Estatísticas Top 10

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

Rede Nacional de Ensino e Pesquisa – RNP

Centro de Atendimento a Incidentes de Segurança - CAIS

GTER15 + GTS Abril, 2003

Conteúdo

Introdução

- Estatísticas são uma excelente fonte de informações **(confiança?)**
- Estatísticas permitem visualização geral ou específica **(foco!)**
- Estatísticas devem estar disponíveis em tempo real **(agora!)**
- Estatísticas devem ser geradas automaticamente **(facilidade!)**

Motivação

- Prover informação útil aos técnicos dos Grupos de Segurança para tomada de decisões e planejamento estratégicos.
- Gerar informações adicionais para os alertas de segurança.
- Montar uma rede em larga escala e confiável.
- Trocar informações com outros Grupos de Segurança.
- Estatísticas na área de segurança são escassas.

Estatísticas

- Top 10 Portas — hora / diário / semanal / mensal
- Top 10 IPs — hora / diário / semanal / mensal
- Tendências — hora / diário / semanal / mensal
- Novas portas x Histórico de portas — **(uhm!)**
- Slow scan/probe — semanal / mensal — **(uhm!!)**
- Detector de Aceleração — **(uhm!!!)**
- Verificação de IPs das "Redes Atendidas" — **(bonus!)**

Estatísticas

- Exemplo prático de 2003, CodeRed.F
- Date: Mon, 10 Mar 2003 00:00:22 -0300 (BRT)
- From: [redacted]
- To: [redacted]
- Subject: ips-portas diaria Mon Mar 10 00:00:00 BRT 2003

- 445 1112
- **80 438**
- 524 166
- 443 71
- 1080 22
- 21 16
- 53 13

Estatísticas

- Exemplo prático de 2003, CodeRed.F
- Date: Tue, 11 Mar 2003 00:00:21 -0300 (BRT)
- From: [redacted]
- To: [redacted]
- Subject: ips-portas diaria Tue Mar 11 00:00:00 BRT 2003

- 445 792
- **80 534**
- 524 162
- 139 24
- 1080 20
- 3128 12

Estatísticas

- Exemplo prático de 2003, CodeRed.F
- Date: Wed, 12 Mar 2003 00:02:34 -0300 (BRT)
- From: [redacted]
- To: [redacted]
- Subject: ips-portas diaria Wed Mar 12 00:00:00 BRT 2003

- **80 4683**
- 445 244
- 524 150
- 1080 82
- 139 79
- 3128 41
- 8080 37

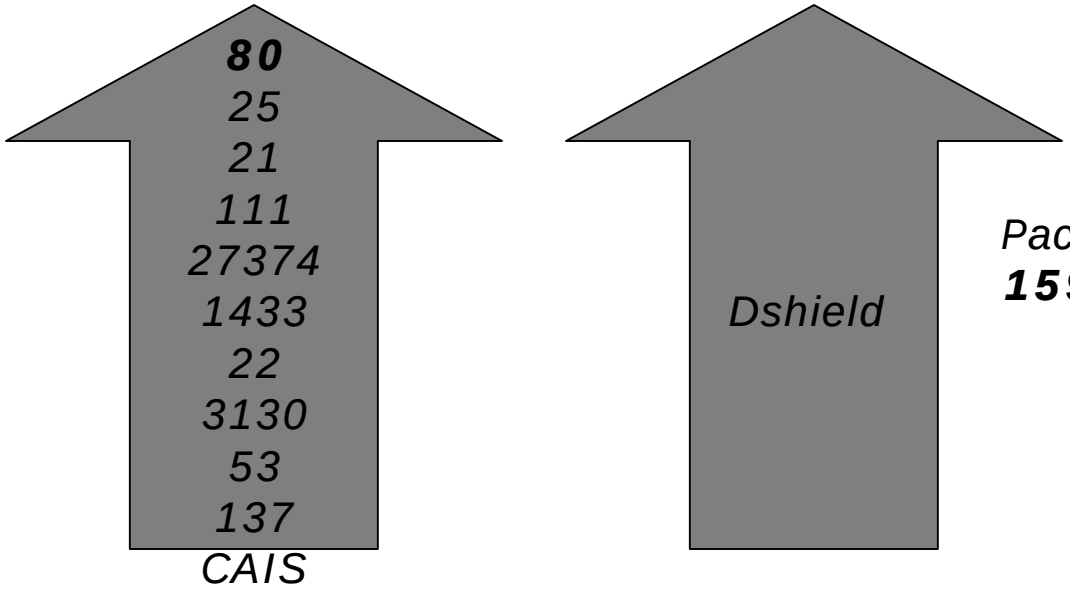
Estatísticas

- Exemplo prático de 2003, CodeRed.F
- Date: Thu, 13 Mar 2003 00:03:09 -0300 (BRT)
- From: [redacted]
- To: [redacted]
- Subject: [top-10] ips-portas diaria Thu Mar 13 00:00:00 BRT 2003

