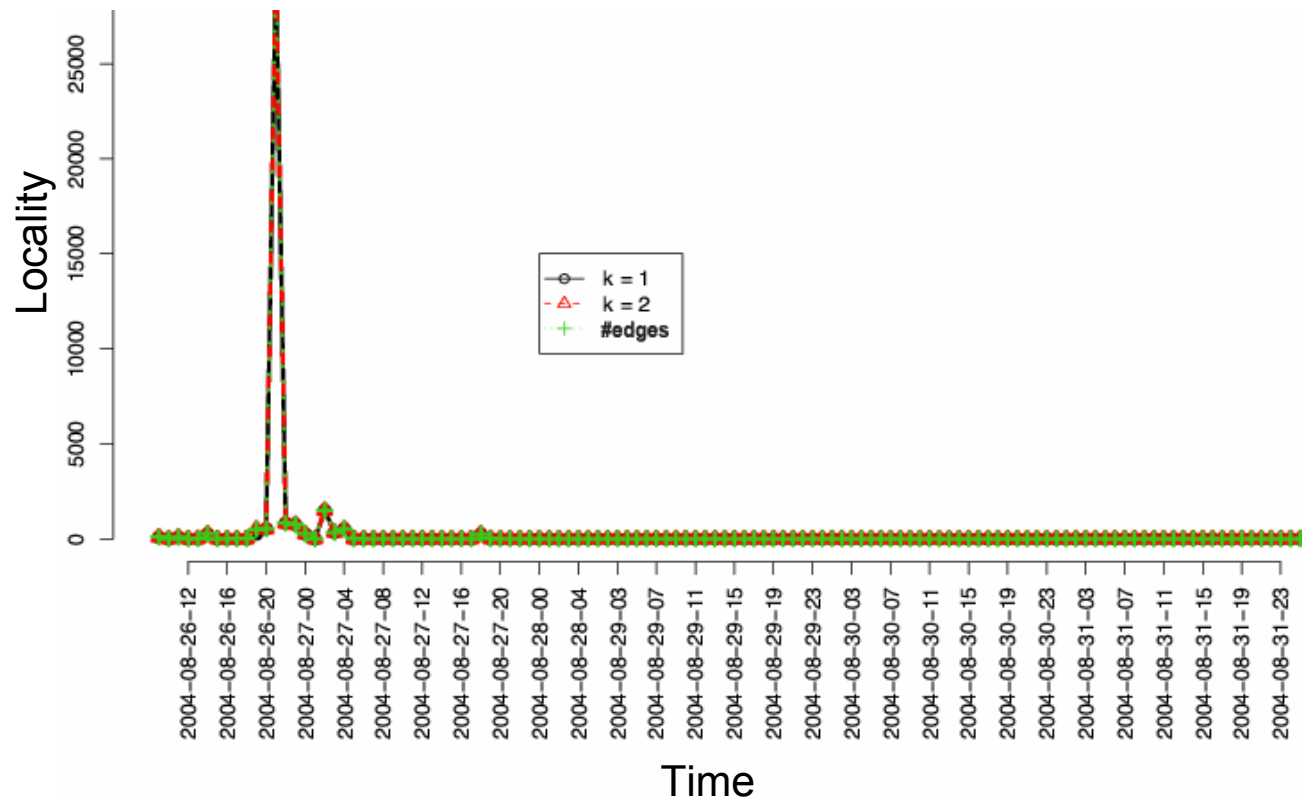
Peak = when the detected ports are different

(backscatter packets only)

# Intersection graphs

## Source ports analysis : telescope

1. By /16 subnetwork
2. Modeling : 2 subnetworks (vertices) linked if common source ports  $< 5\%$



No difference between subnetworks



Peak with 3 central nodes

# Intersection graphs

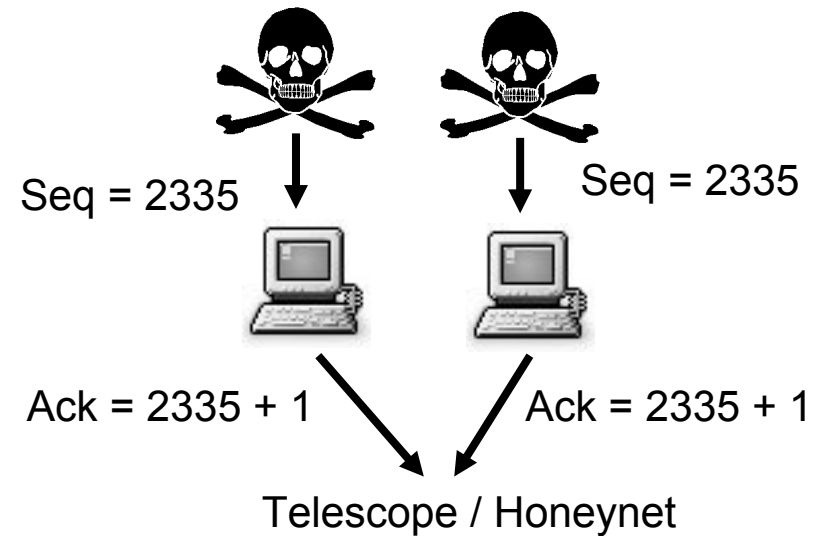
## Attack tool fingerprinting

### Objective

- Monitor the acknowledgment numbers in order to detect the use of the same attack tool

### Honeynet

- From may to december 2004, per week
- By platform (3 destination IP addresses), only when the port is open



