Estatísticas sobre o Spam no Brasil

Klaus Steding-Jessen
jessen@nic.br

Marcelo H. P. C. Chaves
mhp@nic.br

NIC BR Security Office – NBSO

Brazilian Computer Emergency Response Team

Comitê Gestor da Internet no Brasil

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

Roteiro

- Objetivos da manutenção de estatísticas
- Origem dos dados
- Categorias de abuso
- Estatísticas agrupadas por:
  - blocos CIDR
  - endereços IP
  - contatos das redes
- Recomendações

Objetivos

- Traçar o perfil do spam no Brasil
  - tipo de abuso mais cometido
  - origens dos problemas
- Ajudar as redes brasileiras a direcionar os esforços
- Acompanhar as mudanças (melhoras ou pioras do quadro)
- **Não** usar os dados para *blacklist*

Origem dos dados

- Emails recebidos em `mail-abuse@nic.br`

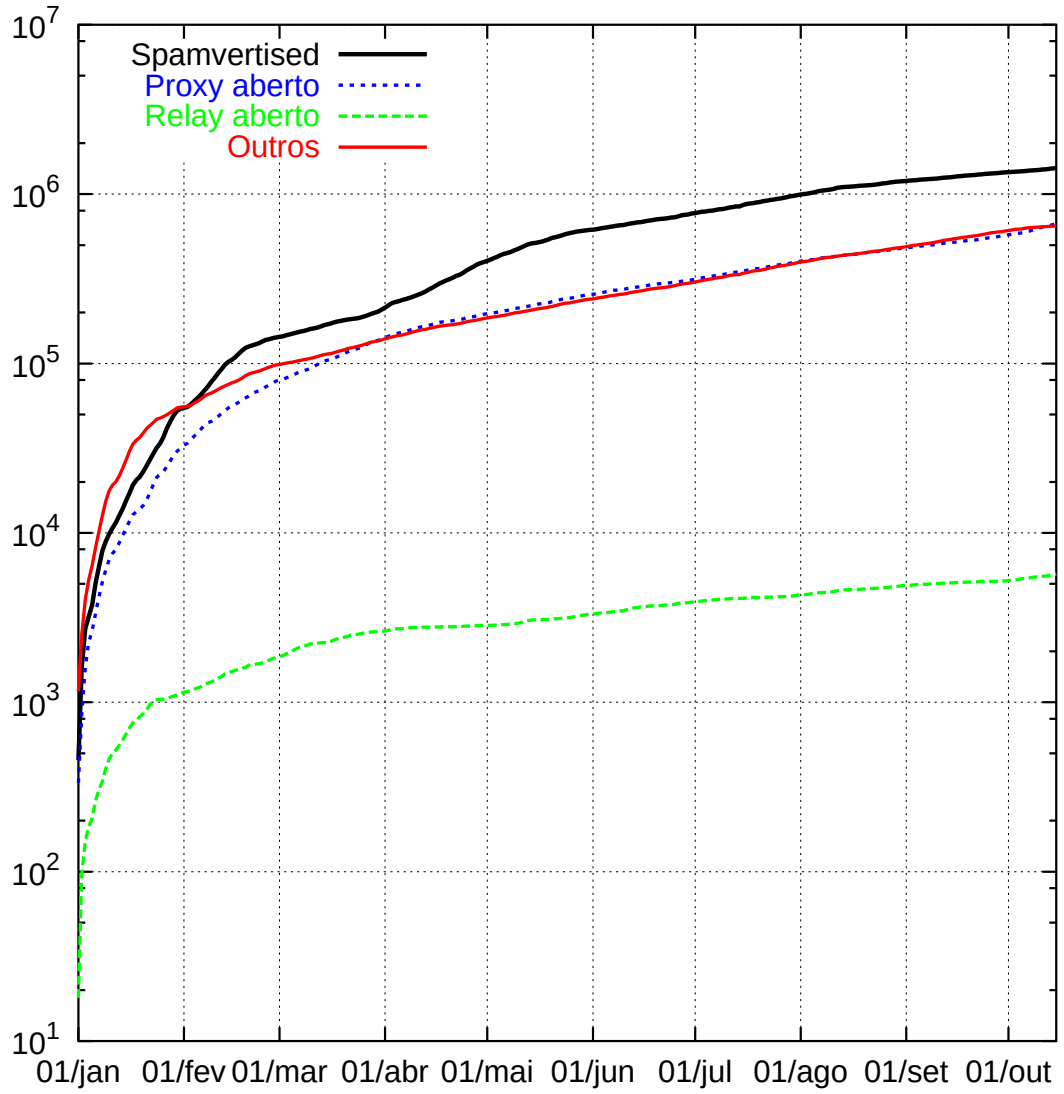
Período:	01/01 a 15/10/2003
Total de emails:	3.057.962
Enviados pelo SpamCop:	2.748.018