- **80 7007**
- 139 90
- 1080 16
- 25 14
- 21 12
- 22 6
- 3128 4

Estatísticas

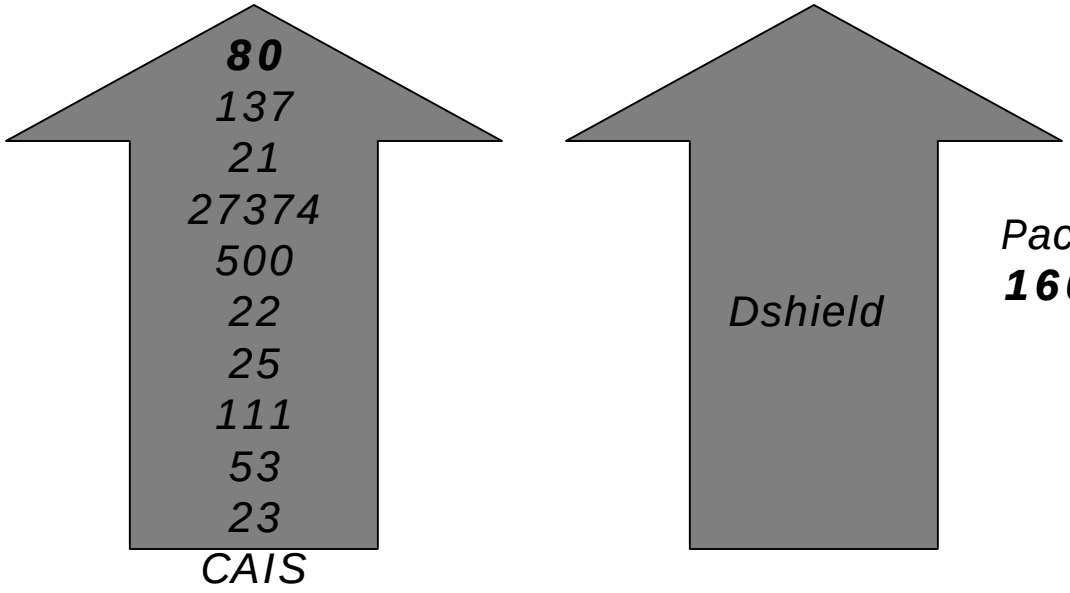
- Janeiro 2002



Pacotes bloqueados:
159.760

Estatísticas

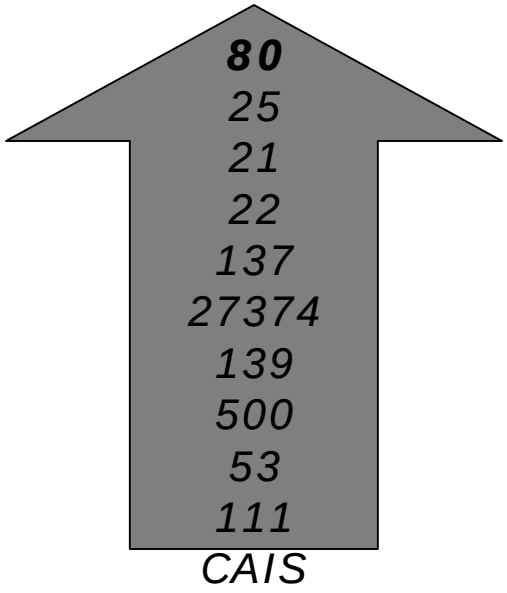
- Fevereiro 2002

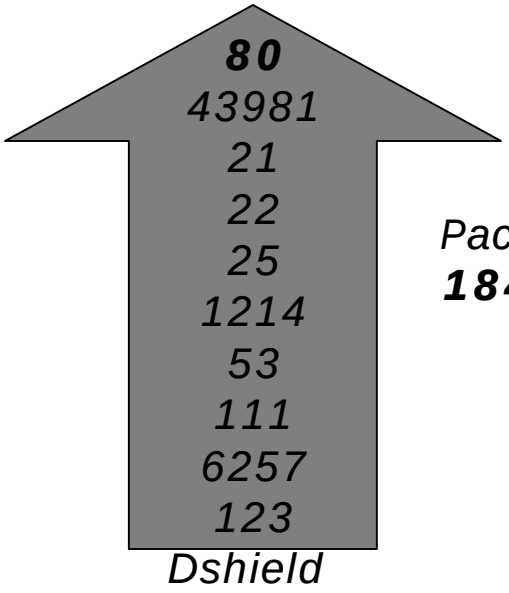


Pacotes bloqueados:
160.109

Estatísticas

- Março 2002

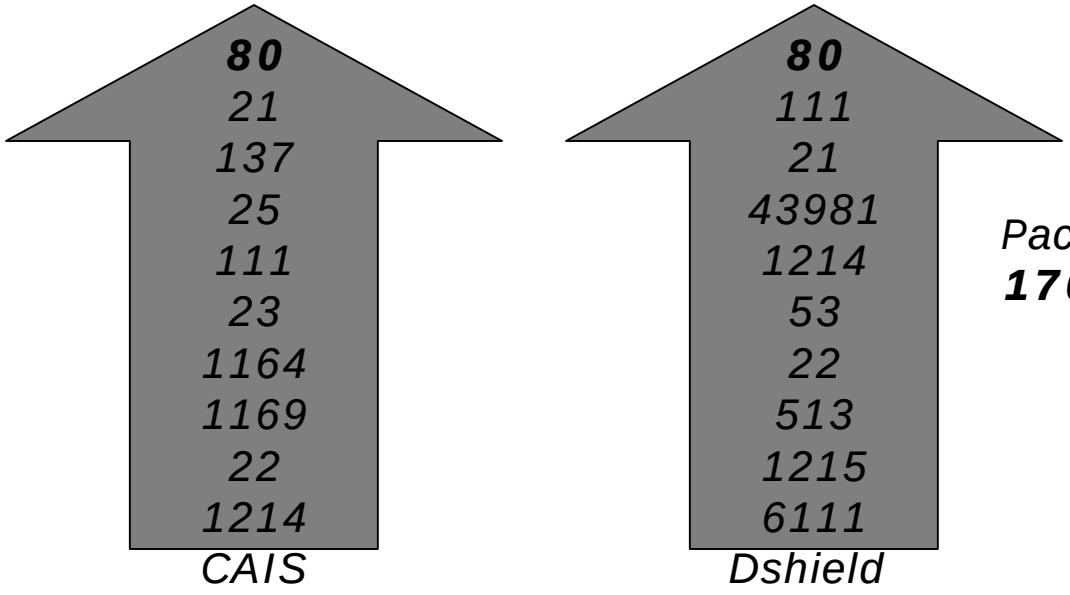




