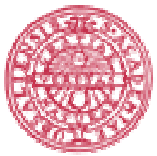
Top 10 Statistics

Jacomo Dimmit Boca Piccolini - jacomo@cais.rnp.br

CAIS/RNP: Brazilian Research Network CSIRT

FIRST Technical Colloquium, Uppsala

February, 2003



UPPSALA
UNIVERSITET

RNP

Contents

Introduction

- Statistics is a good source of information **(trust?)**
- Statistics can look to the big picture or to the little guy **(focus!)**
- Statistics availability must be in real time **(now!)**
- Statistics must be automatic generated **(easy!)**
- I like statistics ✍

Motivation

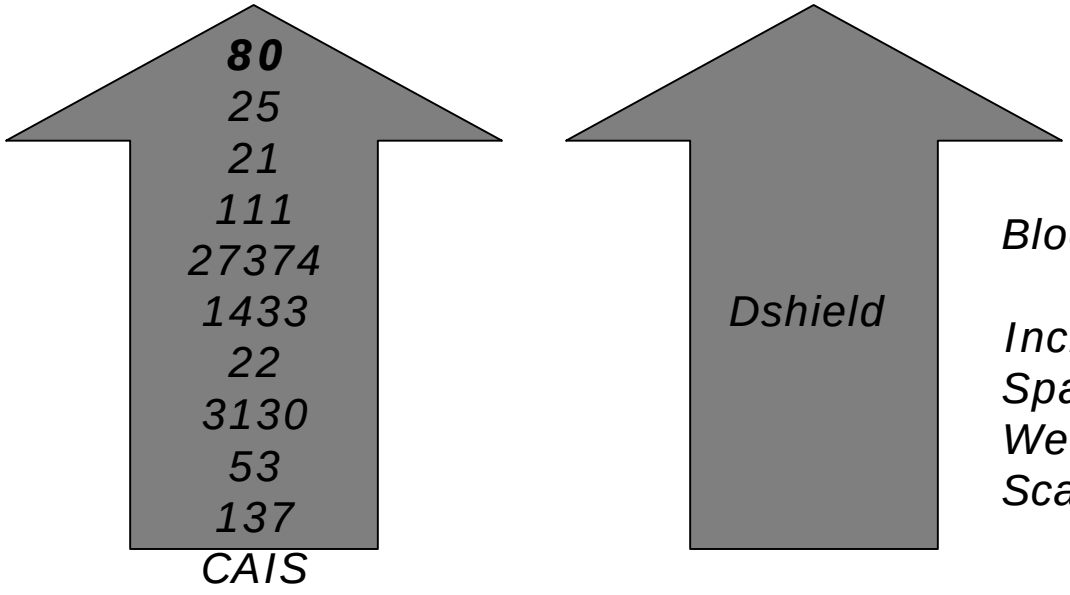
- Provide useful information to CSIRTs technical staff and support manager decisions and strategic plans.
- Improve security alerts to our constituency.
- Build a large scale source network and a reliable source network.
- Share information with FIRST members and other CSIRTs.
- We have been noticed worldwide lack of statistics on security. CAIS has been received requests of statistics about our constituency, about Brazil and Latin America hacker activities.
- Still a pilot-project...
- ... besides that, we've been working on it for the last year.
- I really like statistics ✍ ✍

Statistics

- Top 10 Ports — hourly / daily / weekly / monthly
- Top 10 IPs — hourly / daily / weekly / monthly
- Trends — hourly / daily / weekly / monthly
- New Port appearance x Cached Information — **(uhm!)**
- Slow scan/probe — weekly / monthly — **(uhm!!)**
- Acceleration / Explosion Detector — **(uhm!!!)**
- IP Constituency Check — **(bonus!)**

