



# eCSIRT.net The European CSIRT Network

**Final Status Update  
16 January 2004**

Slide 1  
© 2000-2004 by PRESECURE® Consulting GmbH



## Topics for the Presentation

- **eCSIRT.net in perspective**
- **Some results for IDS related activities**
  - eCSIRT.net tools
  - But operational data of PRESECURE
- **Workshop on Early Warning**

Slide 2  
© 2000-2004 by PRESECURE® Consulting GmbH



# eCSIRT.net in Perspective

- **Project formally ended on December 31, 2003**
  - Final Review within January 2004
  - Final Results made available on the web



## Problem Statement

- **While researching the WP4 Type 3 statistics, the question came up, how this data relates to other data from real networks**
- **The approach taken was to analyse other available data (ARGUS) and compare the outcome with results from WP4 Type 3**
- **ARGUS network monitoring data**
  - operational network
  - 10 IP addresses
  - 7 March – 7 December 2003



# Overall Observations

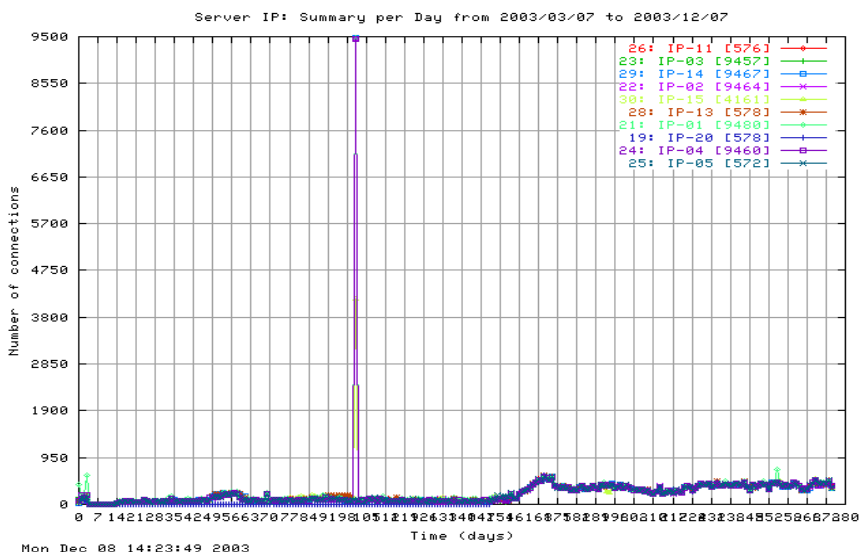
- **Within the time frame of March 7 to December 7 in total 704.625 malicious connections from 46.978 IP addresses were identified:**
  - 297.513 (42,22%) from 37.610 (80,06 %) IP addresses that hadn't send any ICMP packets  
→ 7,91 connections/IP
  - 407.112 (57,77%) from 9.368 (19,93 %) IP addresses that had send ICMP packets  
→ 43,46 connections/IP (including ICMP)
- **IP addresses that send ICMP packets have more activities then others!**
  - **Caveat:** As one big port scan contributes to approx 51.100 connections, the real numbers are somewhat lower (~ 38 connections/IP without ICMP)