Pacotes bloqueados:
184.647

Estatísticas

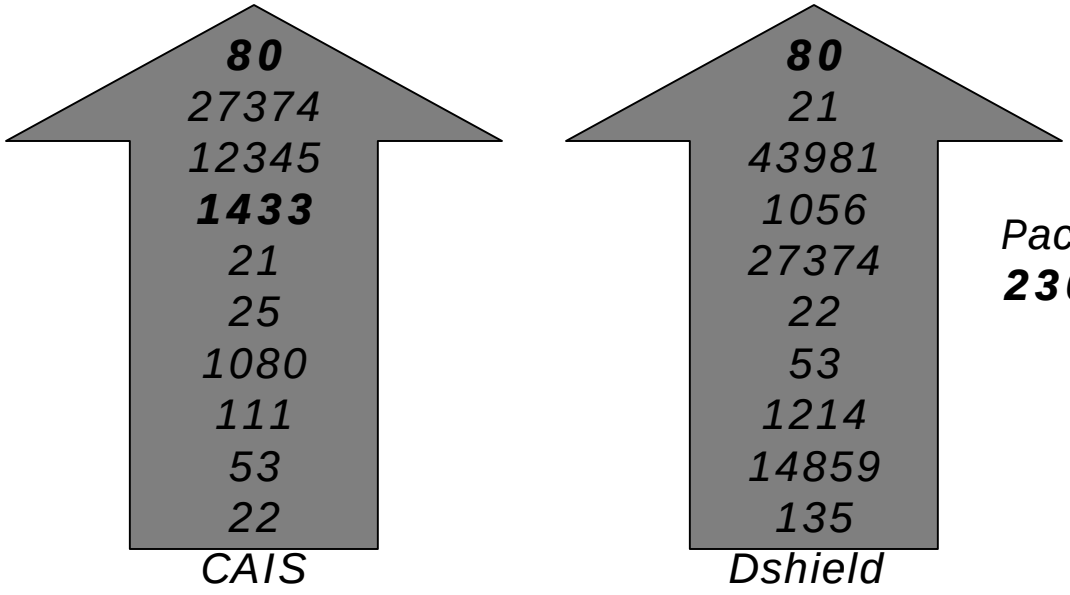
- Abril 2002



Pacotes bloqueados:
170.037

Estatísticas

- Maio 2002

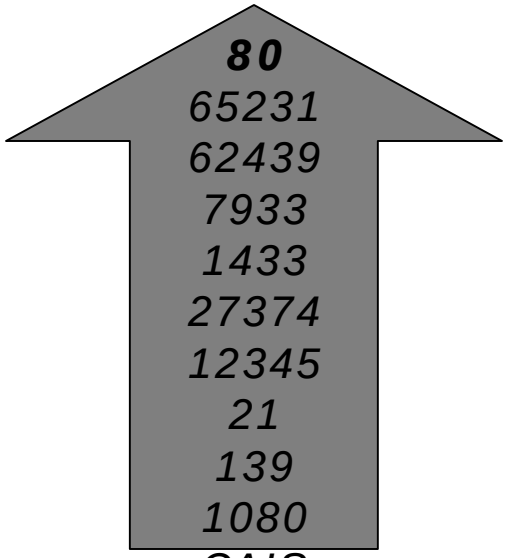


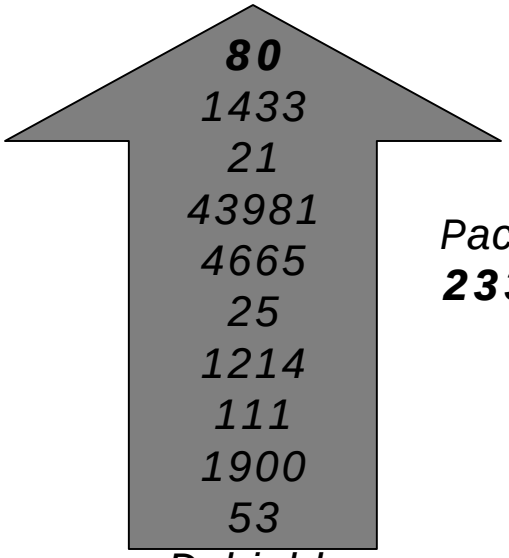
Pacotes bloqueados:
230.671

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

Estatísticas

- Junho 2002