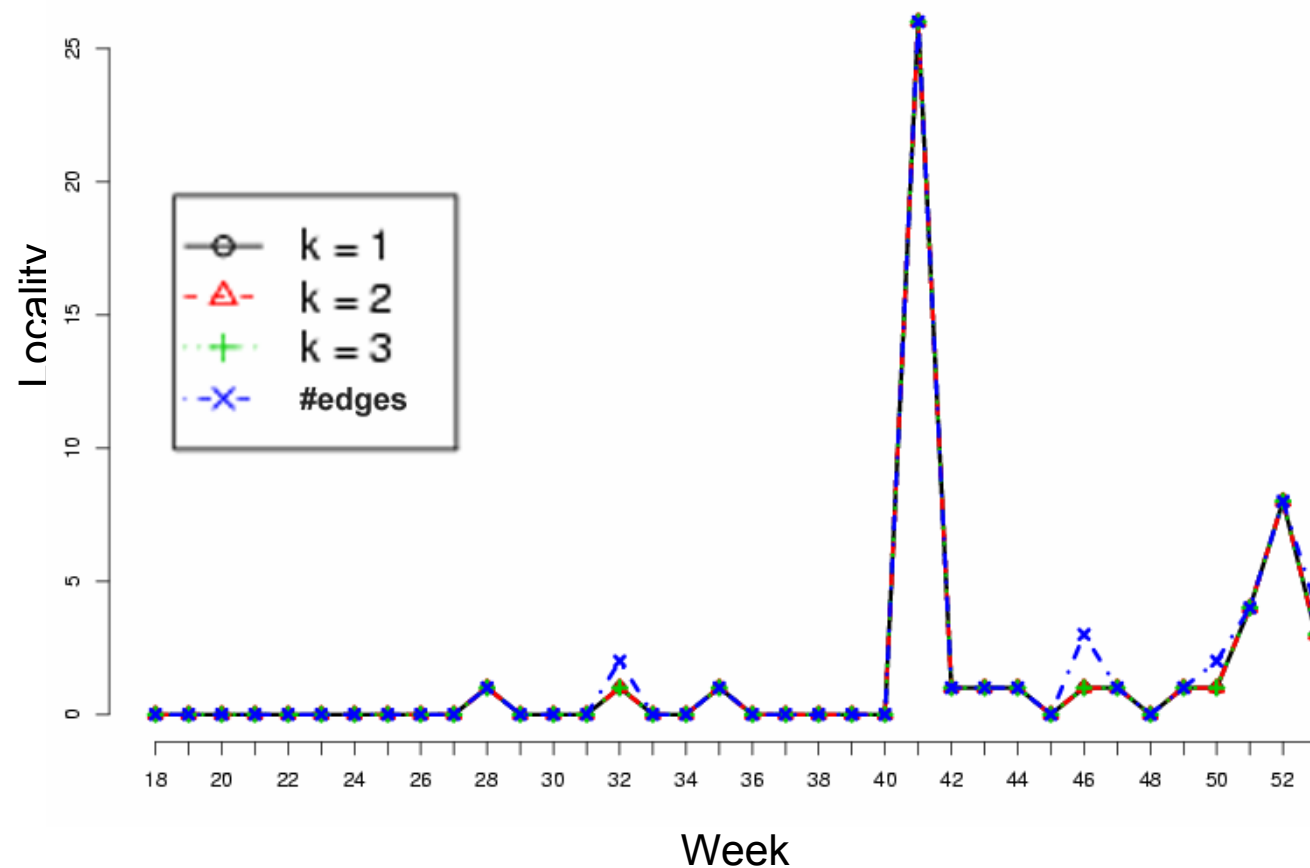
Modeling: 2 platforms (vertices) linked if common acknowledgment numbers  $> 90\%$

# Intersection graphs

## Attack tool fingerprinting

### Honeynet

- Locality curve (same curve for standardized curve)