Statistics

- January 2002

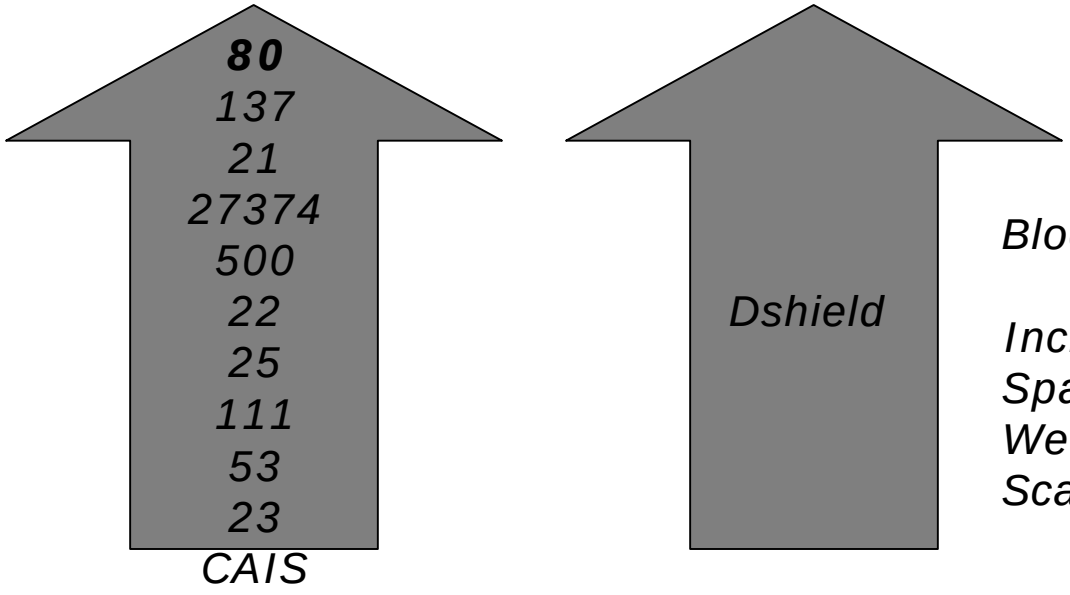


Blocked packets: ***159.760***

Incidents: 788
SpamCop: 59
WebDefacements: 20
Scans: 220

Statistics

- February 2002

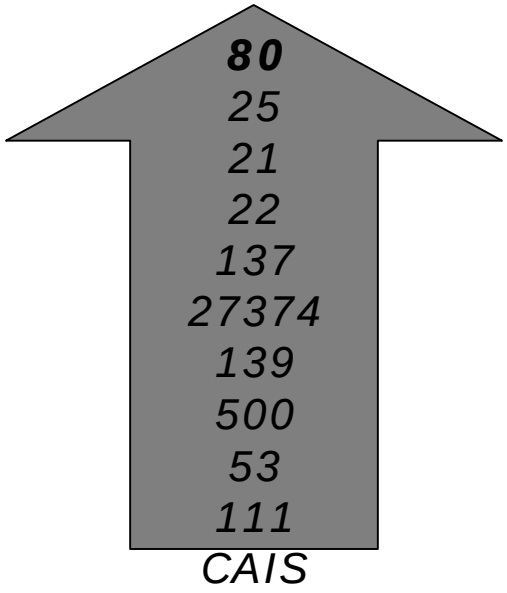


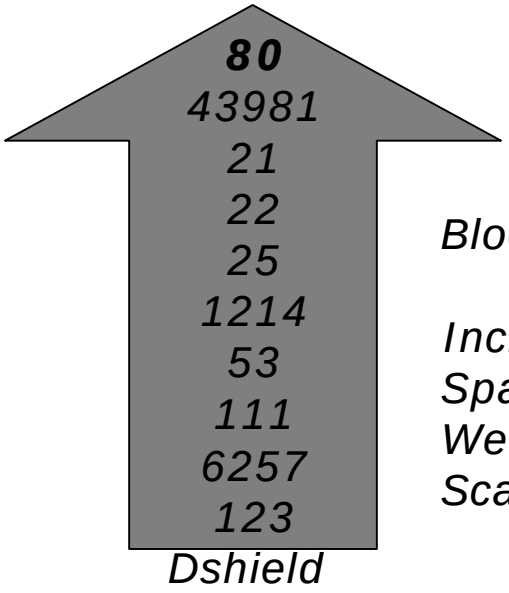
Blocked packets: ***160.109***

Incidents: 580
SpamCop: 30
WebDefacements: 2
Scans: 201

Statistics

- March 2002



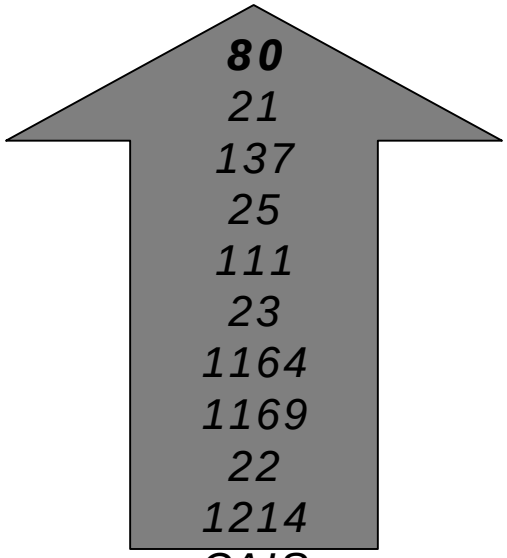


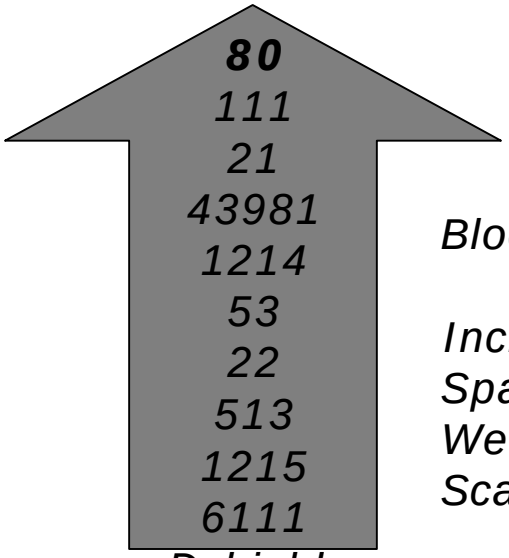