Categorias de Abuso

- Spamvertised Website
  - páginas com informações de produtos e serviços sendo oferecidos no spam
- Proxy Aberto
  - máquinas com serviço de *proxy* mal configurado, sendo abusadas
- Relay Aberto
  - máquinas com serviço de *email* mal configurado, sendo abusadas

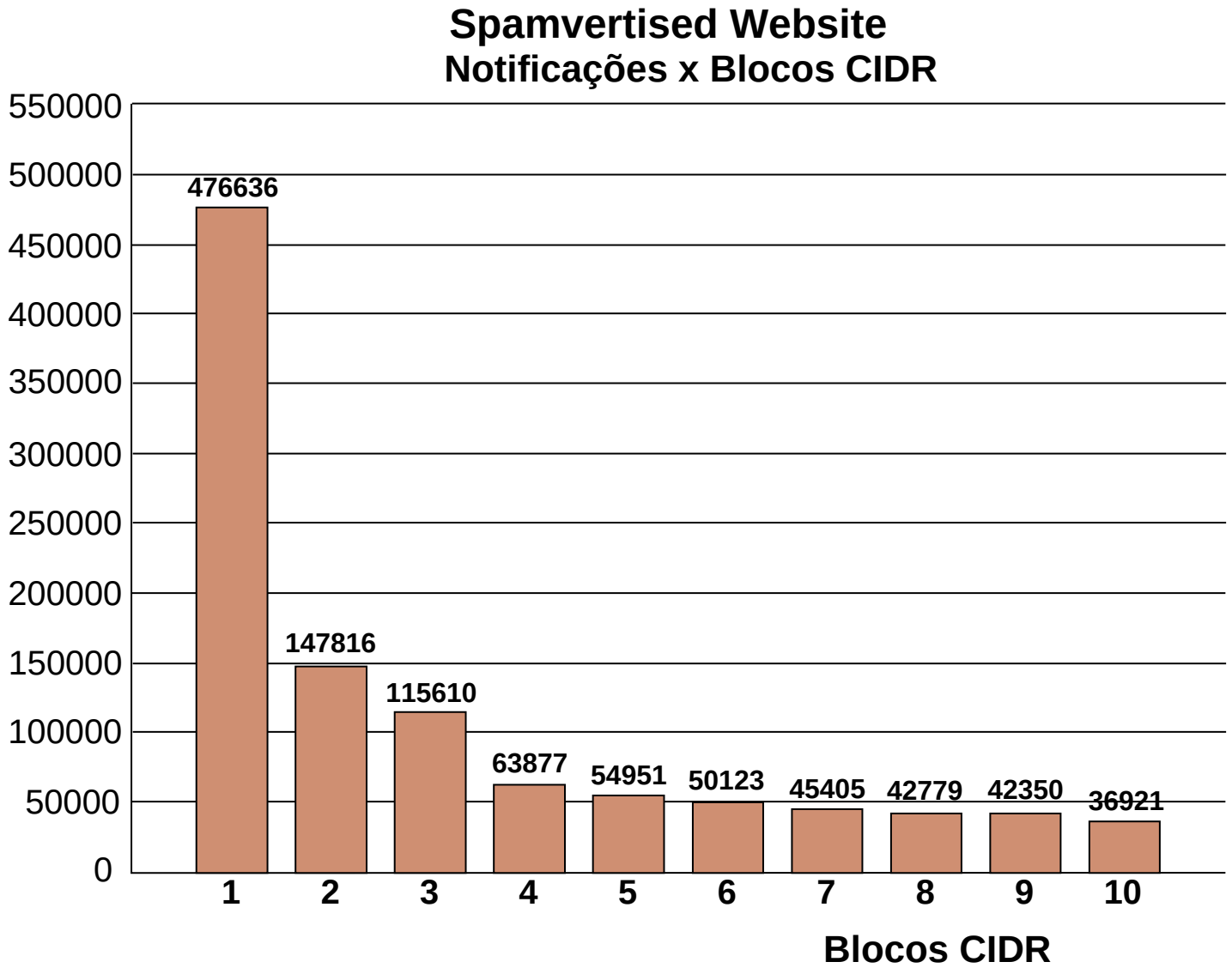
Estatísticas

Números Totais



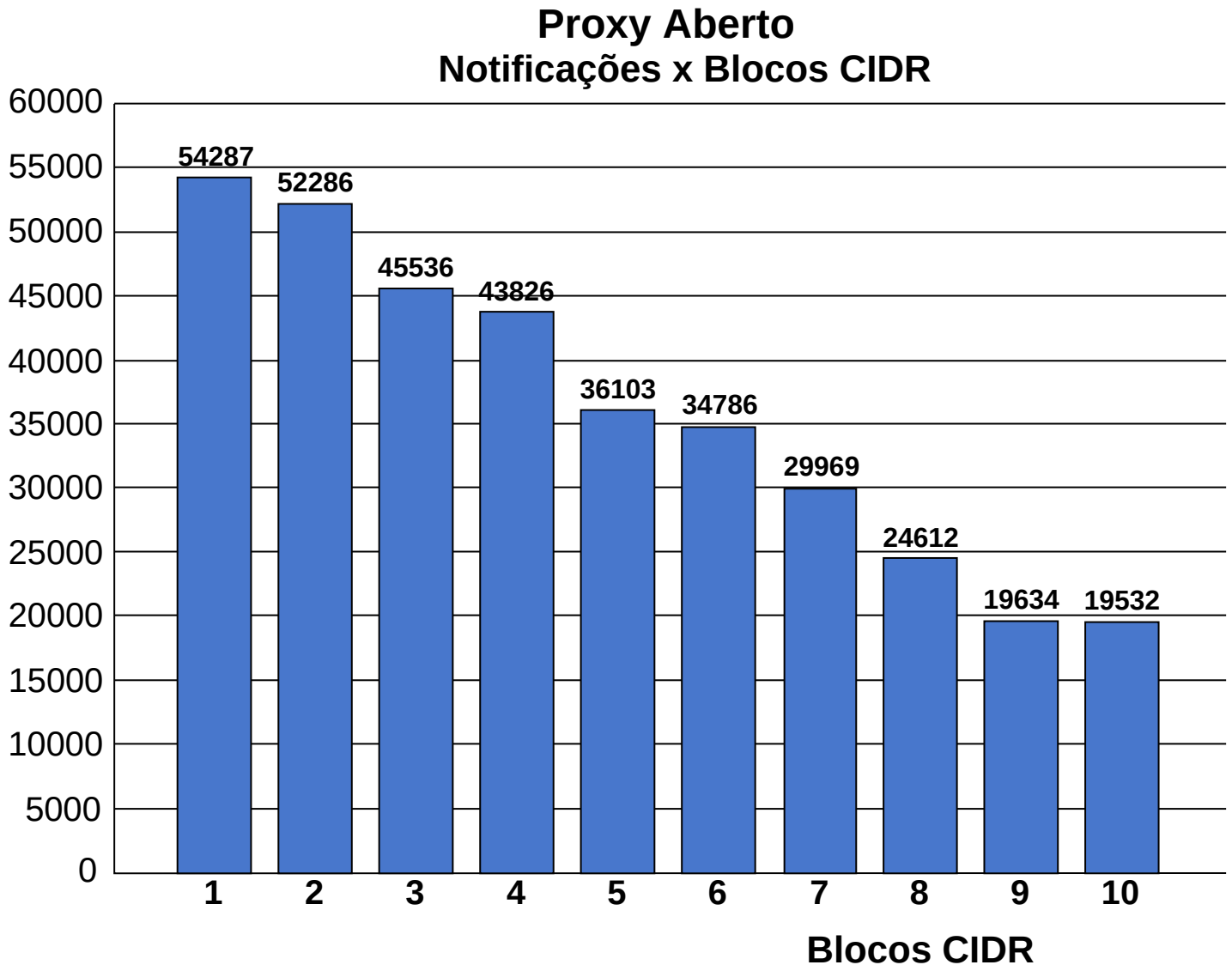
Totais Jan–Out 2003	
Spamvertised	**1.423.171**
Proxy aberto	**669.222**
Relay aberto	**5.707**
Outros	**649.918**
Total SpamCop	**2.748.018**
Total	**3.057.962**