Next to 0 main time

↓  
Variety and sophisticated tools

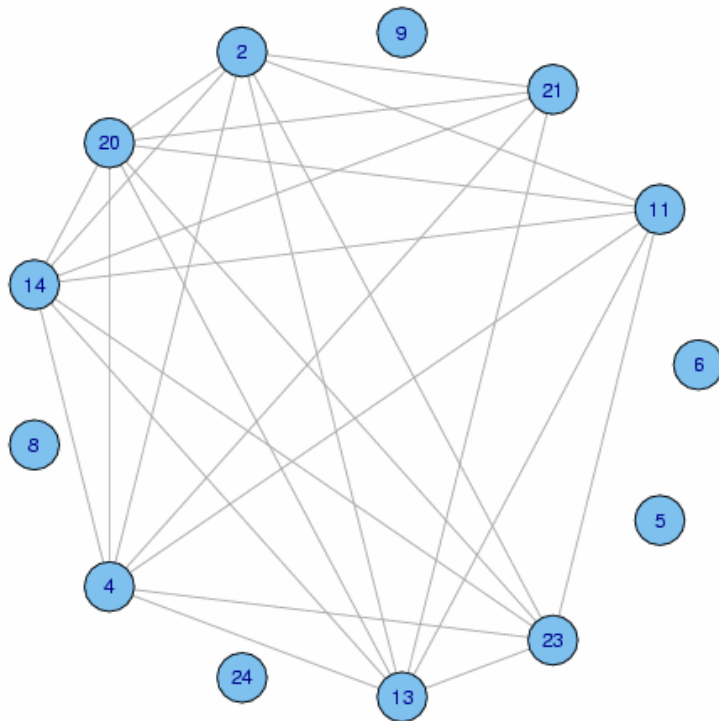
Peaks with confused curves

↓  
Very central platform

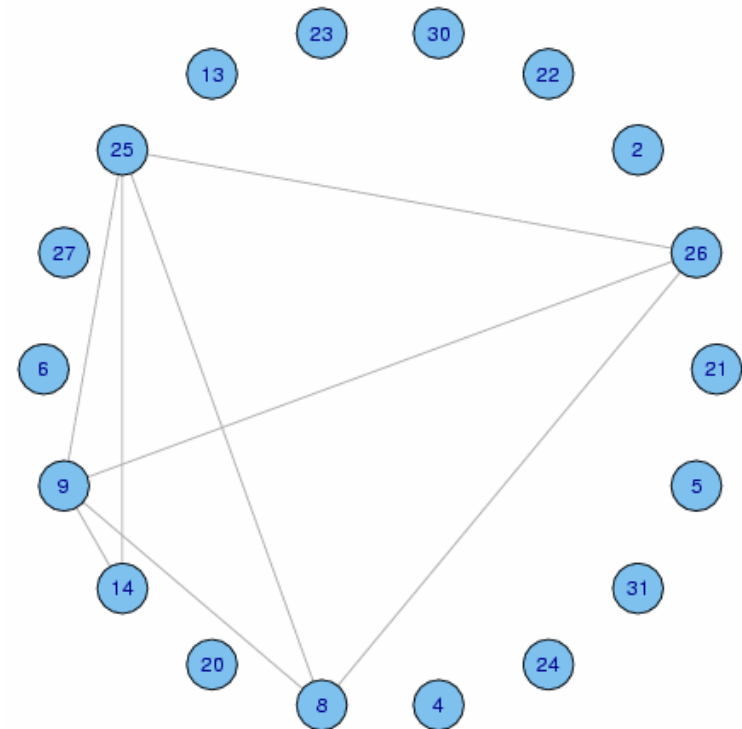
# Intersection graphs

## Attack tool fingerprinting

### Honeynet



Week 41: same tool



Week 52: tool with a bad random generator number

# Configuration errors

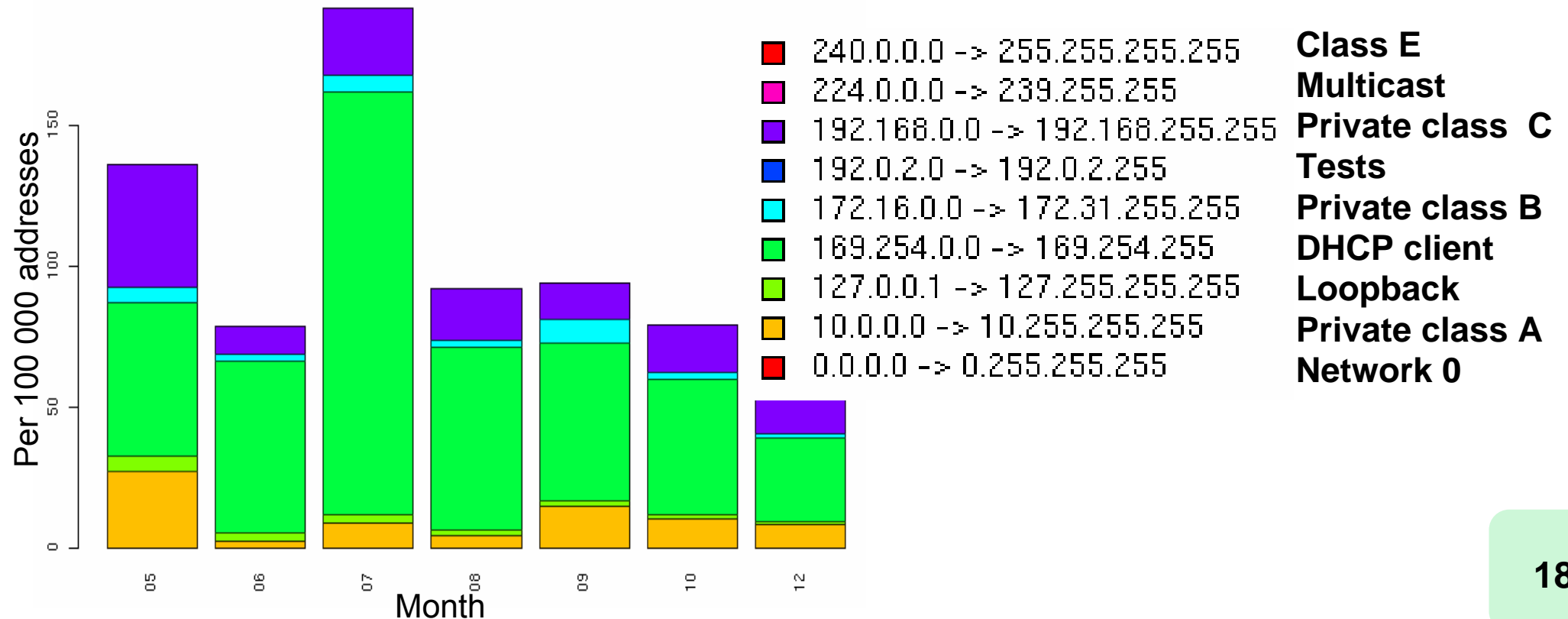
## Goals

- Highlight the configuration errors of the Internet Service Provider and their customers
- Comparison of the honeynet results (1,8 GB) with data from the telescope (120 GB)

# Configuration errors

## Source IP addresses

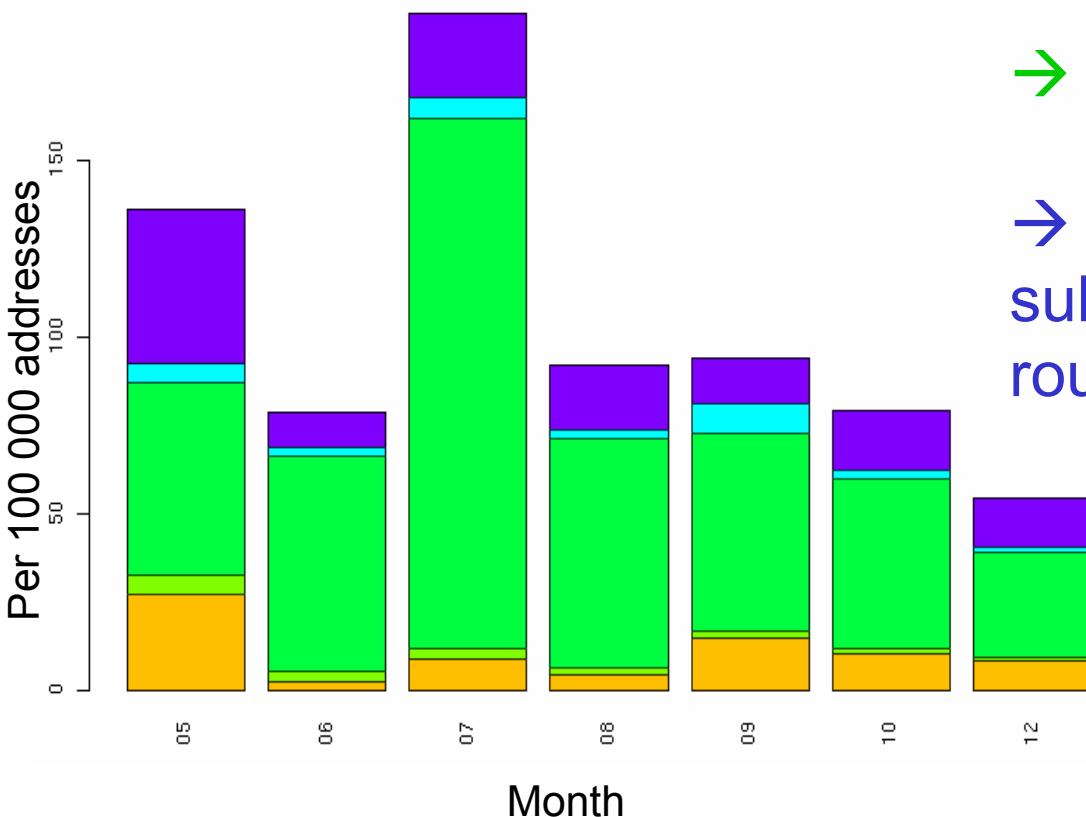
- Abnormal IP addresses as source IP addresses (victim packets)
- Honeynet : per month and per 100 000 addresses