Blocked packets: ***184.647***

Incidents: 826
SpamCop: 92
WebDefacements: 37
Scans: 279

Statistics

- April 2002



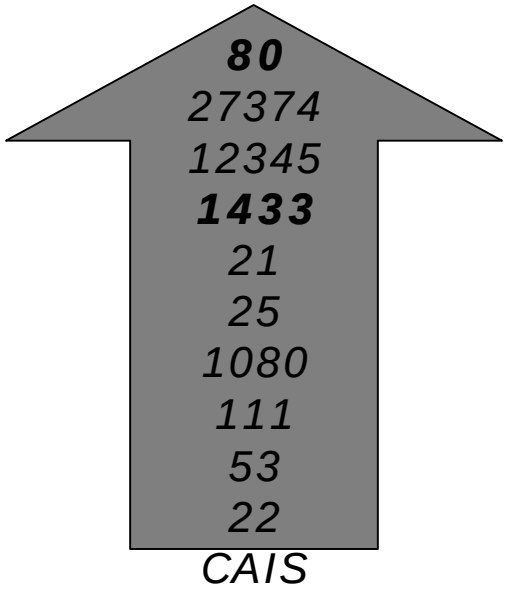


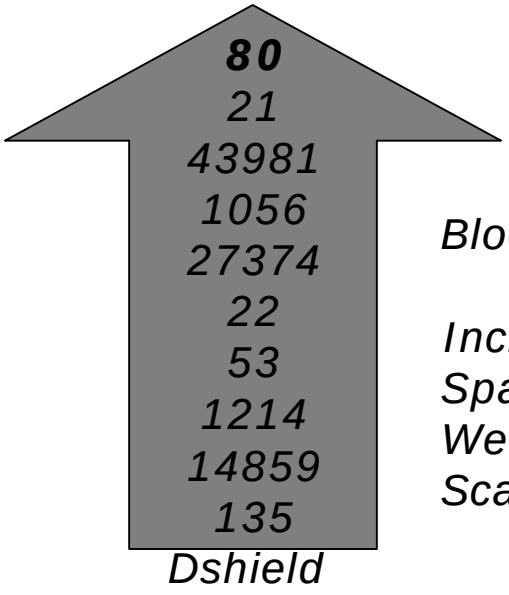
Blocked packets: ***170.037***

Incidents: 969
SpamCop: 174
WebDefacements: 54
Scans: 483

Statistics

- May 2002





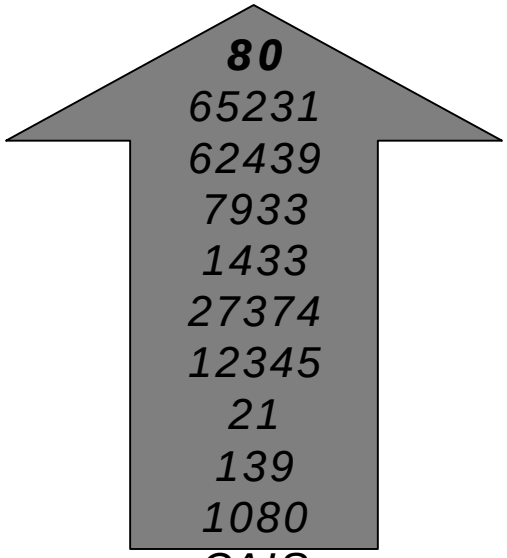
*Blocked packets:**230.671***

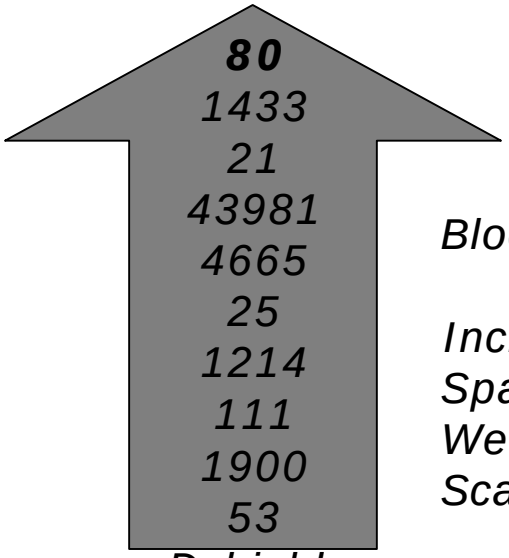
Incidents: 1222
SpamCop: 353
WebDefacements: 25
Scans: 556