Slide 5

© 2000-2004 by PRESECURE® Consulting GmbH



# Overall traffic for all servers

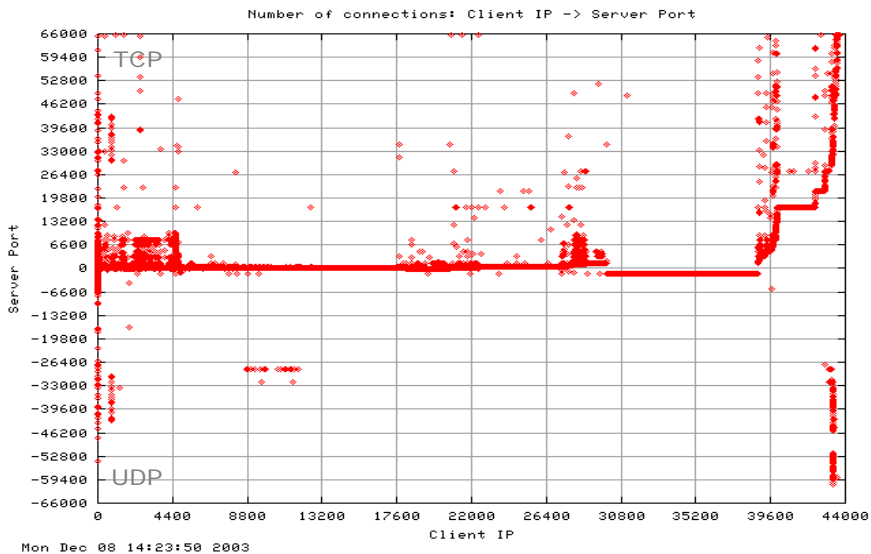


Slide 6 data/data-01-all.png

© 2000-2004 by PRESECURE® Consulting GmbH



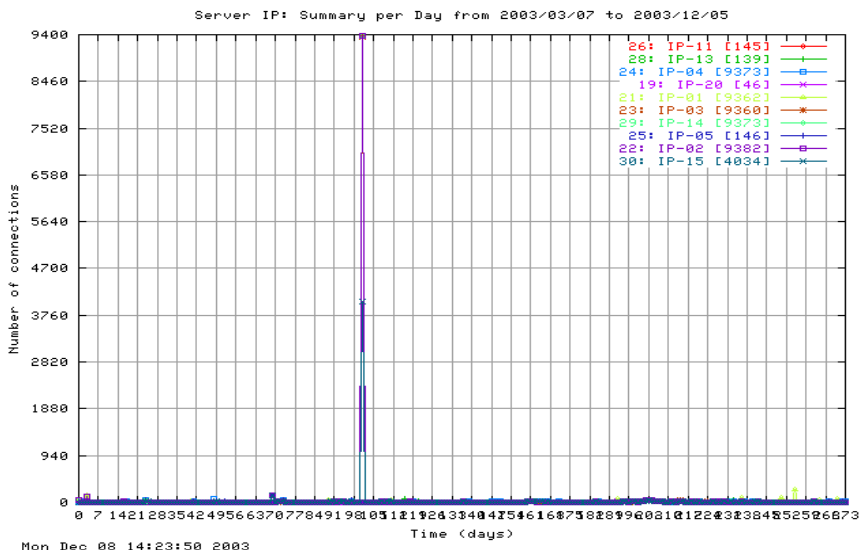
# Overall traffic connection matrix



Slide 7 data/data-connections-si-dp.png  
© 2000-2004 by PRESECURE® Consulting GmbH