# Configuration errors

## Source IP addresses

- Honeynet : per month and per 100 000 addresses



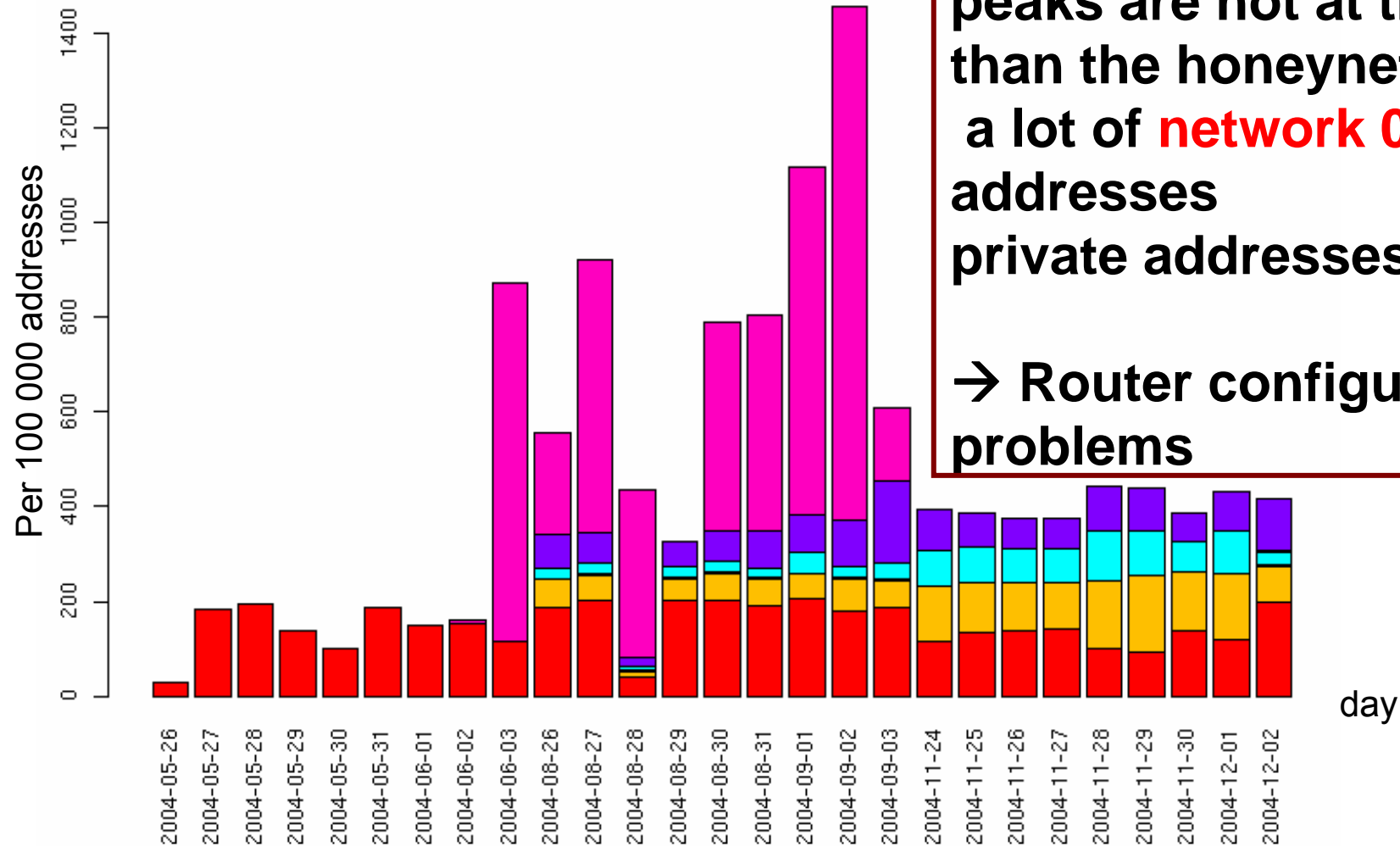
→ DHCP + router configuration error

→ Private addresses: private subnetwork connected to Internet + router problem

# Configuration errors

## Source IP addresses

- Telescope : per day and per 100 000 addresses

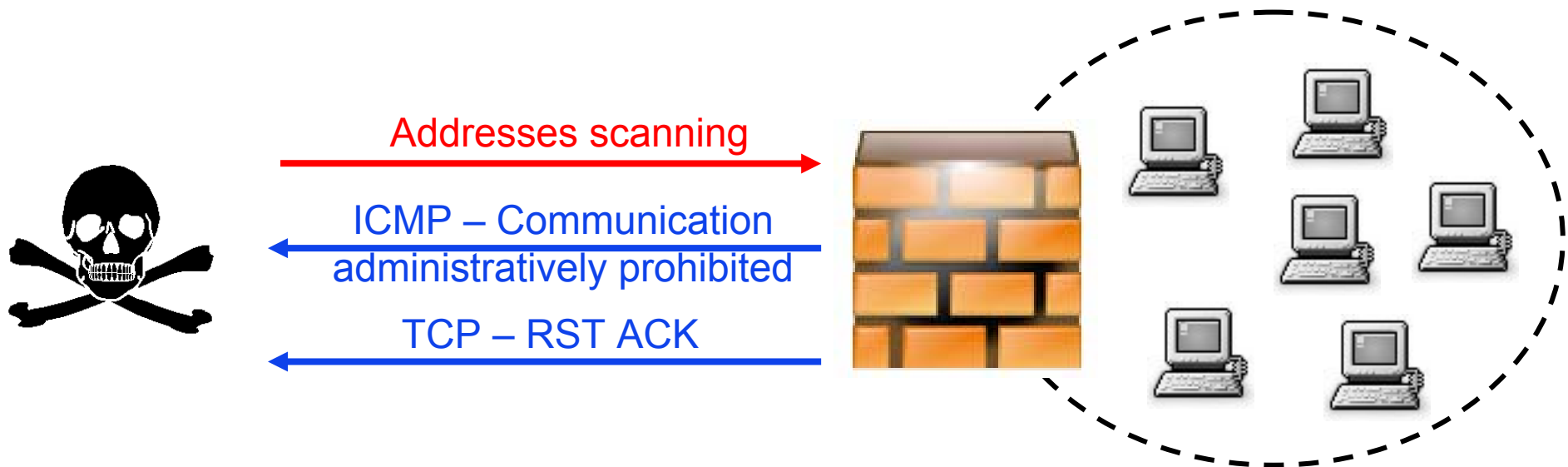


peaks are not at the same time than the honeynet  