- *MS02-007, MS02-020, SQL*

Statistics

- June 2002



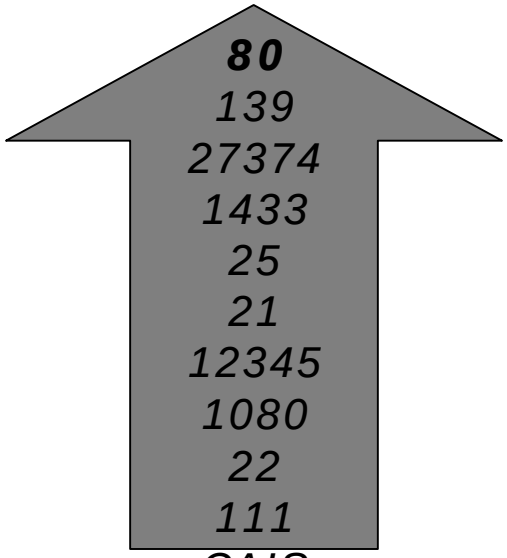


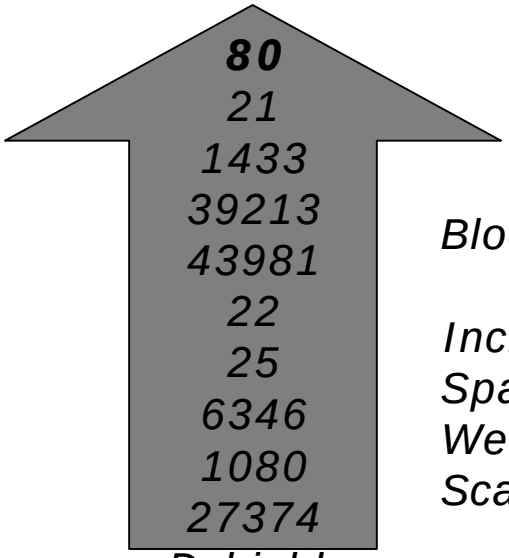
*Blocked packets:**233.919***

Incidents: 785
SpamCop: 125
WebDefacements: 22
Scans: 414

Statistics

- July 2002



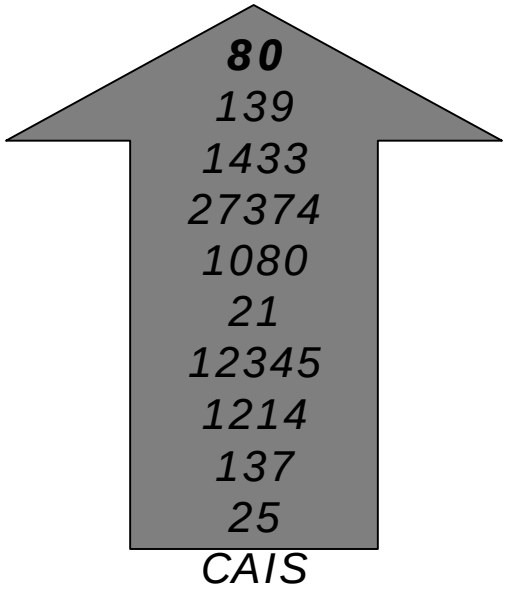


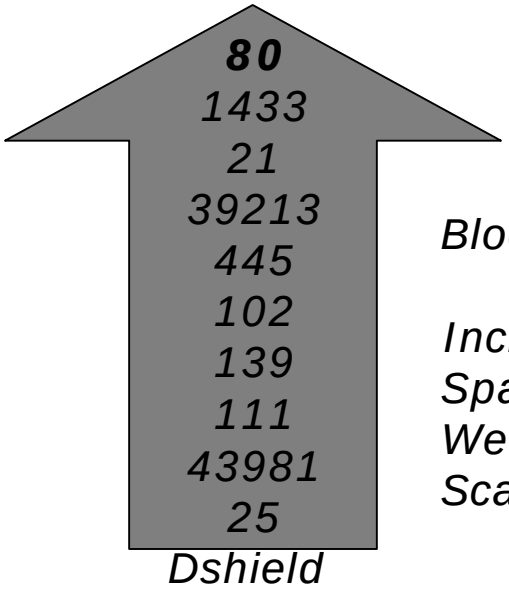
Blocked packets: ***155.258***

Incidents: 878
SpamCop: 172
WebDefacements: 48
