Uso de Honeypots de Baixa Interatividade na Resposta a Incidentes de Segurança

NIC BR Security Office – NBSO

Brazilian Computer Emergency Response Team

Comitê Gestor da Internet no Brasil

http://www.nbso.nic.br/

Roteiro

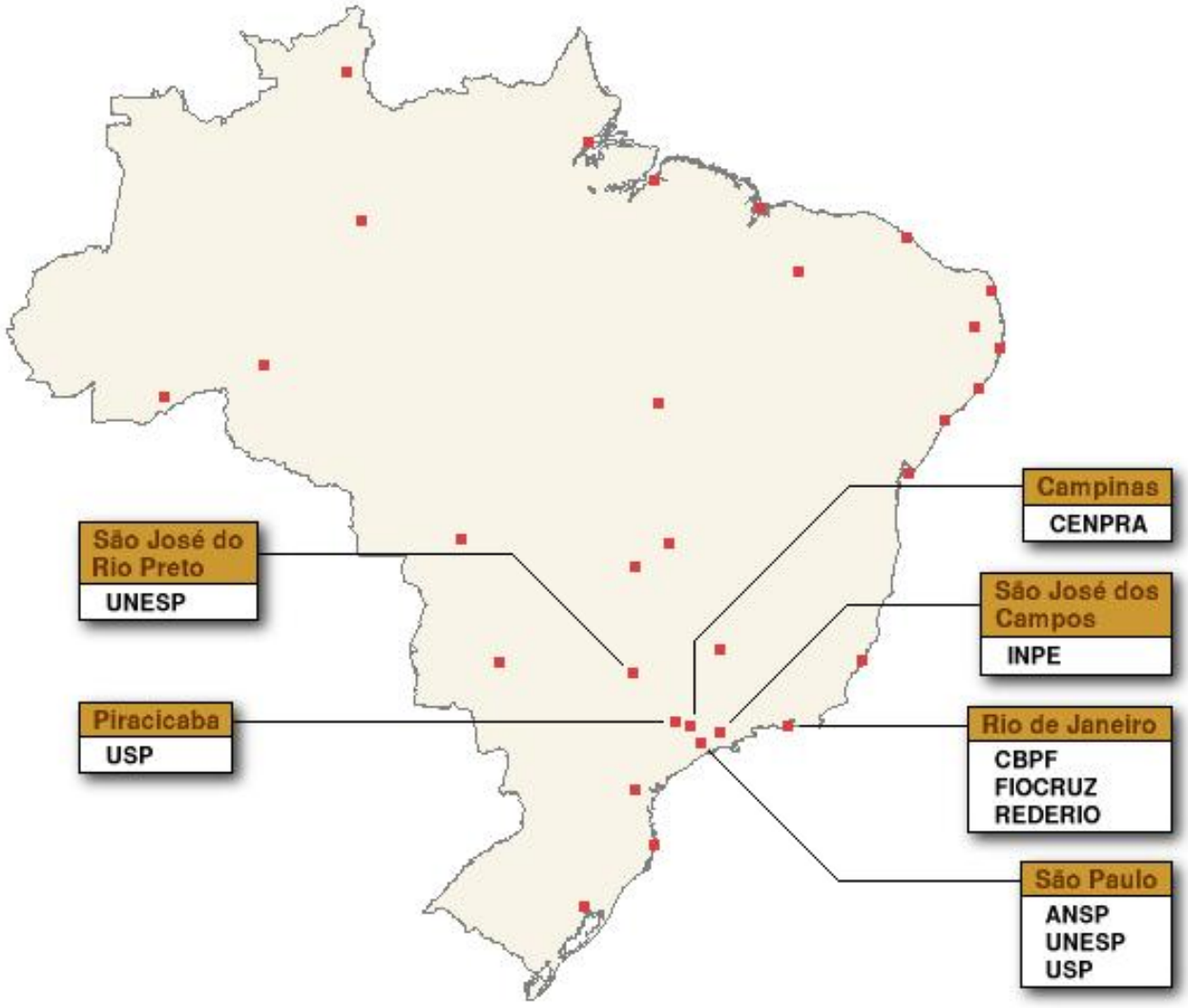
- Consórcio brasileiro de honeypots
- Uso dos dados pelo NBSO
  - identificação do tráfego malicioso
  - envio de notificações
- Atividades observadas
  - worms/vírus
  - origem das atividades
  - sistemas operacionais de origem
- Conclusões

Consórcio Brasileiro de Honeypots

- Honeypots são mantidos pelas instituições consorciadas
- Objetivo de aumentar, no espaço Internet brasileiro, a capacidade de:
  - detecção de incidentes
  - correlação de eventos
  - determinação de tendências de ataques
- Utilização dos dados por grupos de resposta a incidentes

Consórcio Brasileiro de Honeypots

http://www.honeypots-alliance.org.br/



Uso dos Dados pelo NBSO

- Identificação de ataques conhecidos
  - detecção de servidores comprometidos realizando varreduras
- Detecção de worms/vírus:
  - mostram um número enorme de máquinas vulneráveis, facilmente exploráveis
- Comparação com incidentes reportados voluntariamente

Uso dos Dados pelo NBSO (cont)