a lot of **network 0** and **multicast** addresses  
private addresses  
→ Router configuration problems

# Security policy changes

**ICMP ‘Destination Unreachable implies that the host is can not be connected to:**

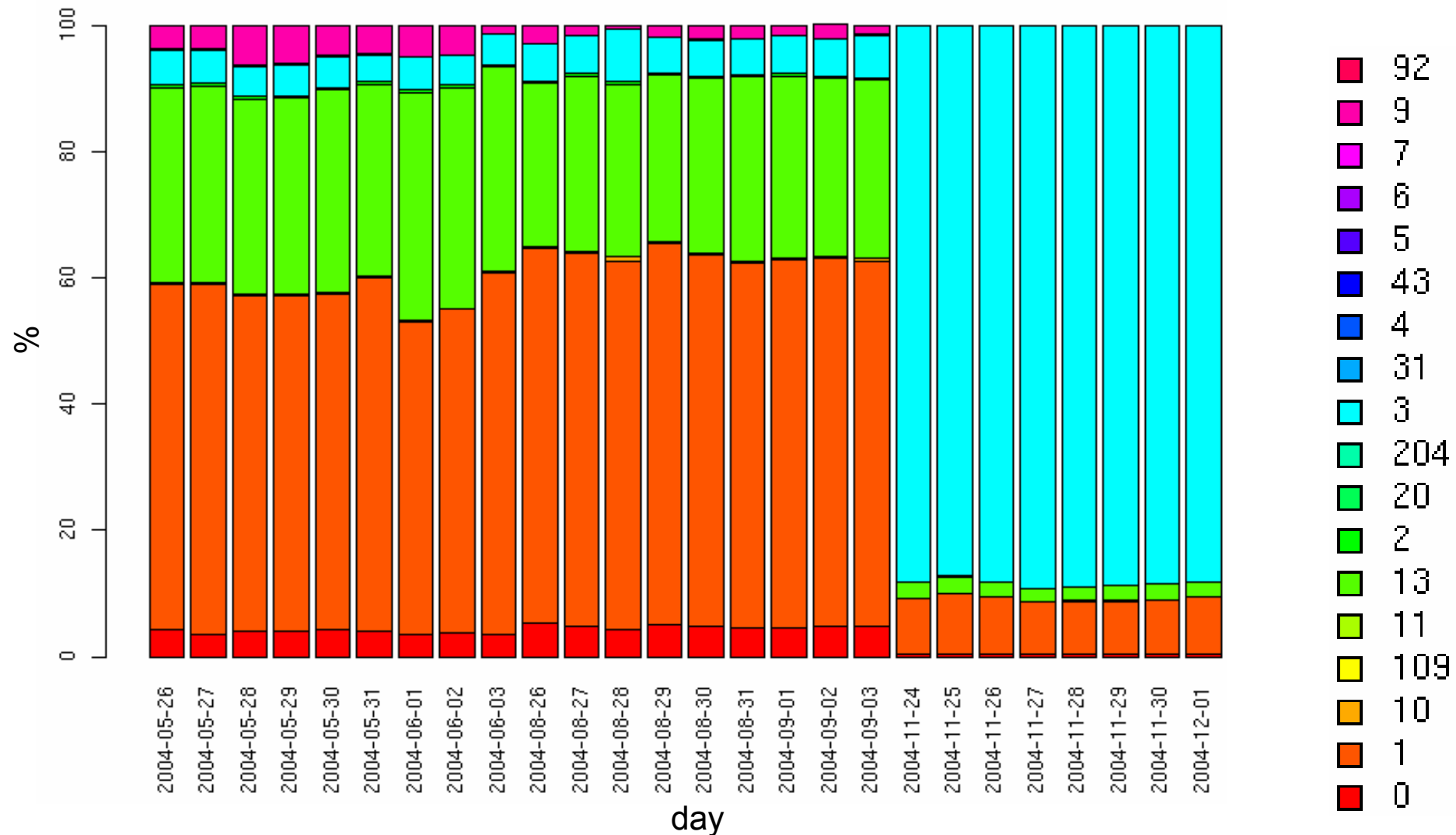
- Several codes show the reason → very helpful for the administrator but can give some clues to the attackers about the use of a firewall and its configuration