Blocos CIDR



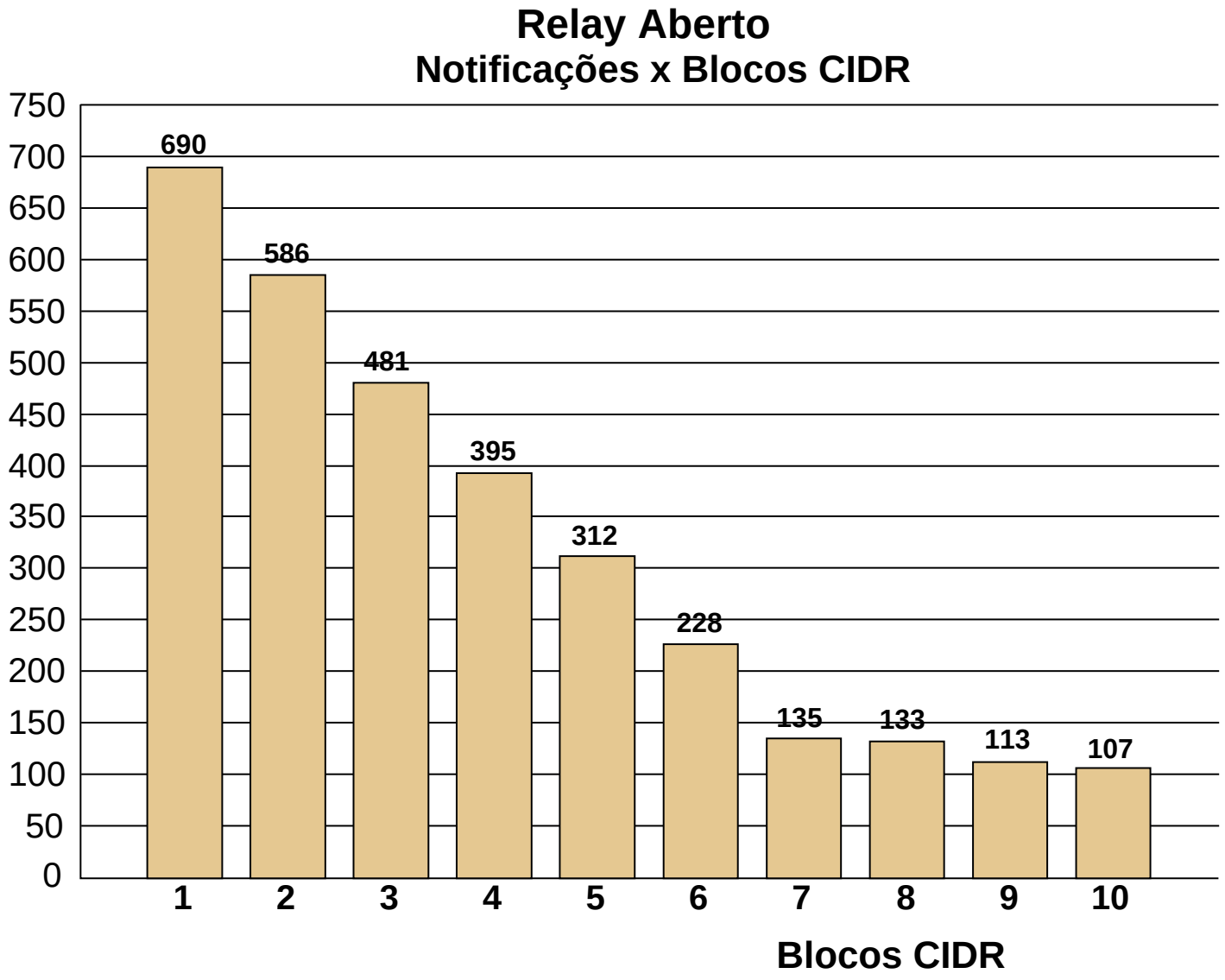
1	200.206.0.0/16
2	200.206.128.0/17
3	200.232.0.0/17
4	200.168.0.0/16
5	200.194.192.0/19
6	200.232.78.0/25
7	200.189.160.0/19
8	200.216.0.0/16
9	200.187.137.0/27
10	200.162.240.0/20

Blocos CIDR (cont.)