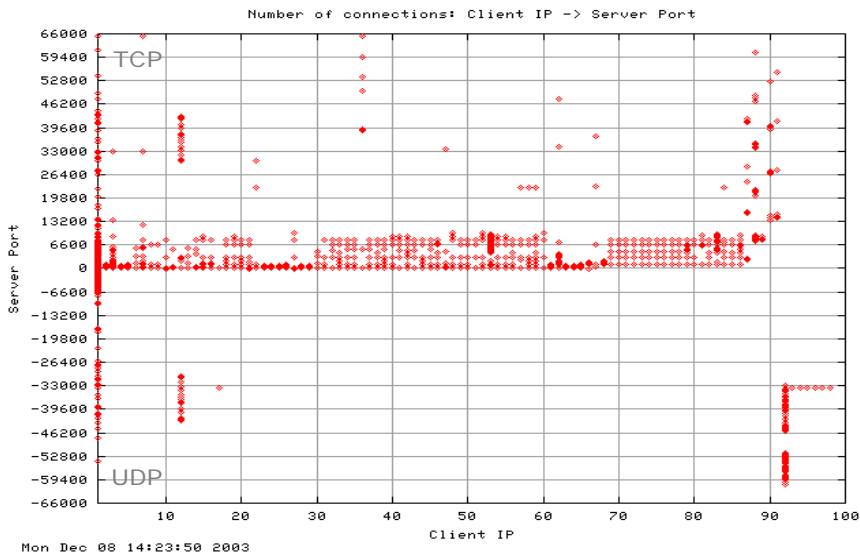
# Portscan related connections



Slide 8 data/portscan-all-01-all.png  
© 2000-2004 by PRESECURE® Consulting GmbH



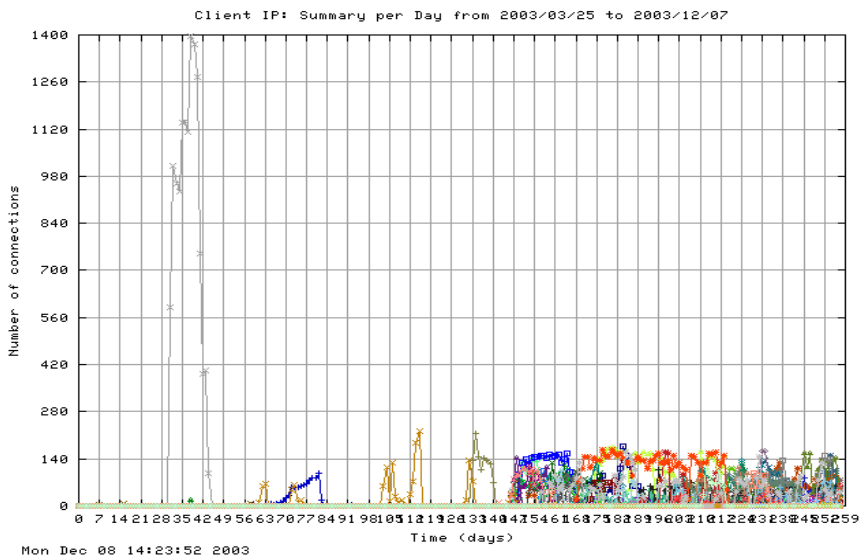
# Portscan connection matrix



Slide 9 data/portscan-all-connections-si-dp.png  
© 2000-2004 by PRESECURE® Consulting GmbH



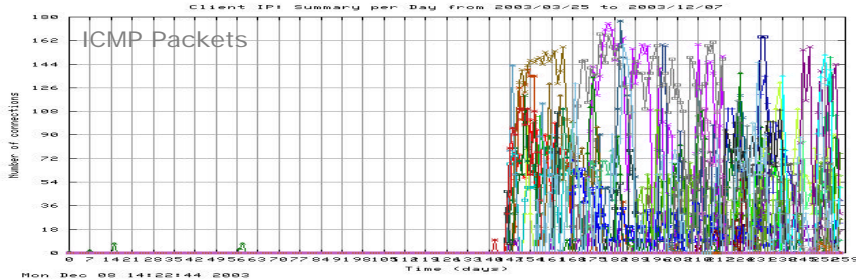
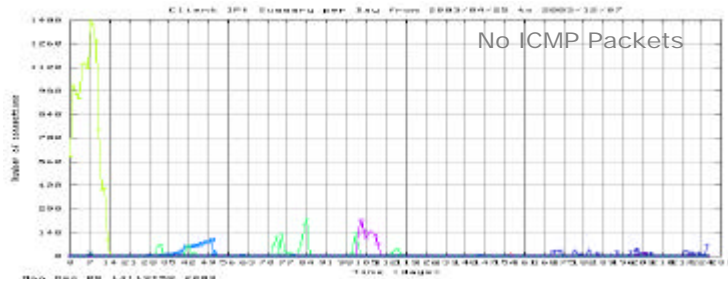
# Unusual high numbers of connections. 135/tcp, 137/udp and 445/tcp



Slide 10 data/highportnos-si-01-all.png  
© 2000-2004 by PRESECURE® Consulting GmbH