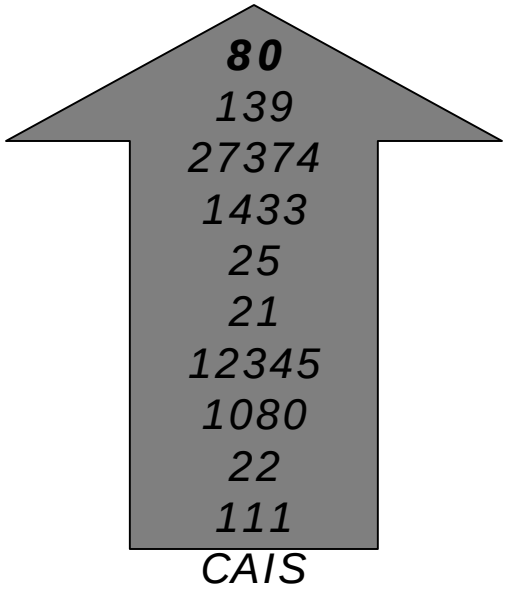


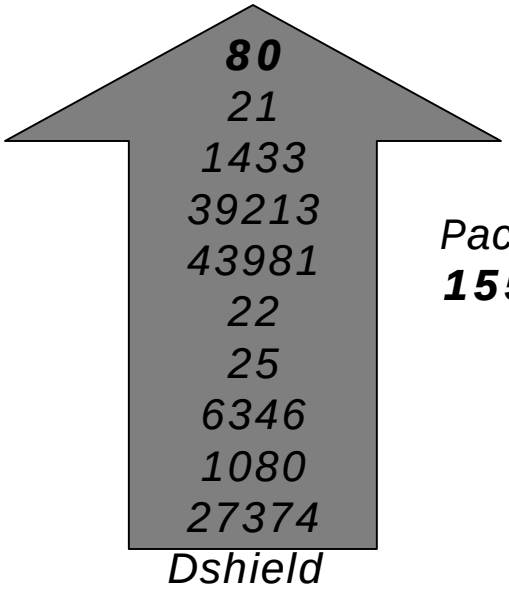


Pacotes bloqueados:
233.919

Estatísticas

- Julho 2002

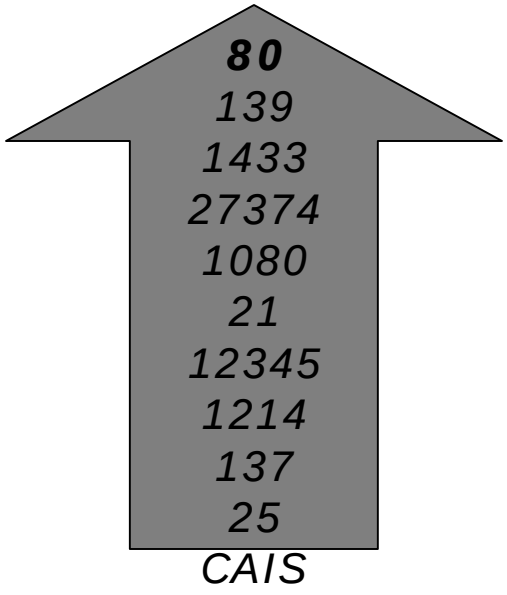


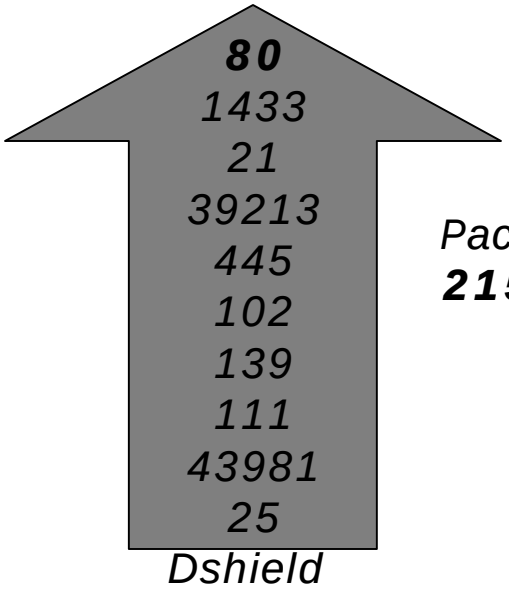


Pacotes bloqueados:
155.258

Estatísticas

- Agosto 2002

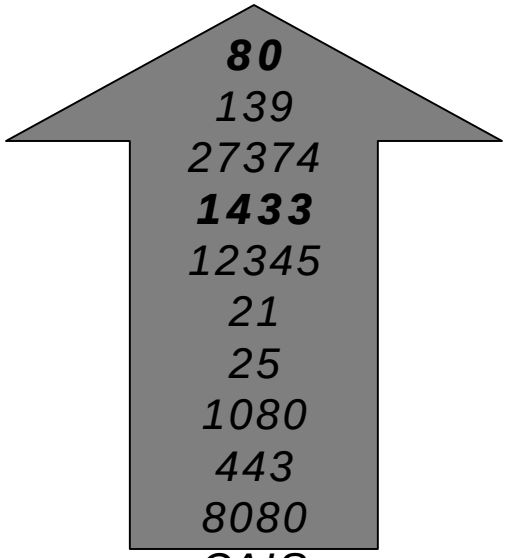


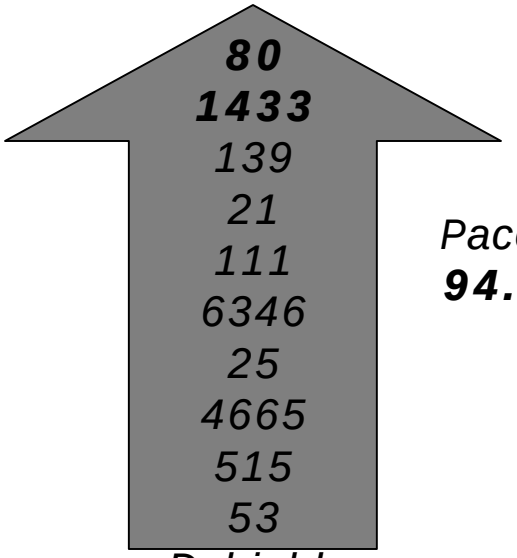


Pacotes bloqueados:
215.169

Estatísticas

- Setembro 2002



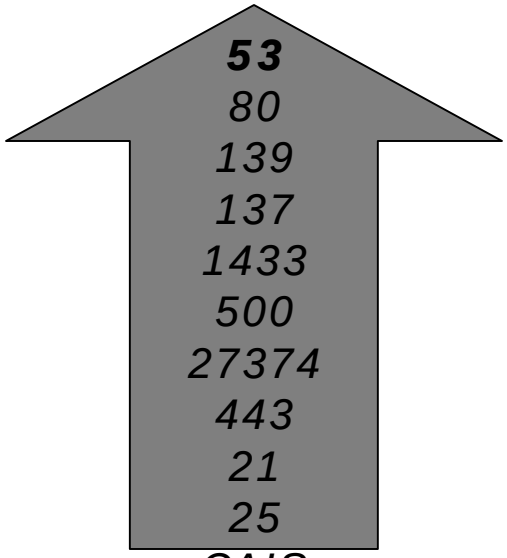


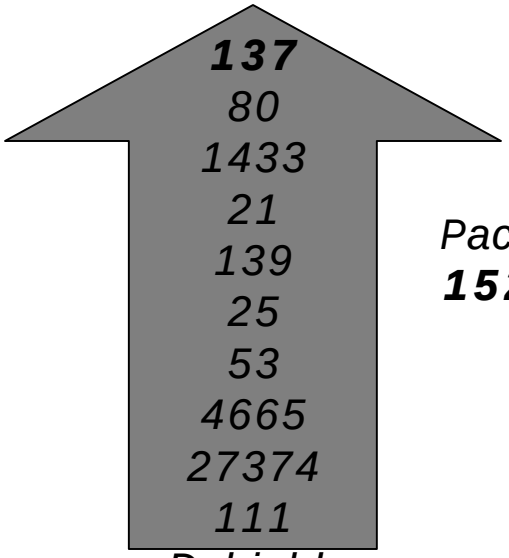
Pacotes bloqueados:
94.177

- *CA-2002-27 Worm Slapper*

Estatísticas

- Outubro 2002

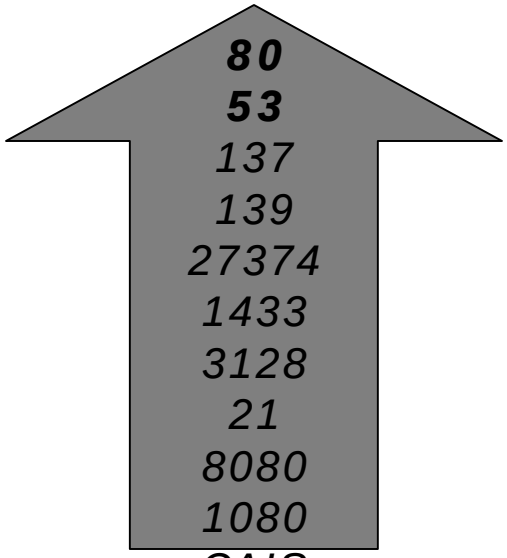


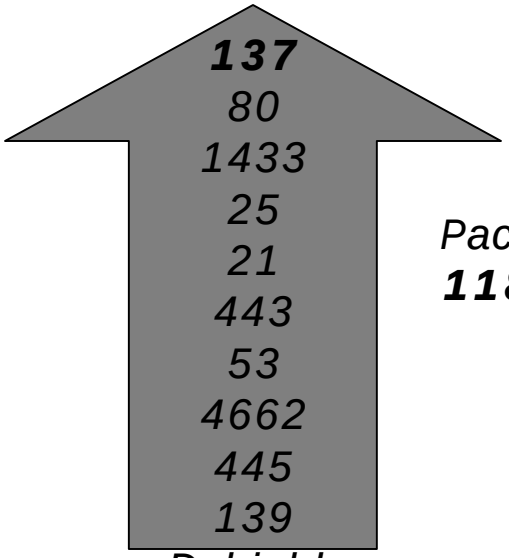


Pacotes bloqueados:
152.844

Estatísticas

- Novembro 2002