- Uma vez identificada a atividade maliciosa:
  - identificados IPs de origem brasileiros
  - logs são agrupados por IP de origem
  - os contatos são determinados (whois, CSIRTs, etc)
  - montagem e envio dos emails
    * podem ser agrupados por contato

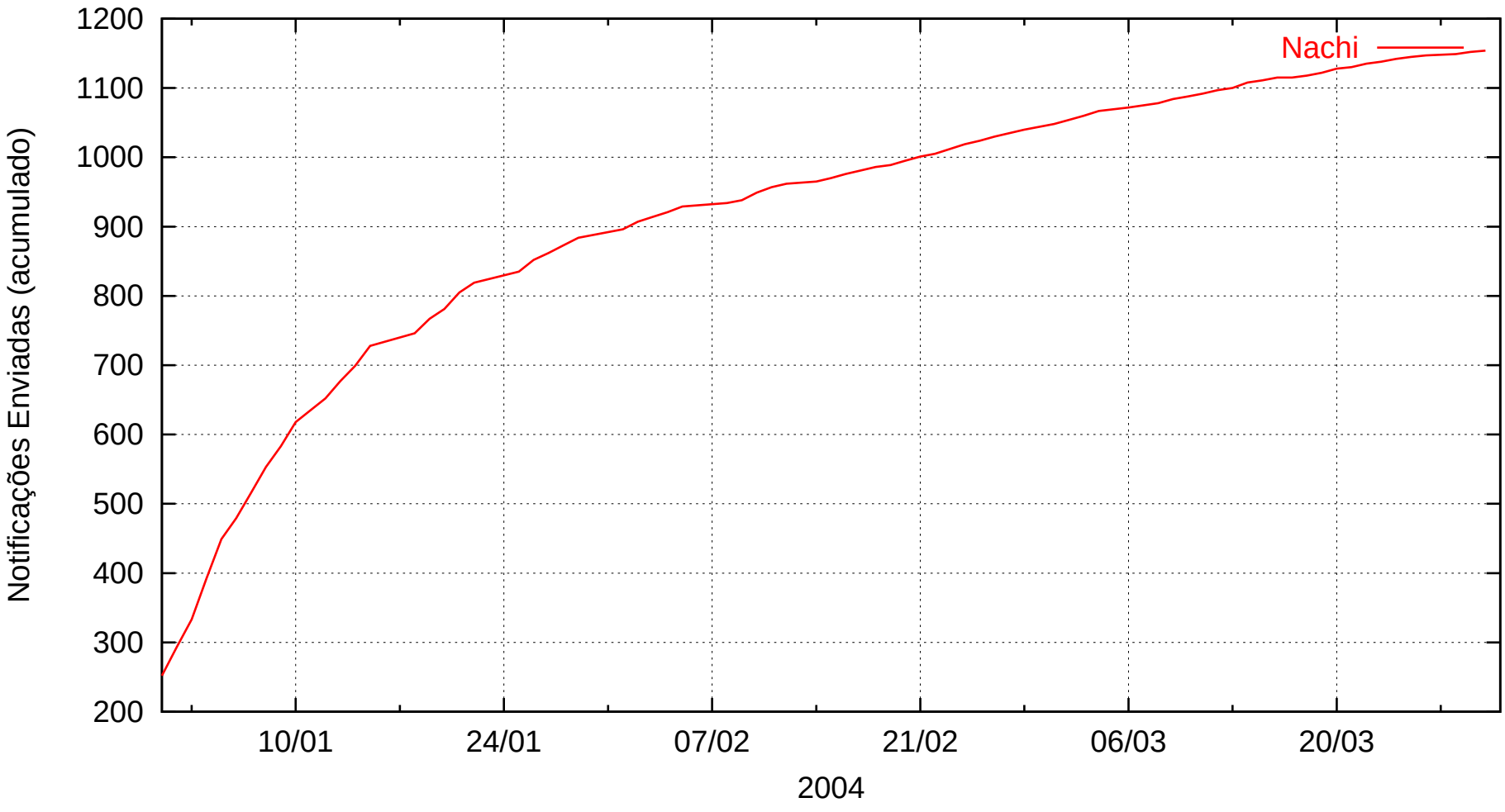
Detecção do tráfego malicioso

- pelo cabeçalho do pacote (src port, dst port, TTL, etc)
- por conteúdo
- Exemplo:

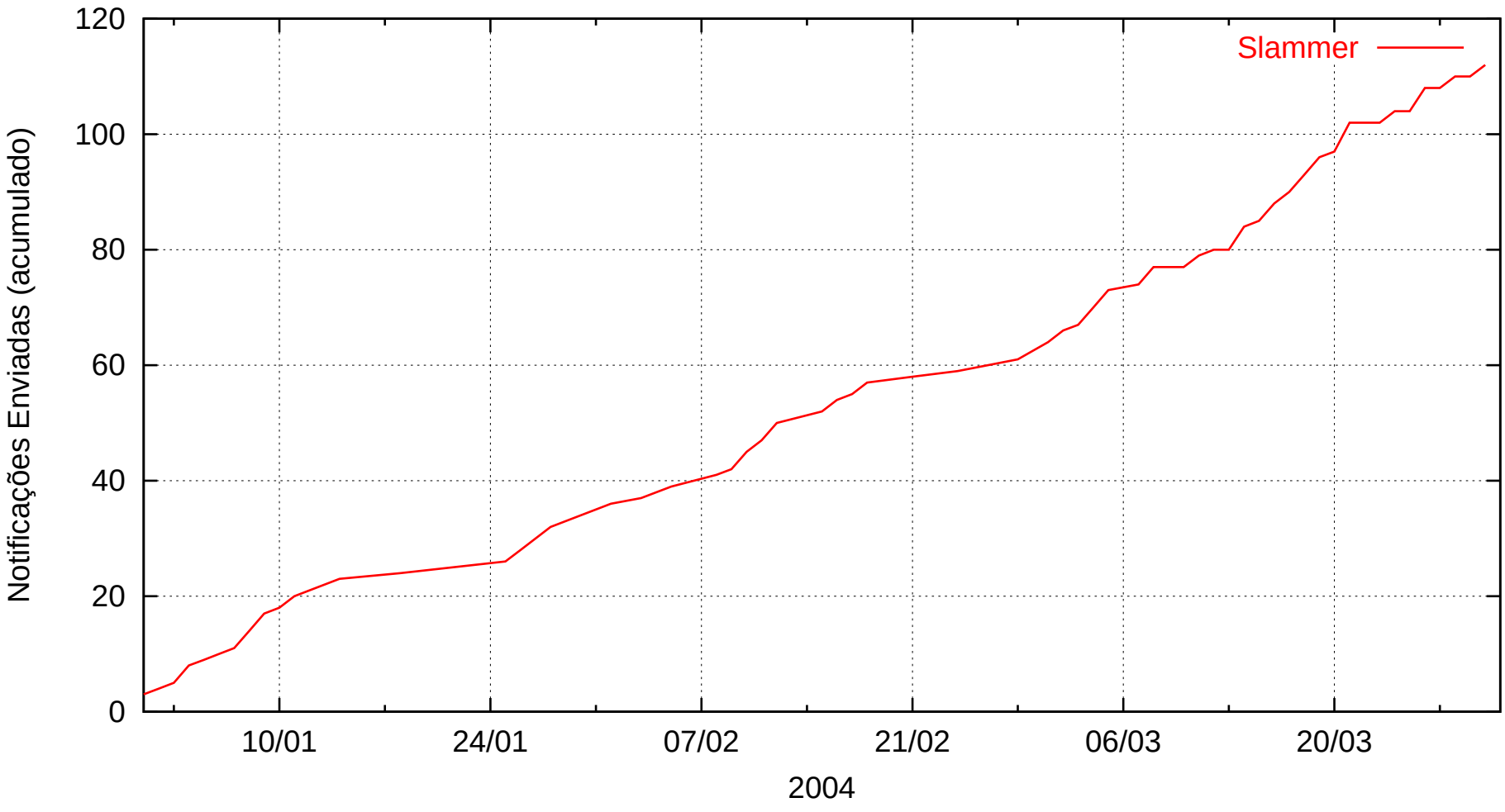
```
ip[8] <= 128 and
ip[8] >= 64 and
ip[2:2] == 92 and
icmp[0] == 8 and
icmp[24:2] == 0xaaaa
```