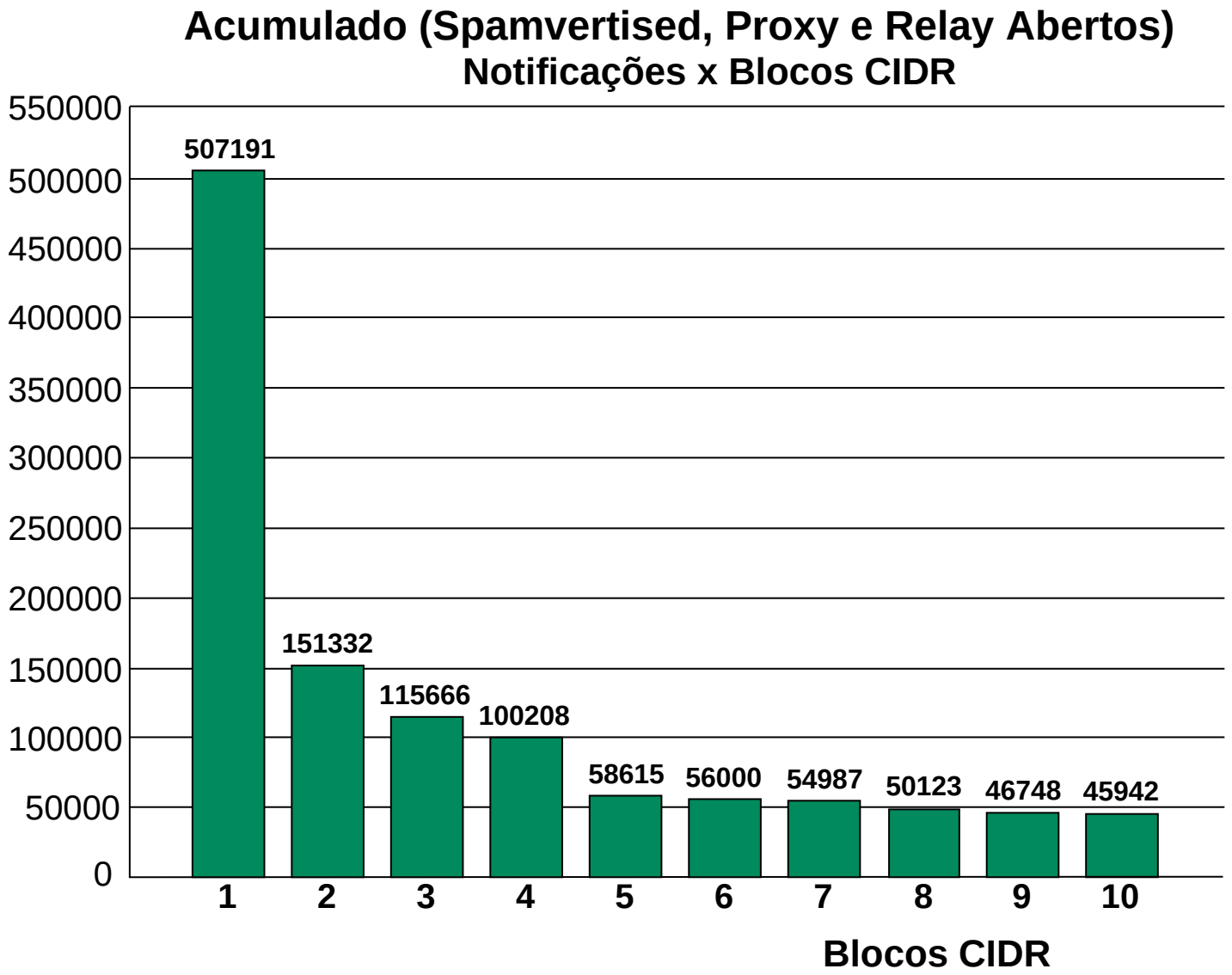
1	200.207.0.0/16
2	200.171.0.0/16
3	200.204.0.0/16
4	200.161.0.0/16
5	200.168.0.0/16
6	200.158.0.0/17
7	200.206.0.0/16
8	200.165.0.0/16
9	200.164.0.0/16
10	200.149.128.0/17

Blocos CIDR (cont.)