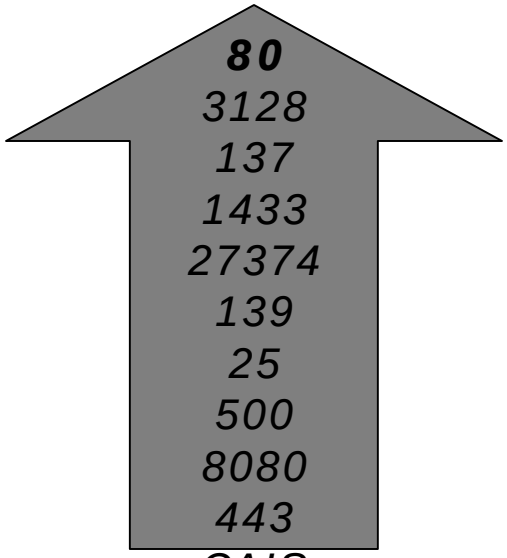


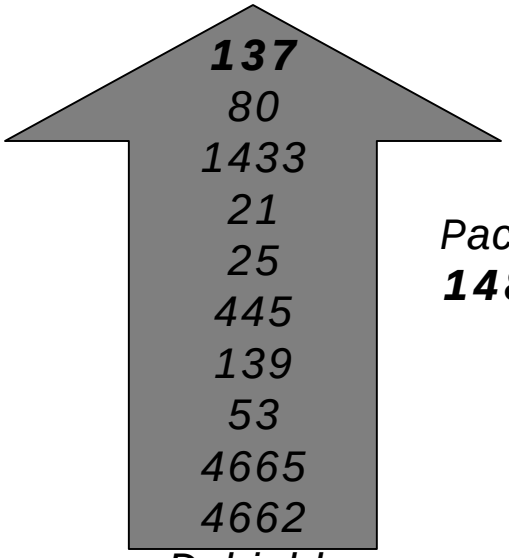
Pacotes bloqueados:
118.114

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

Estatísticas

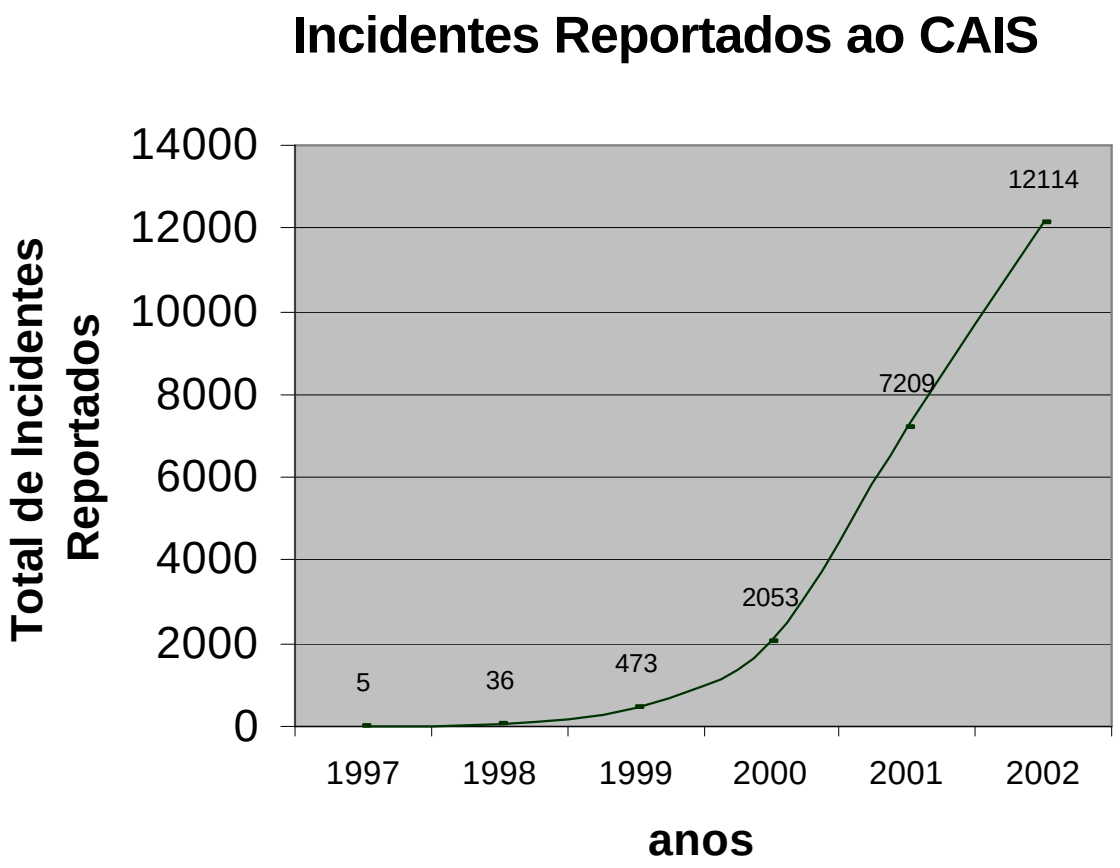
- Dezembro 2002





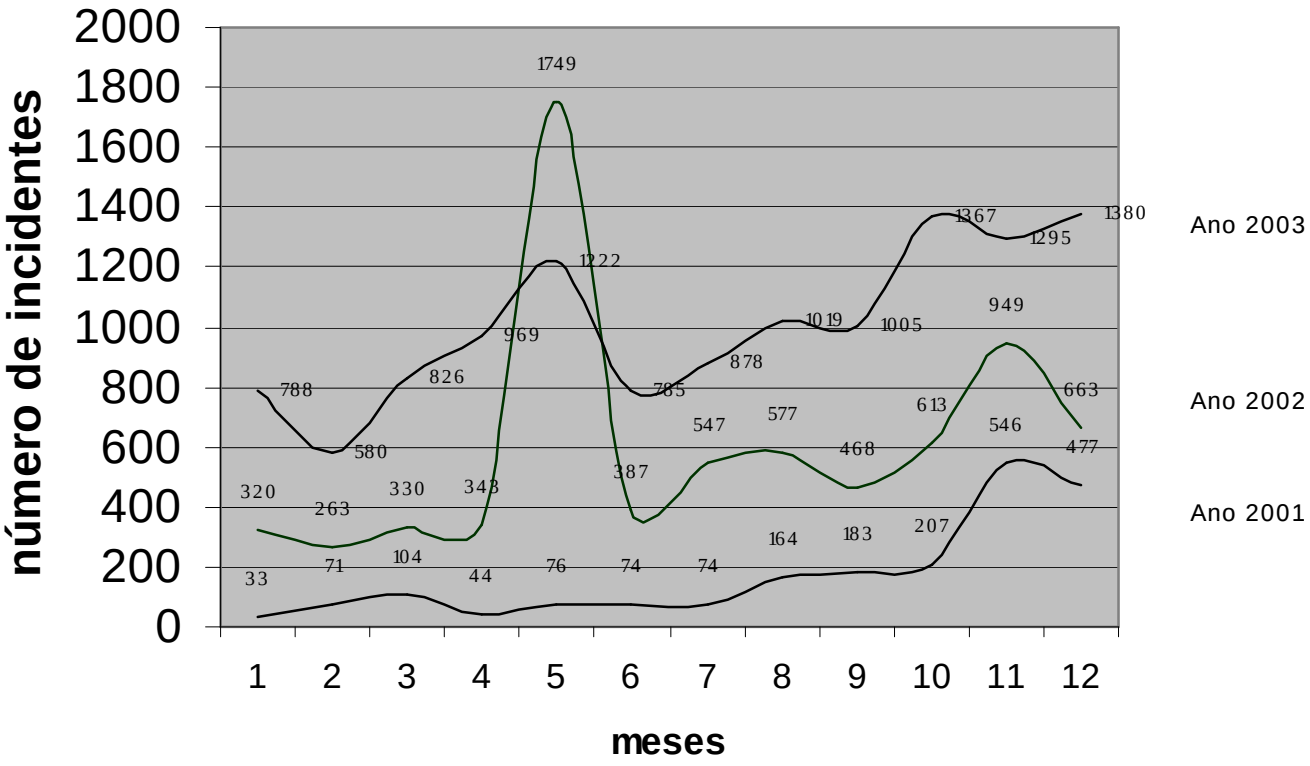
Pacotes bloqueados:
148.398

Estatísticas Anuais: Incidentes Reportados



Estatísticas Anuais: Incidentes Reportados

Incidentes Reportados ao CAIS 2002



Conclusões

- Estatísticas ajudam a prever o futuro, fazer conjecturas sobre atividades *hackers*. Se você tiver estatísticas bem embasadas você poderá traçar tendências.
- Estatísticas provêem suporte para ações que visam aumentar a segurança das suas redes. Estas ações incluem alertas de segurança, recomendações, melhores práticas sobre sistemas e serviços e políticas de segurança.
- Estatísticas fornecem credibilidade para o tratamento de incidentes pois é possível dar "sentido" aos "números" e auxiliam no processo de análise e investigação.

Referências

- 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
- **http://www.nbso.nic.br/stats/**
- **http://www.rnp.br/cais/estatisticas.html**