Atividades Observadas

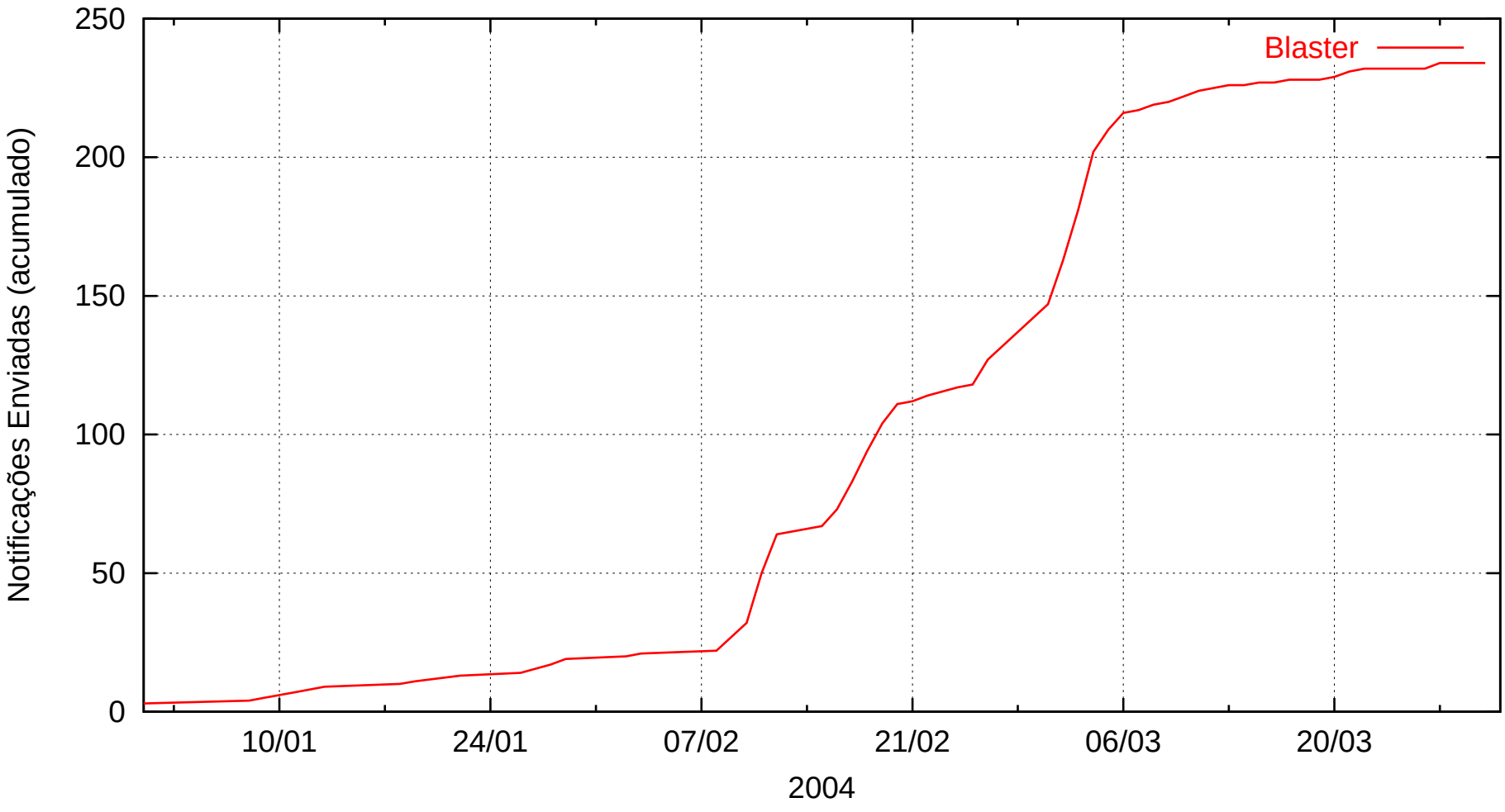
Nachi


Nachi
Notificações Enviadas (acumulado)
1200
1100
1000
900
800
700
600
500
400
300
200
10/01
24/01
07/02
21/02
06/03
20/03
2004

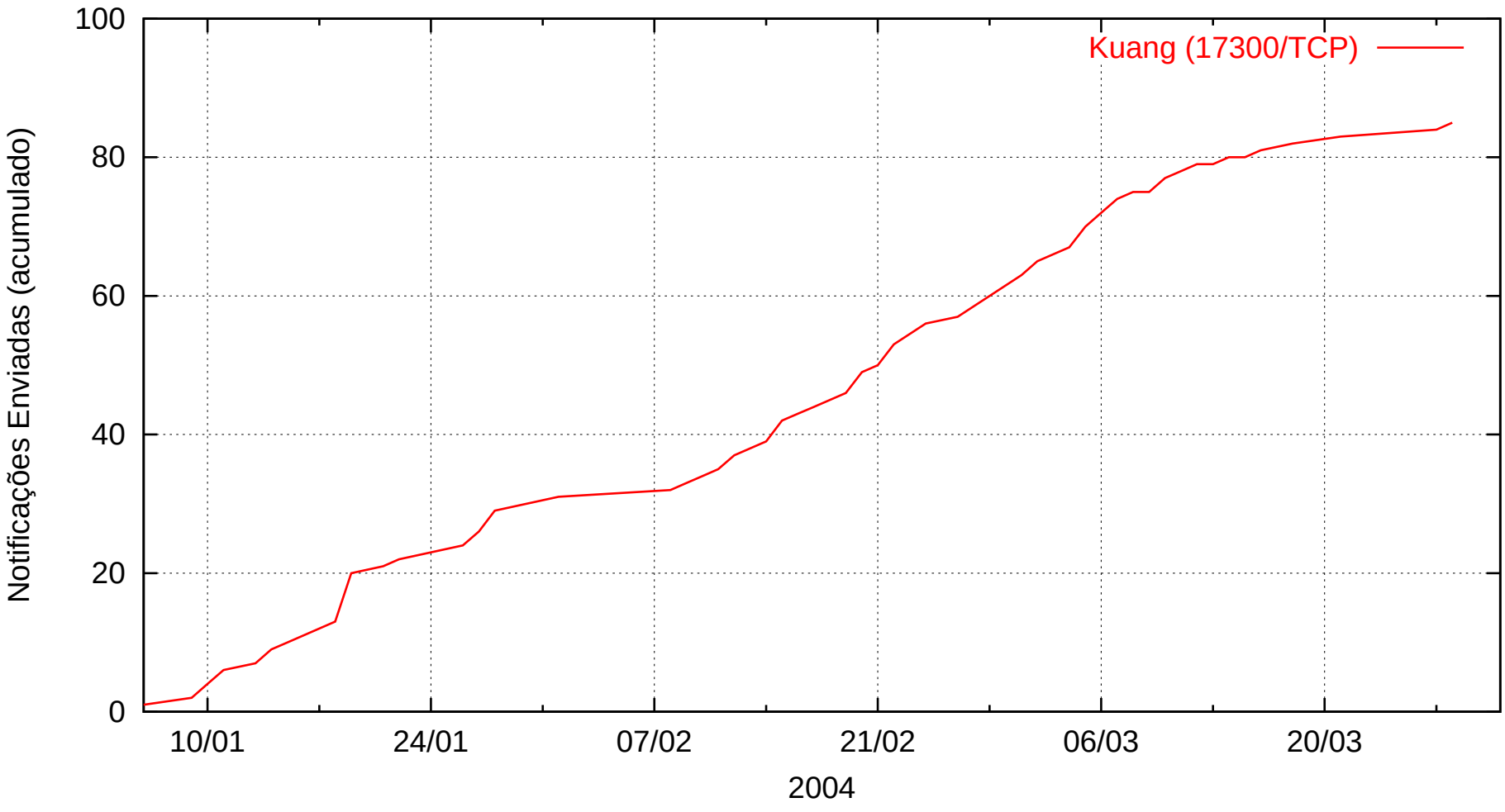
Slammer


Slammer
Notificações Enviadas (acumulado)
120
100
80
60
40
20
0
10/01
24/01
07/02
21/02
06/03
20/03
2004