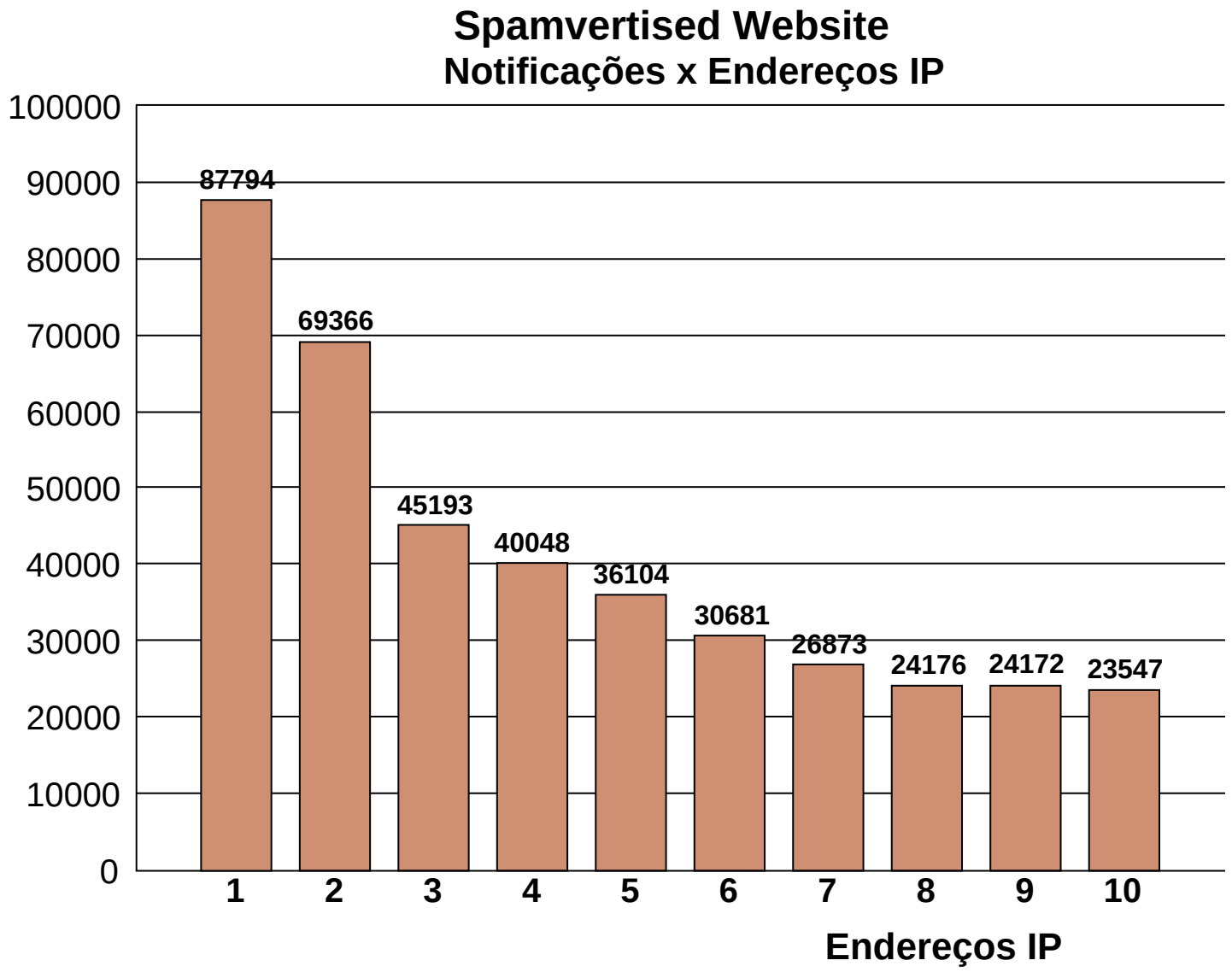
1	200.207.0.0/16
2	200.206.0.0/16
3	200.171.0.0/16
4	200.204.0.0/16
5	200.161.0.0/16
6	200.168.0.0/16
7	200.153.0.0/16
8	200.205.0.0/16
9	200.181.0.0/16
10	200.158.128.0/18

Blocos CIDR (cont.)