# Security policy changes

## ICMP 'Destination Unreachable'

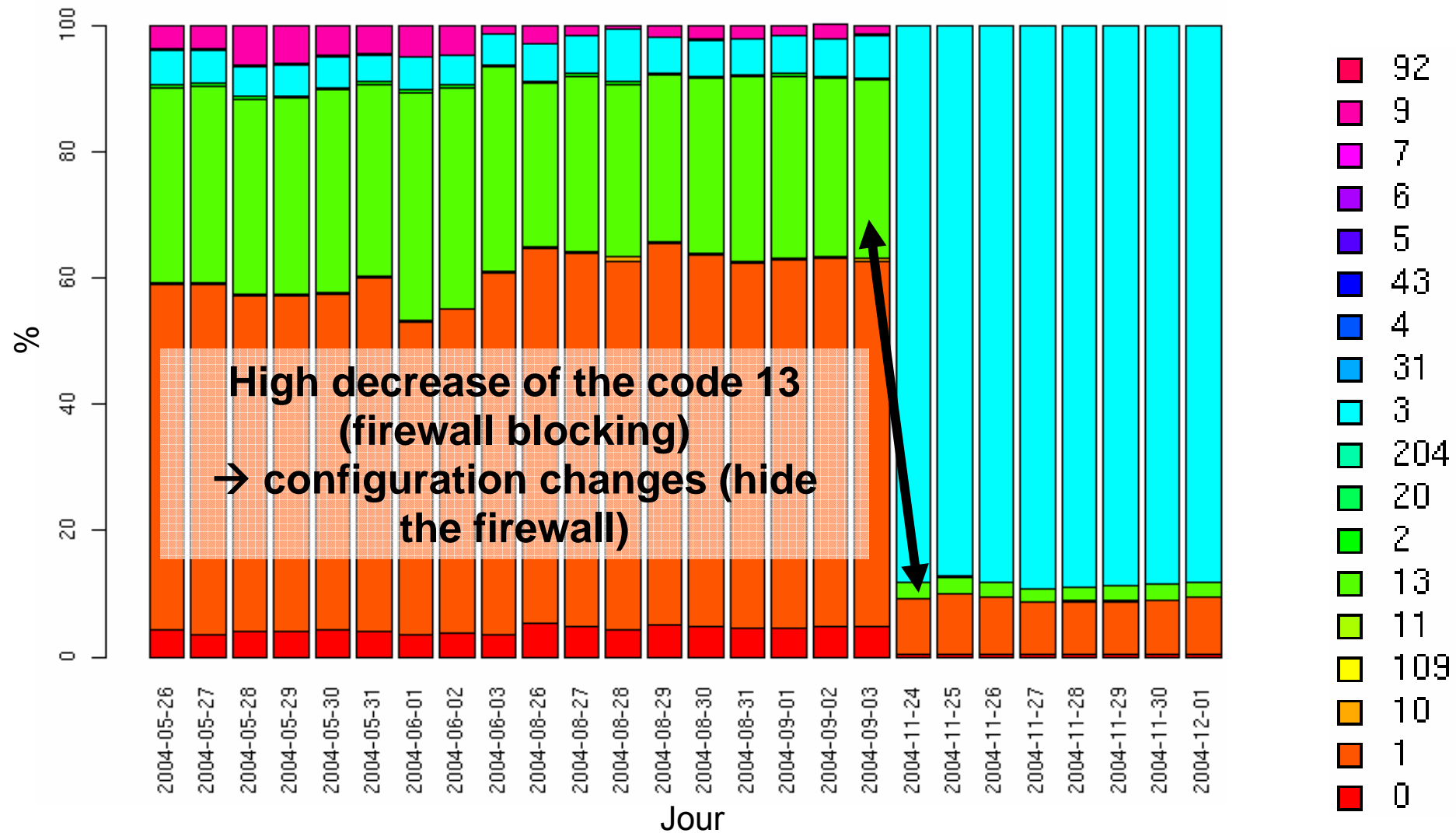
- Telescope : the percentages of each codes



# Security policy changes

## ICMP 'Destination Unreachable'

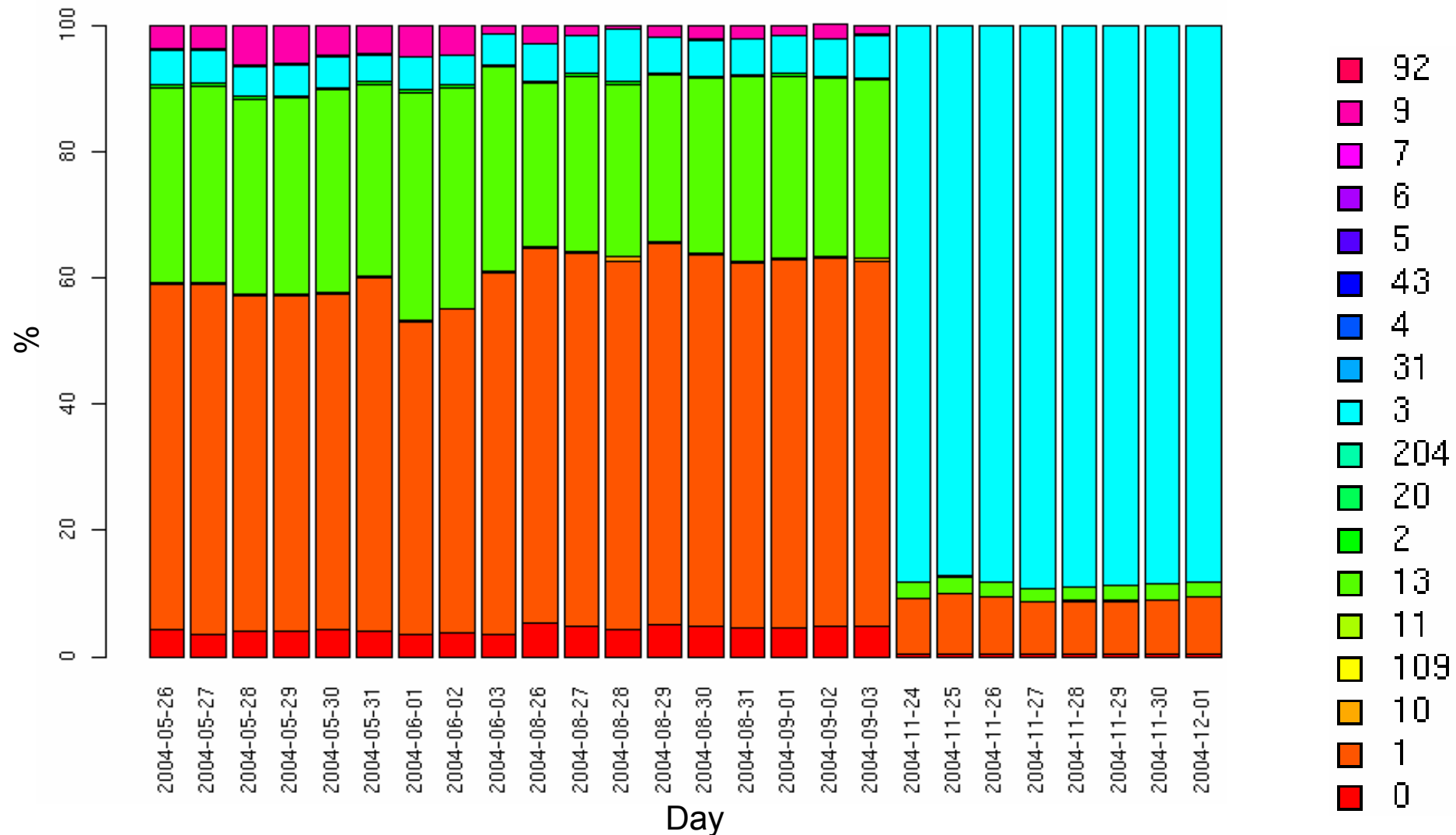
- Telescope : the percentages of each codes