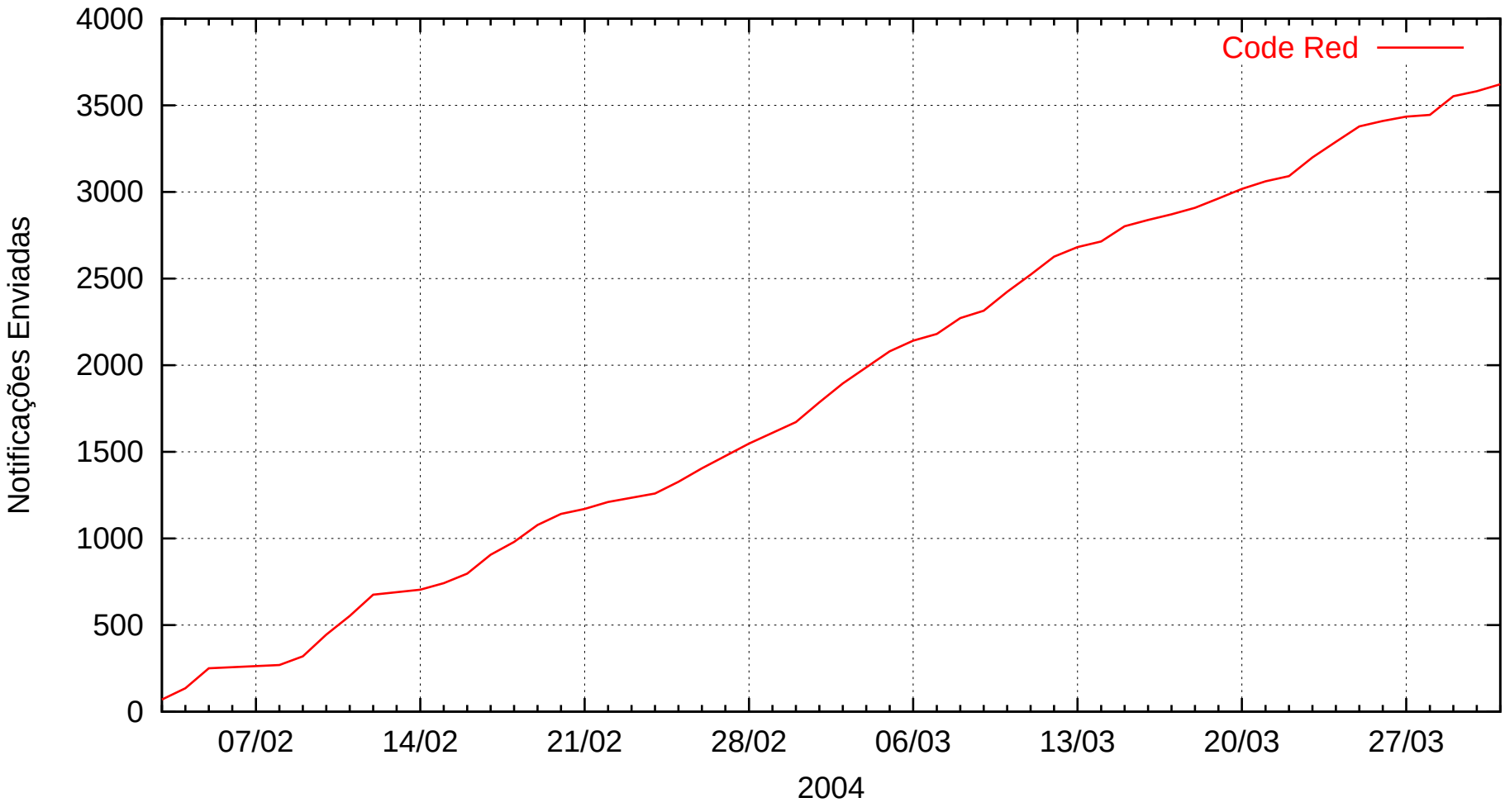
Blaster (DCOM RPC)