Scans: 455

Statistics

- August 2002



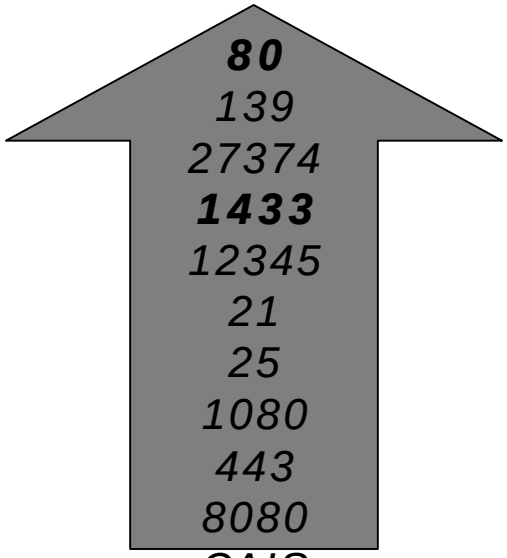


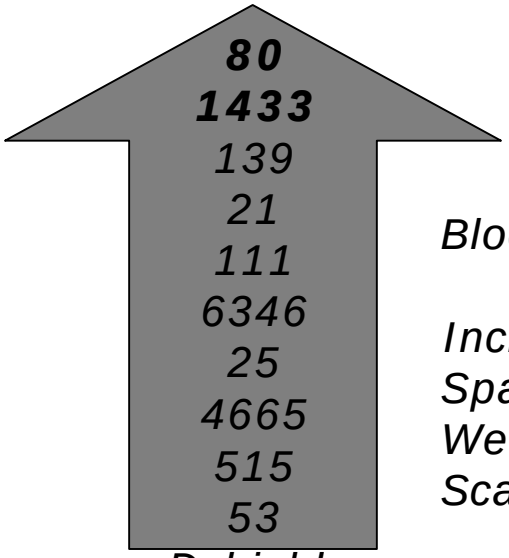
Blocked packets: ***215.169***

Incidents: 1019
SpamCop: 102
WebDefacements: 41
Scans: 623

Statistics

- September 2002





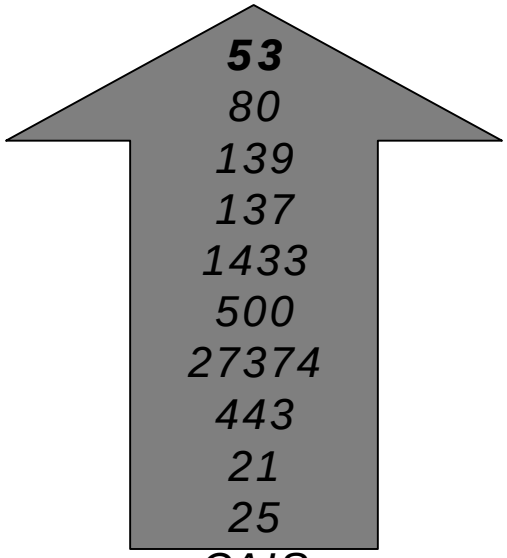
Blocked packets: ***94.177***

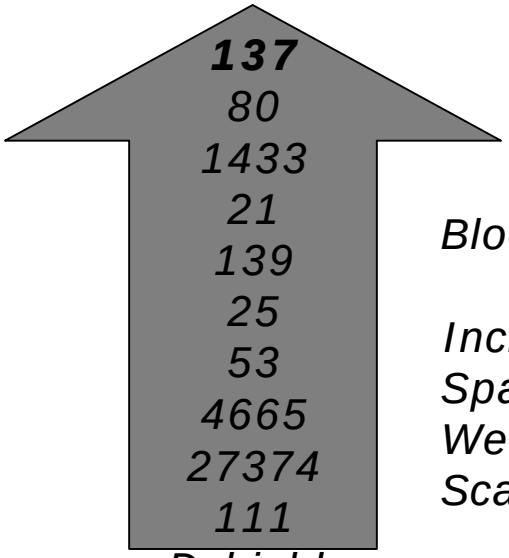
Incidents: 1005
SpamCop: 116
WebDefacements: 32
Scans: 539