# Security policy changes

## ICMP 'Destination Unreachable'

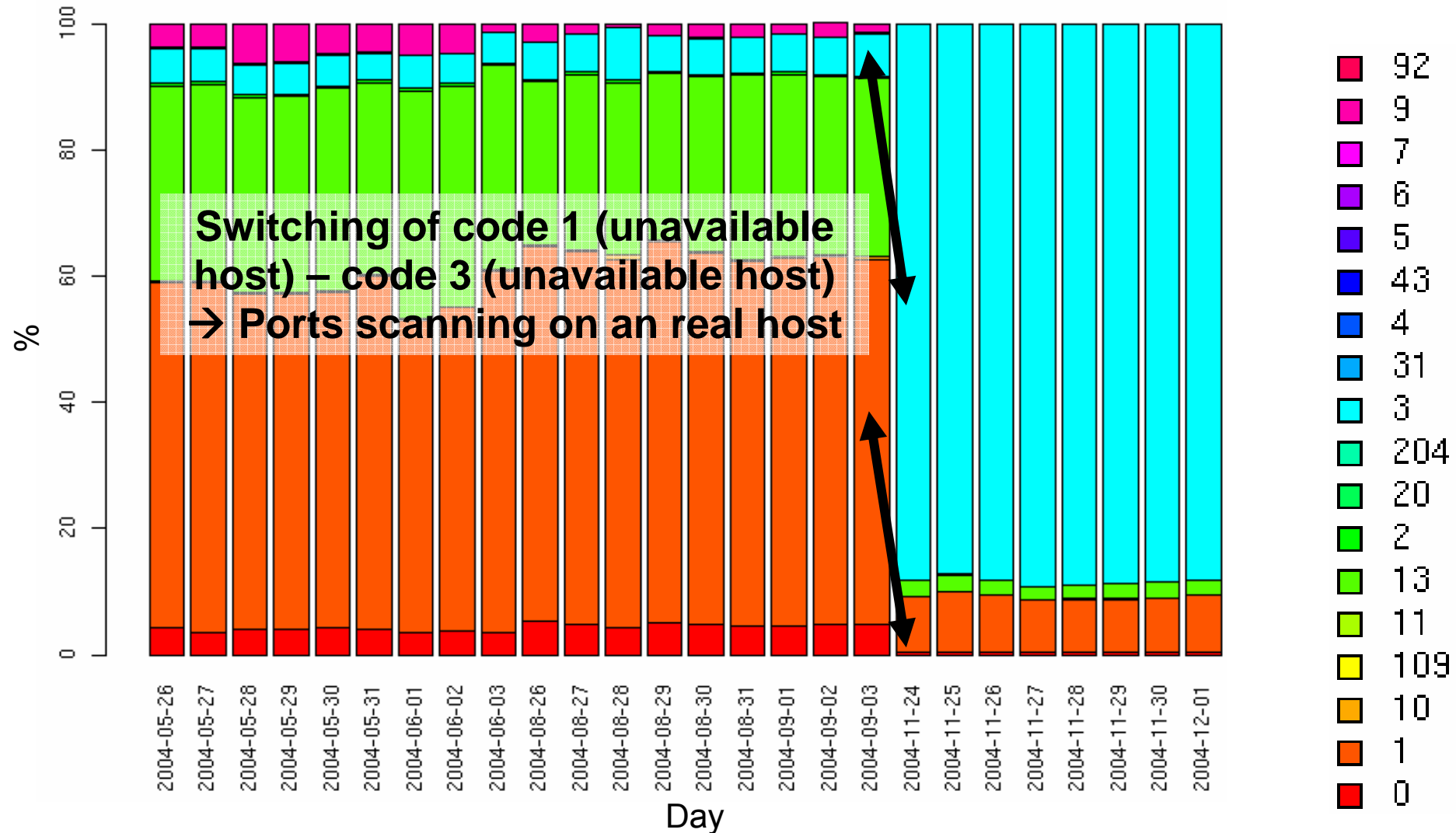
- Telescope : the percentages of each codes