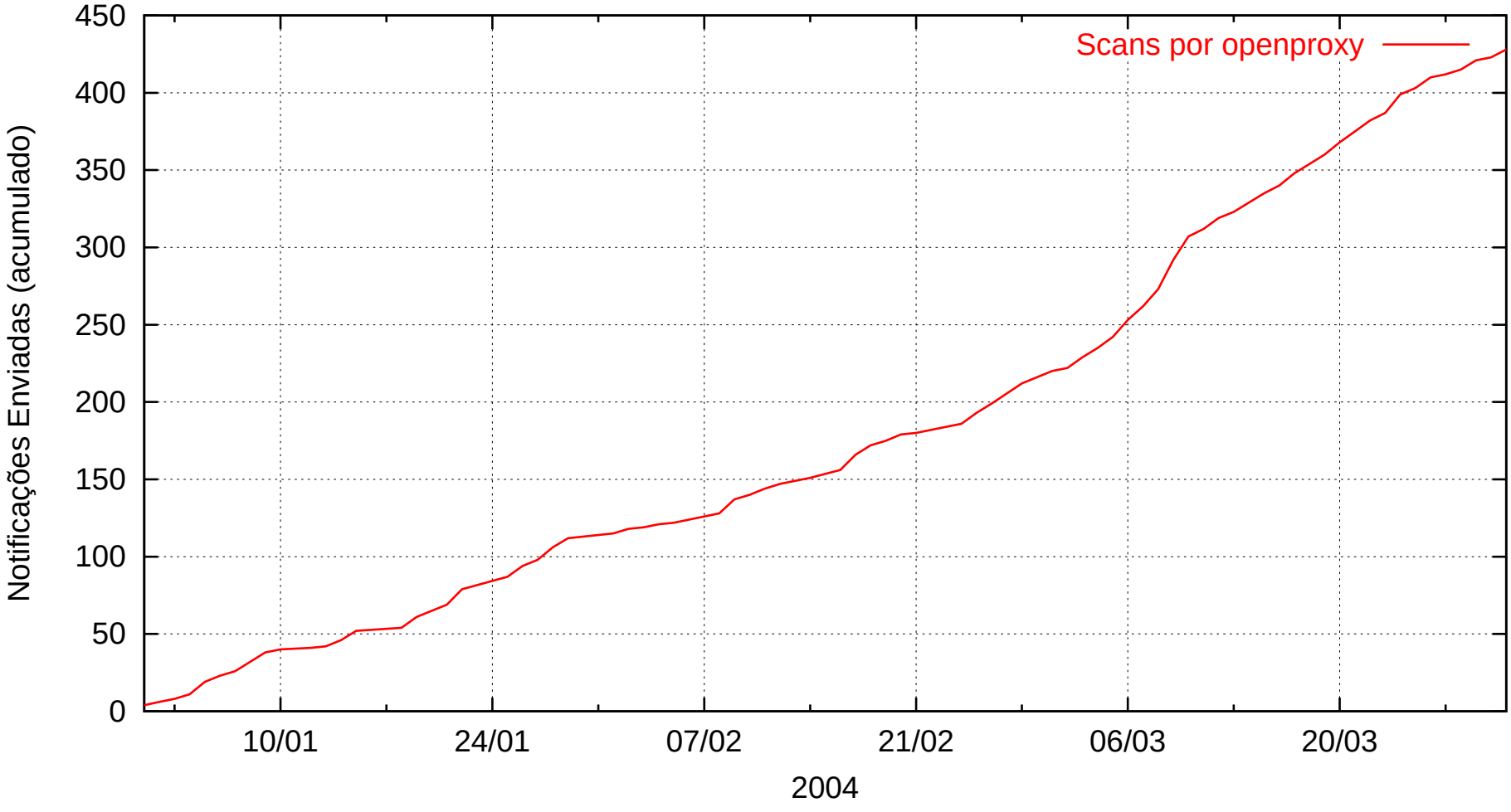
Kuang


Kuang (17300/TCP)
Notificações Enviadas (acumulado)
100
80
60
40
20
0
10/01
24/01
07/02
21/02
06/03
20/03
2004