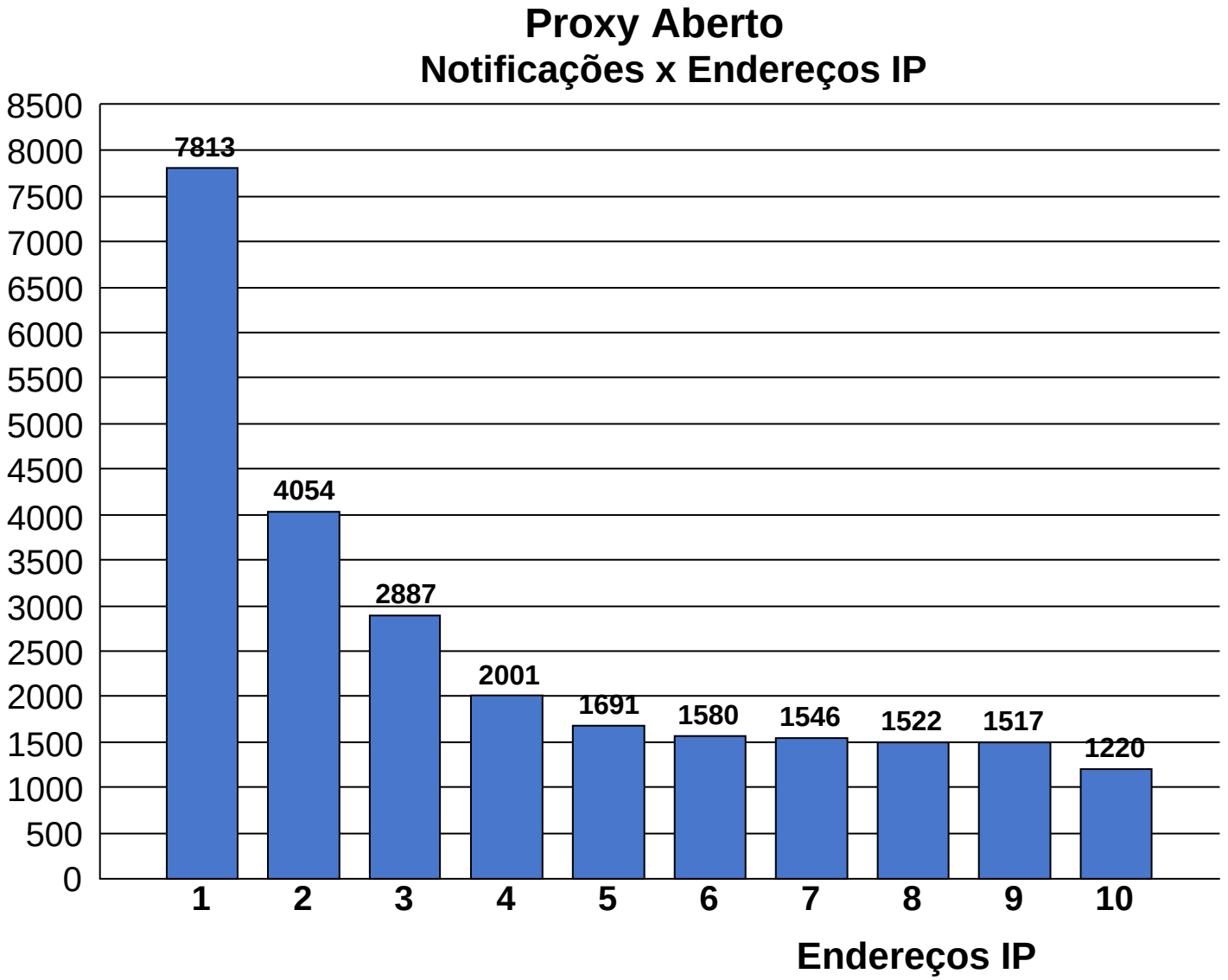
1	200.206.0.0/16
2	200.206.128.0/17
3	200.232.0.0/17
4	200.168.0.0/16
5	200.207.0.0/16
6	200.171.0.0/16
7	200.194.192.0/19
8	200.232.78.0/25
9	200.204.0.0/16
10	200.216.0.0/16