# Security policy changes

## ICMP 'Destination Unreachable'

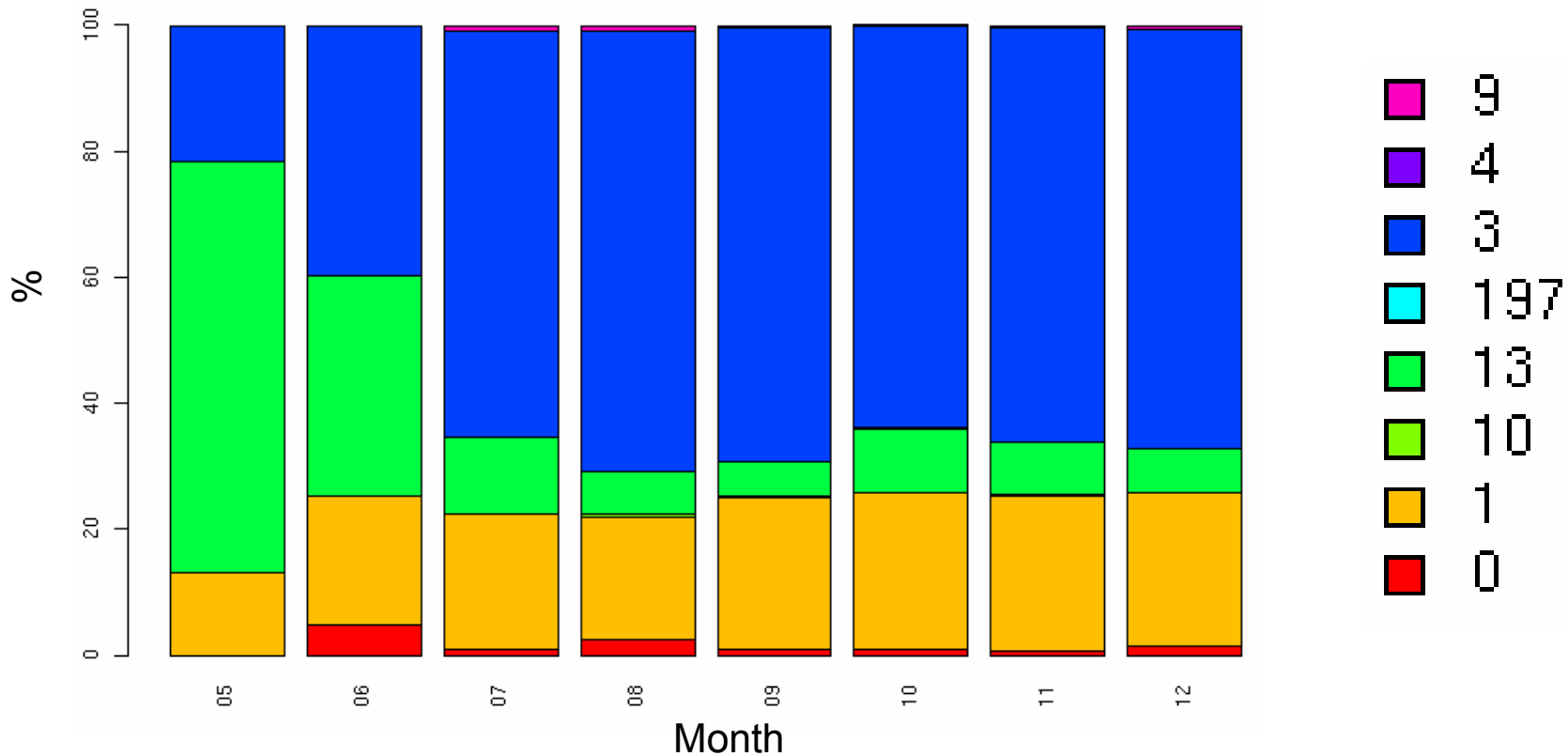
- Telescope : the percentages of each codes



# Security policy changes

## ICMP 'Destination Unreachable'

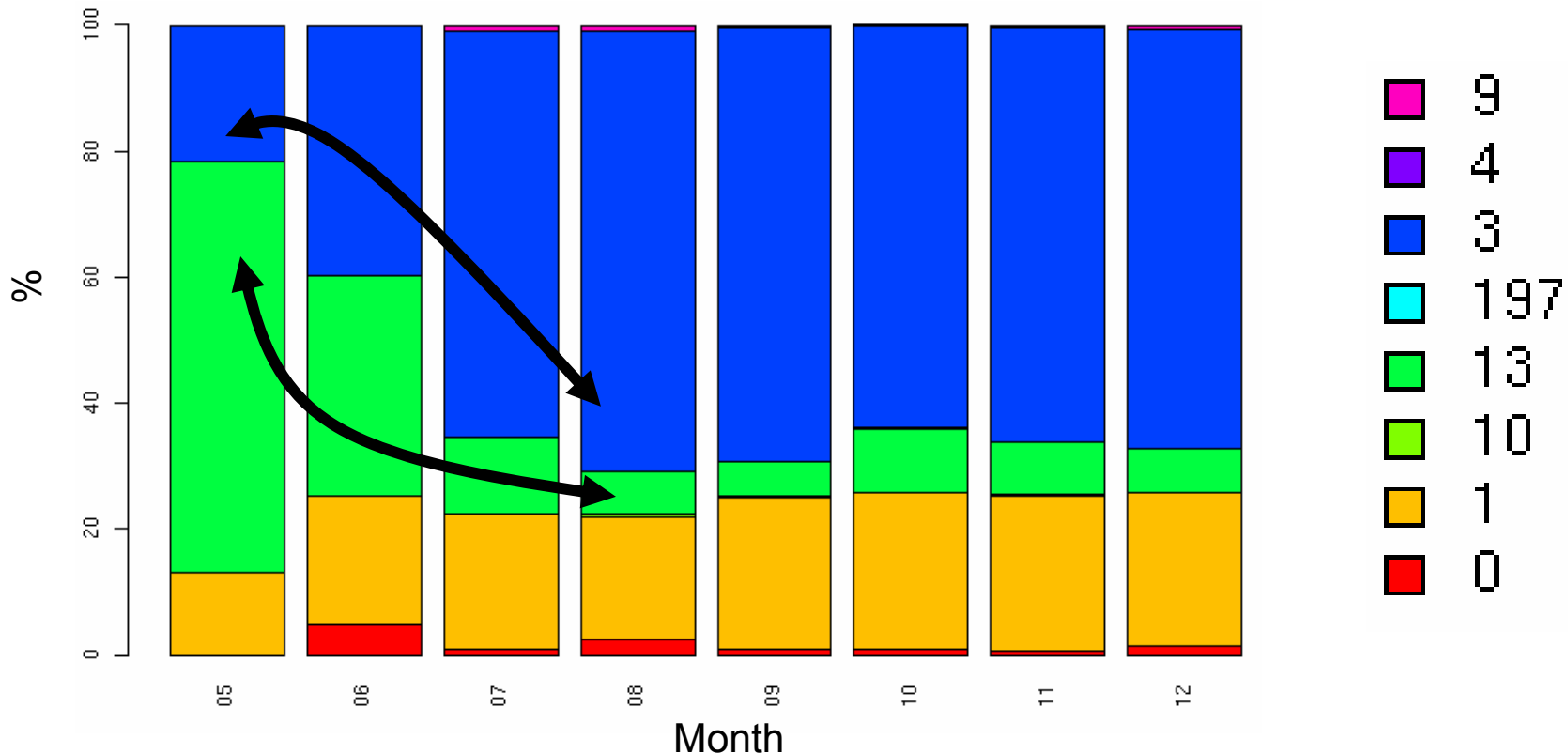
- Honeynet : percentages of each codes



# Security policy changes

## ICMP 'Destination Unreachable'

- Honeynet : the percentages of each codes



Same results but smoother than the telescope (probes distribution)

# Conclusions

- Intersection graphs as a method for large scale data analysis
- Tracking temporal patterns in the monitoring platform
- Honeypots and telescopes are complementary and analysis was done on a common timeframe
- Observing configuration trends at the Internet level