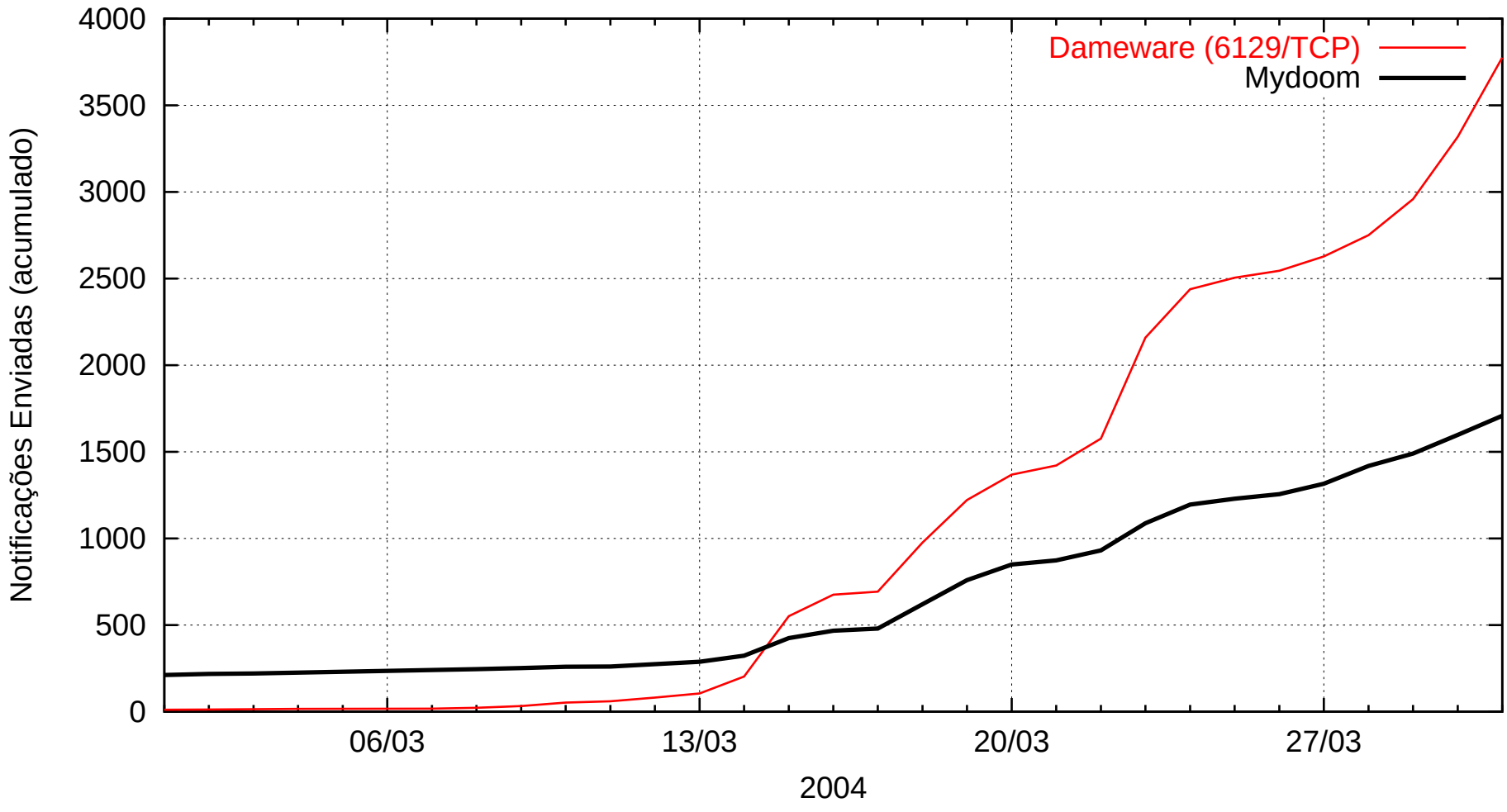
Code Red


Code Red
Notificações Enviadas
4000
3500
3000
2500
2000
1500
1000
500
0
07/02
14/02
21/02
28/02
06/03
13/03
20/03
27/03
2004