- *CA-2002-27 Worm Slapper*

Statistics

- October 2002



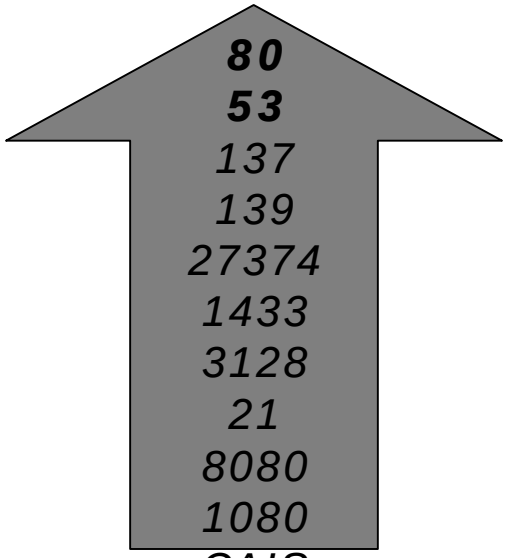


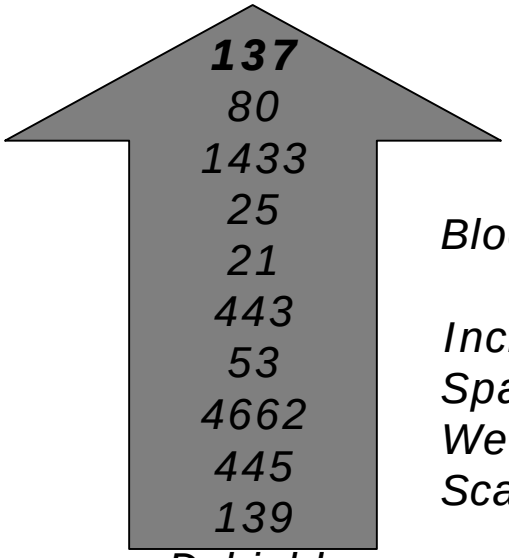
Blocked packets: ***152.844***

Incidents: 1367
SpamCop: 10
WebDefacements: 30
Scans: 944

Statistics

- November 2002





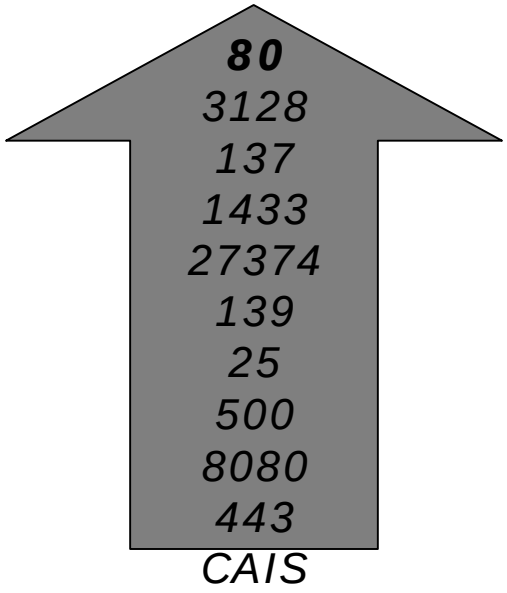
Blocked packets: ***118.114***

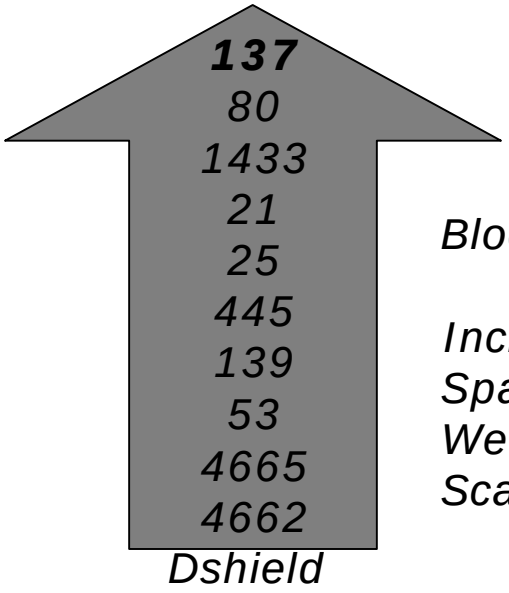
Incidents: 1295
SpamCop: 25
WebDefacements: 24
Scans: 926