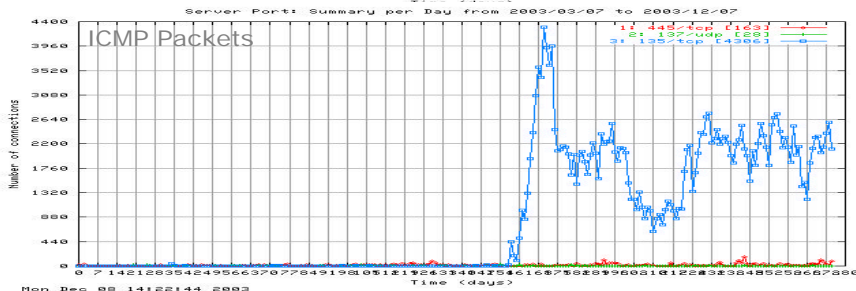
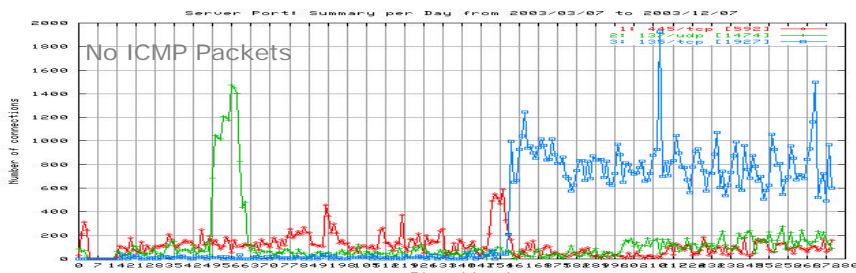
# Unusual high numbers of connections. 135/tcp, 137/udp and 445/tcp



Slide 11 data(-icmp,no-icmp)highportnos-si-01-all.png  
© 2000-2004 by PRESECURE® Consulting GmbH



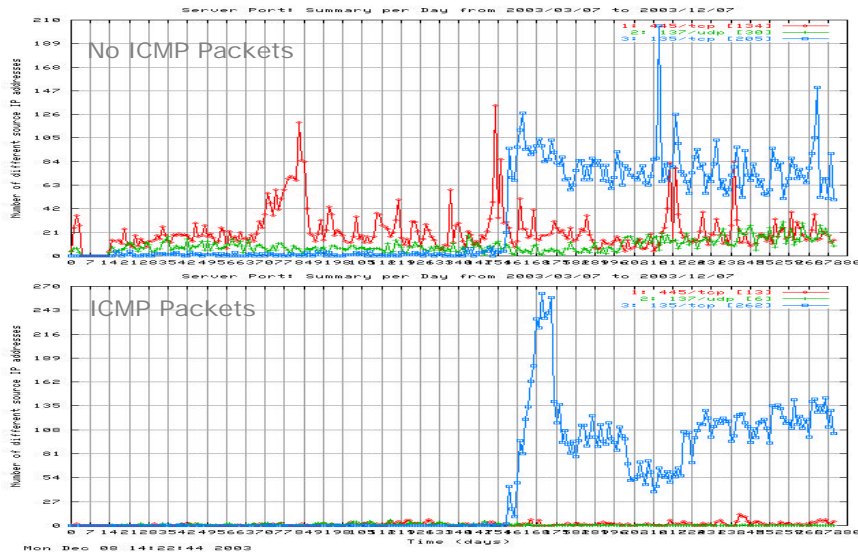
# 135/tcp, 137/udp, 445/tcp in perspective



Slide 12 data(-icmp,no-icmp)highportnos-all-01-all.png  
© 2000-2004 by PRESECURE® Consulting GmbH