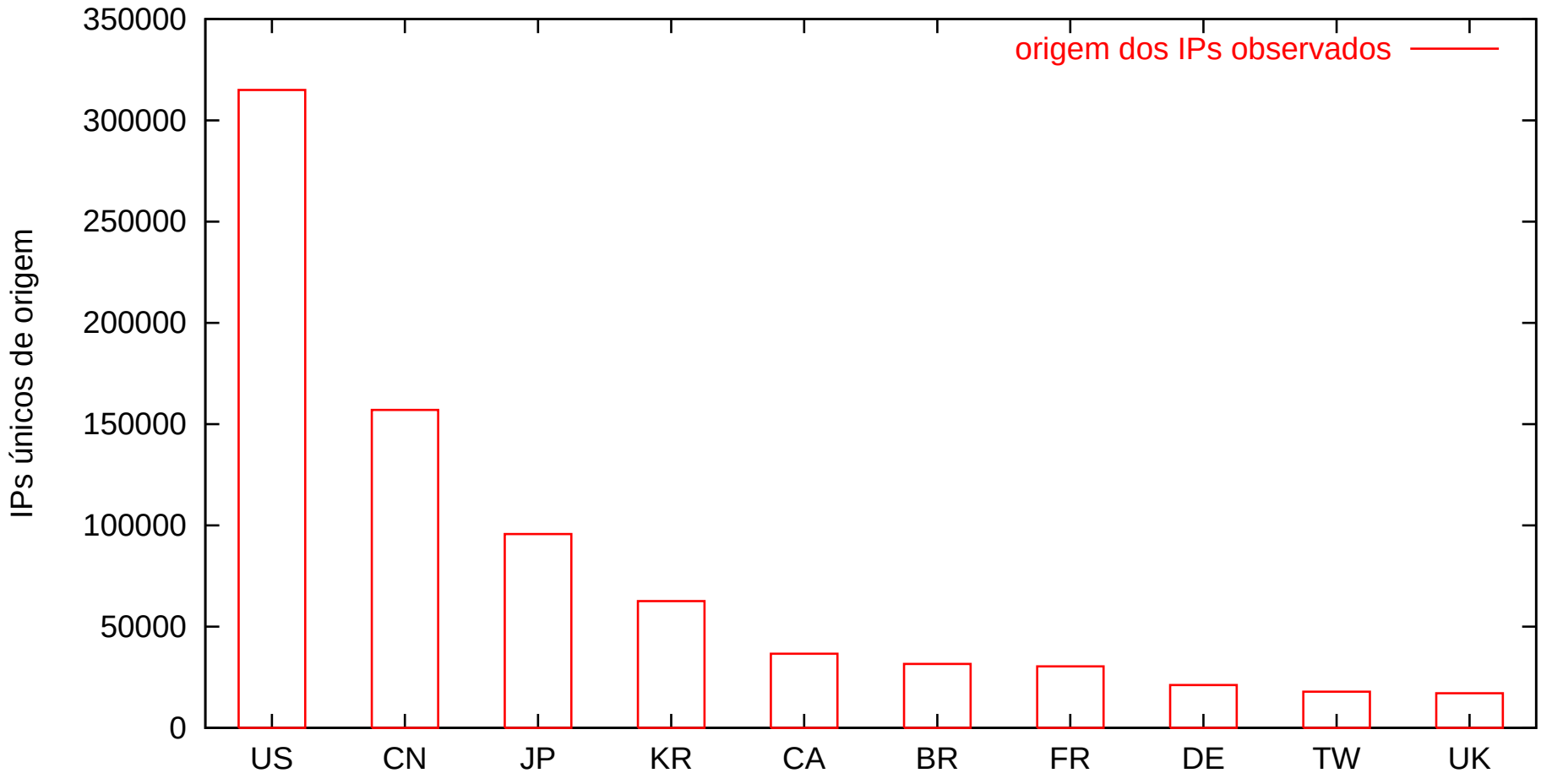
Scan por Open Proxy



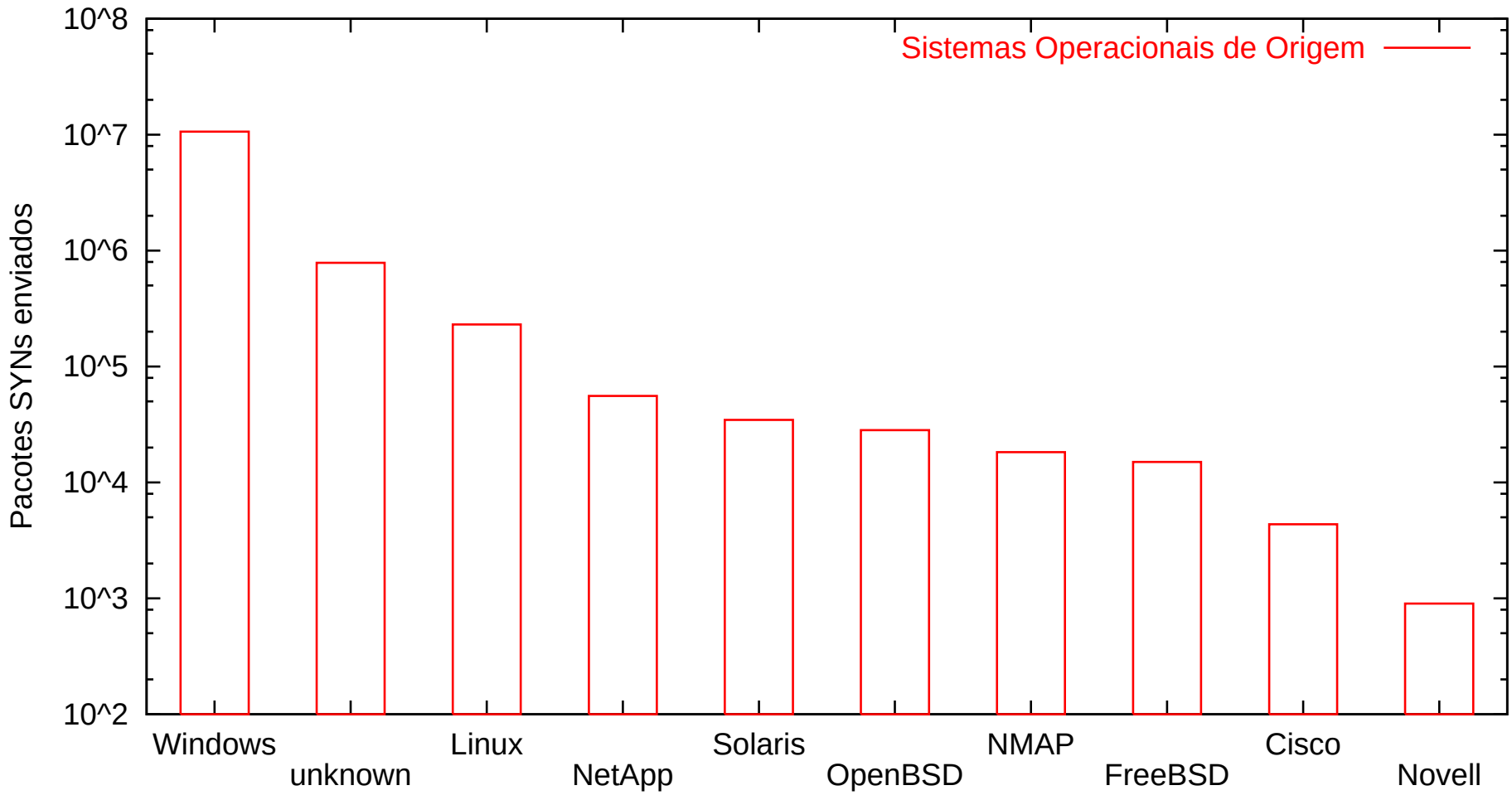
Dameware e Mydoom



Redes de Origem



Sistemas Operacionais de Origem



Conclusões

- Atualmente temos um “Ruído de fundo” na Internet
- Baixo índice de falso positivos
- Evolução das ferramentas de ataque (“API” de exploits)
- A eficácia das notificações dependem das pontas
  - CSIRTs atuantes
  - Contatos técnicos atualizados