- *CA-2002-31 Multiple Vulnerabilities in BIND*

Statistics

- December 2002

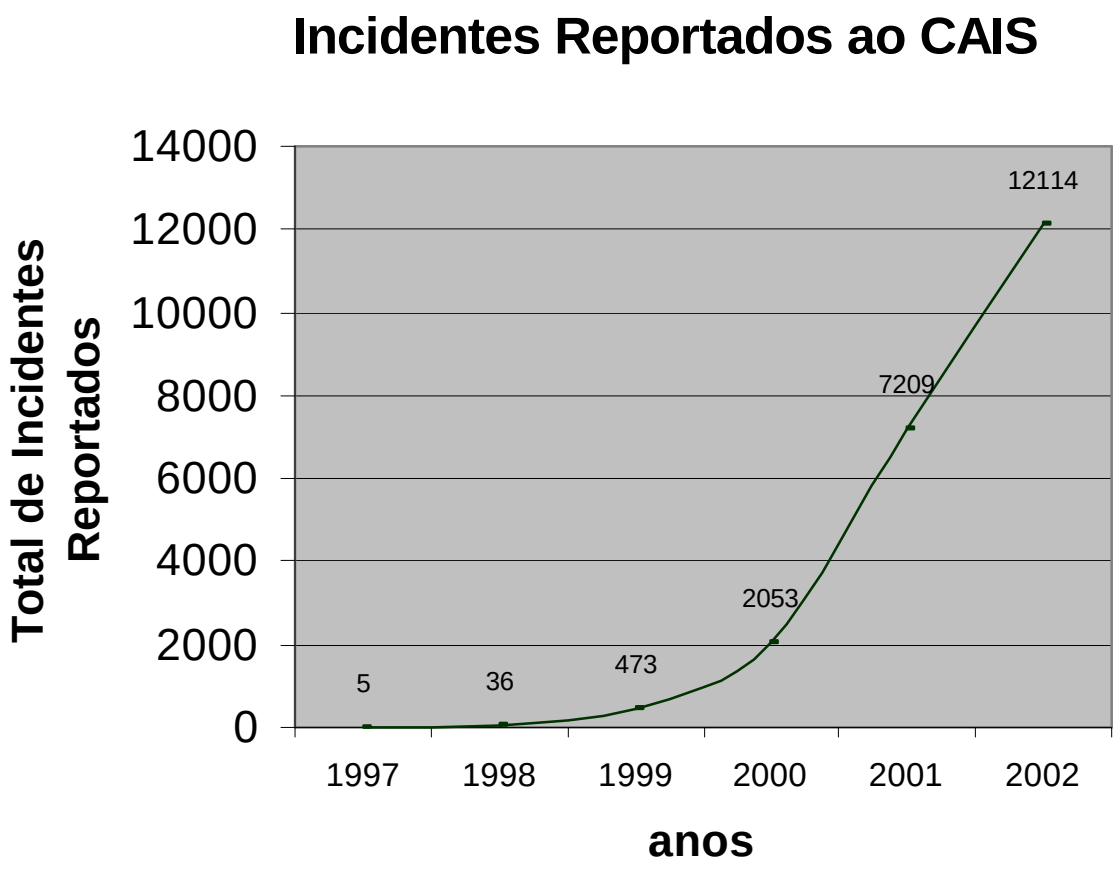




Blocked packets: ***148.398***

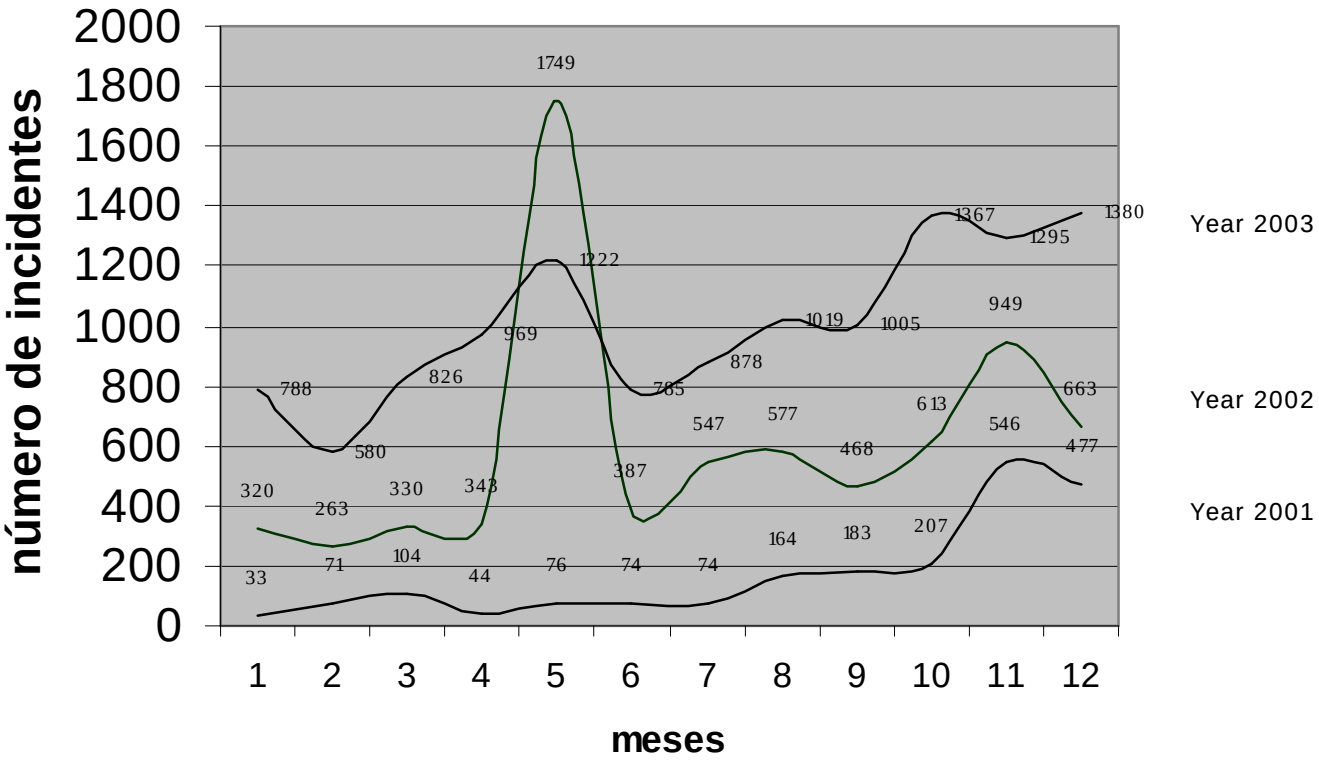
Incidents: 1380
SpamCop: 169
WebDefacements: 36
Scans: 888

Annual Statistics: Incidents Reported



Annual Statistics: Incidents Reported

Incidentes Reportados ao CAIS 2002



Conclusions

- Statistics help to predict the future, make assumptions about hacker activities and so on. If you have solids statistics, they can support you to make trends.
- Statistics support action plans in order to improve security level of your constituency networks. These action plans can include security alerts, recommendations, best practices about systems and services configuration, security policies.
- Statistics give credibility to incident handling activities because your "numbers" gain some "meaning" and help you to improve incident handling procedures, investigation and analysis process.

References

- http://www.caida.org/
- http://www.securitystats.com/
- http://www.cert.org/stats/cert_stats.html
- http://www.dshield.org/
- http://www.mynetwatchman.com/
- http://www.internetsecuritynews.com/securitystatistics.htm