# 155/tcp, 157/udp, 445/tcp in perspective

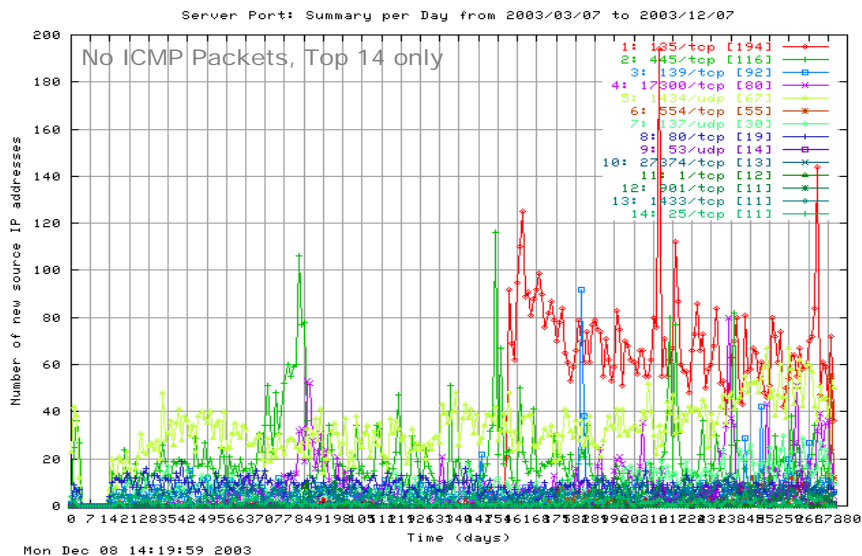


Slide 13 Data(-icmp,no-icmp)/highportnos-all-08-all.png  
© 2000-2004 by PRESECURE® Consulting GmbH



# NEW IP addresses.

## unknown traffic, without portscans



Slide 14 data-no-icmp/unknown-09-top.png  
© 2000-2004 by PRESECURE® Consulting GmbH



# How to split the Unknown?

## ■ Criteria for splitting the unknown:

- Characterization of the connections
  - Combination of source IP addresses and number of connections
- Characterization of the source IP addresses
  - Number of different source addresses for ports
  - Number of new IP addresses per day
- Characterization of the destination port
  - Trojan
  - Services (which are not known to host Trojans)
  - Not listed ports

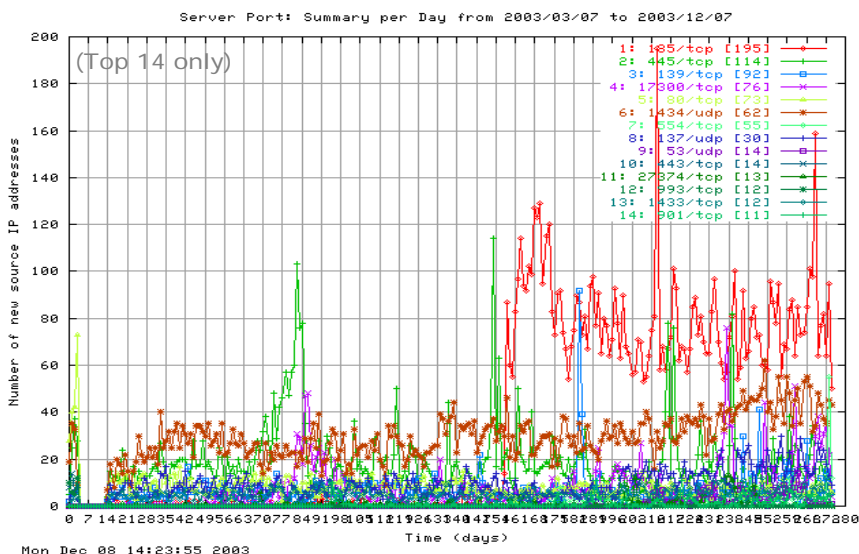
Slide 15

© 2000-2004 by PRESECURE® Consulting GmbH



# IP addresses with one day of activities

## Top 14 ports accessed

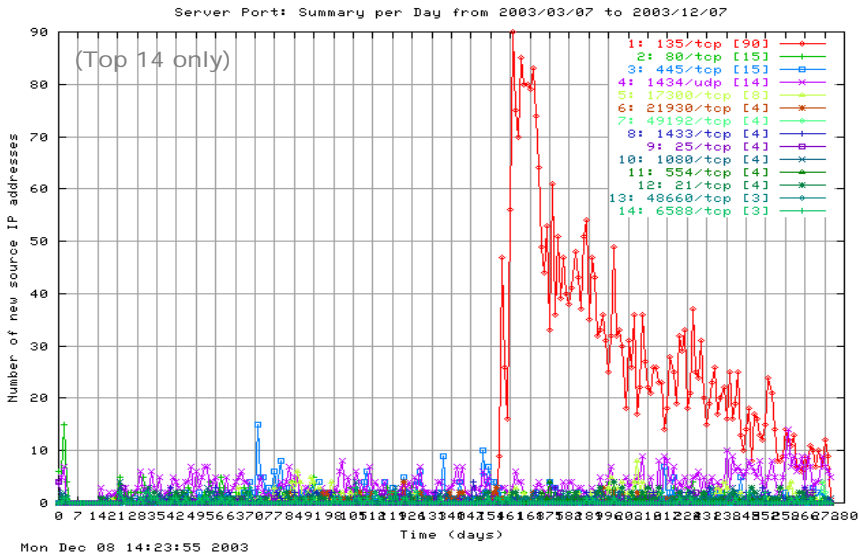


Slide 16 data/unknown-days-001-09-top.png

© 2000-2004 by PRESECURE® Consulting GmbH



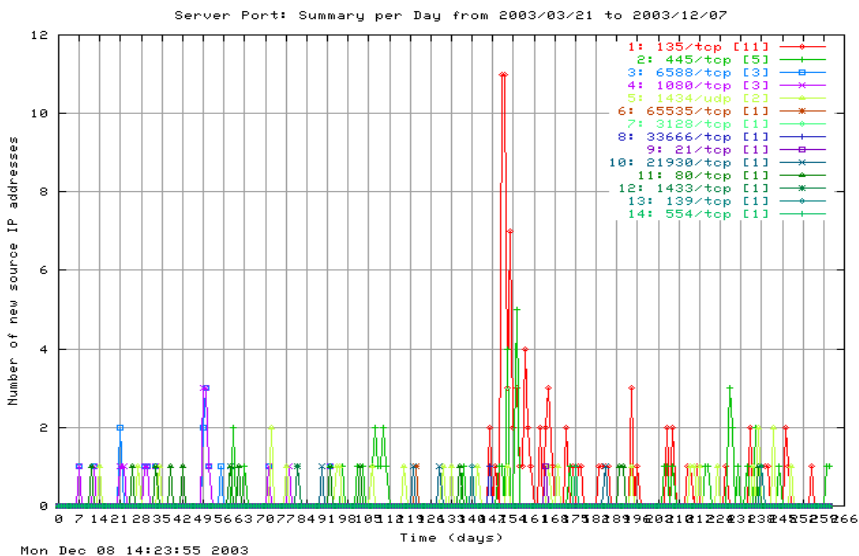
# Top 14 ports accessed



Slide 17 data/unknown-days-010-09-top.png  
© 2000-2004 by PRESECURE® Consulting GmbH



# Top 14 ports accessed



Slide 18 data/unknown-days-100-09-top.png  
© 2000-2004 by PRESECURE® Consulting GmbH



## Warning

### ■ Observations

- Various national activities in this area
- European interest in this area
- Many „local“ activities are known within the community

### ■ Conclusion

- It is time to spend resources on exchanging experiences and lessons learned to save resources
- Get the technical people and practitioners together and have some discussion

? Workshop in Hamburg  
before the TF-CSIRT Meeting!

Slide 19

© 2000-2004 by PRESECURE® Consulting GmbH



Thank  
you!

Slide 20

© 2000-2004 by PRESECURE® Consulting GmbH



# Scientific Coordinator

**Dr. Klaus-Peter Kossakowski**

**WWW: <https://www.pre-secure.de>  
<https://www.pre-secure.com>**

**Email: [kpk@pre-secure.de](mailto:kpk@pre-secure.de)**

**Mobil: (+49) 0171 / 5767010**