Endereços IP



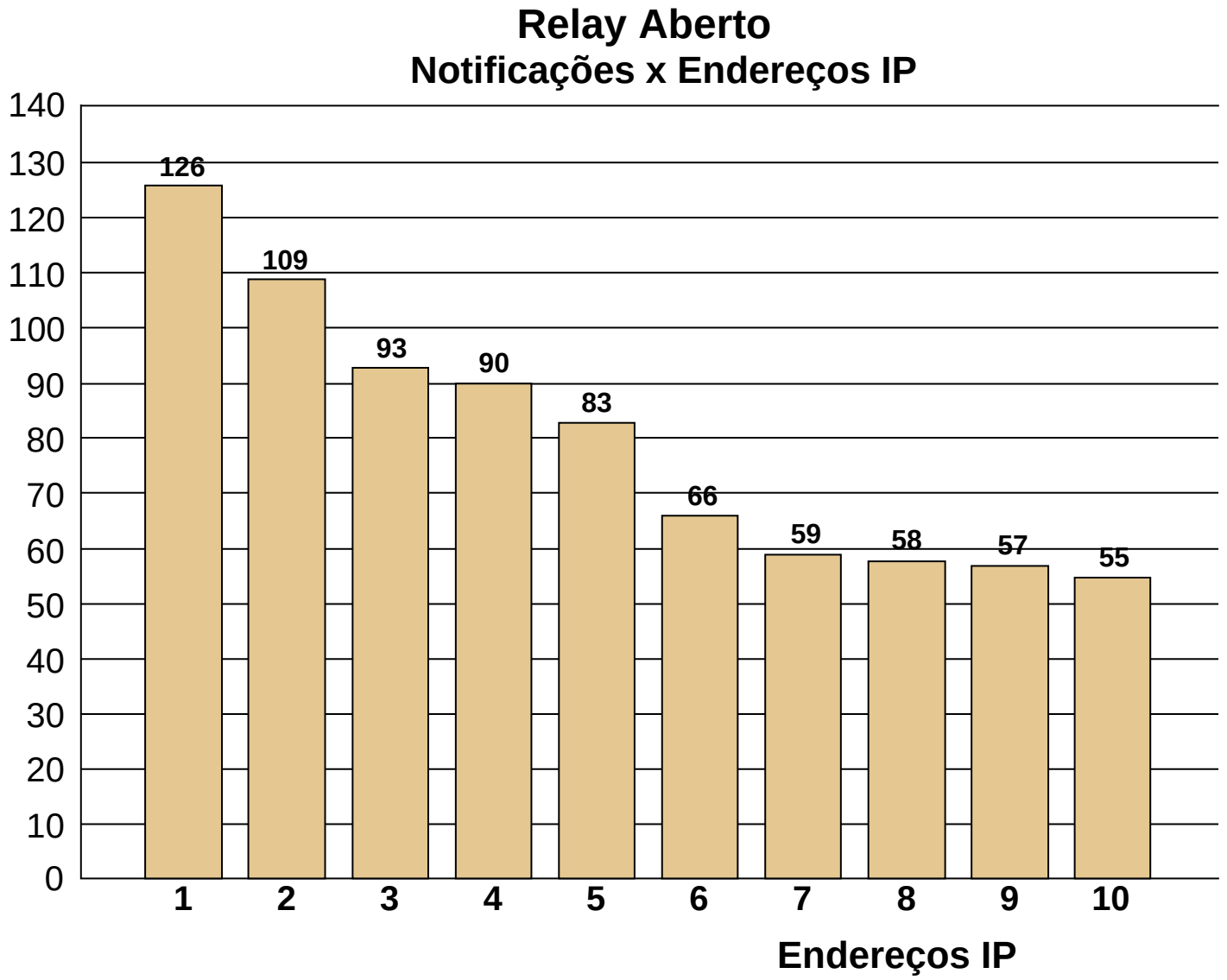
1	200.232.77.20
2	200.206.185.136
3	200.206.191.247
4	200.168.14.44
5	200.206.185.198
6	200.206.185.105
7	200.194.216.108
8	200.206.186.34
9	200.206.193.190
10	200.232.78.100

Endereços IP (cont.)



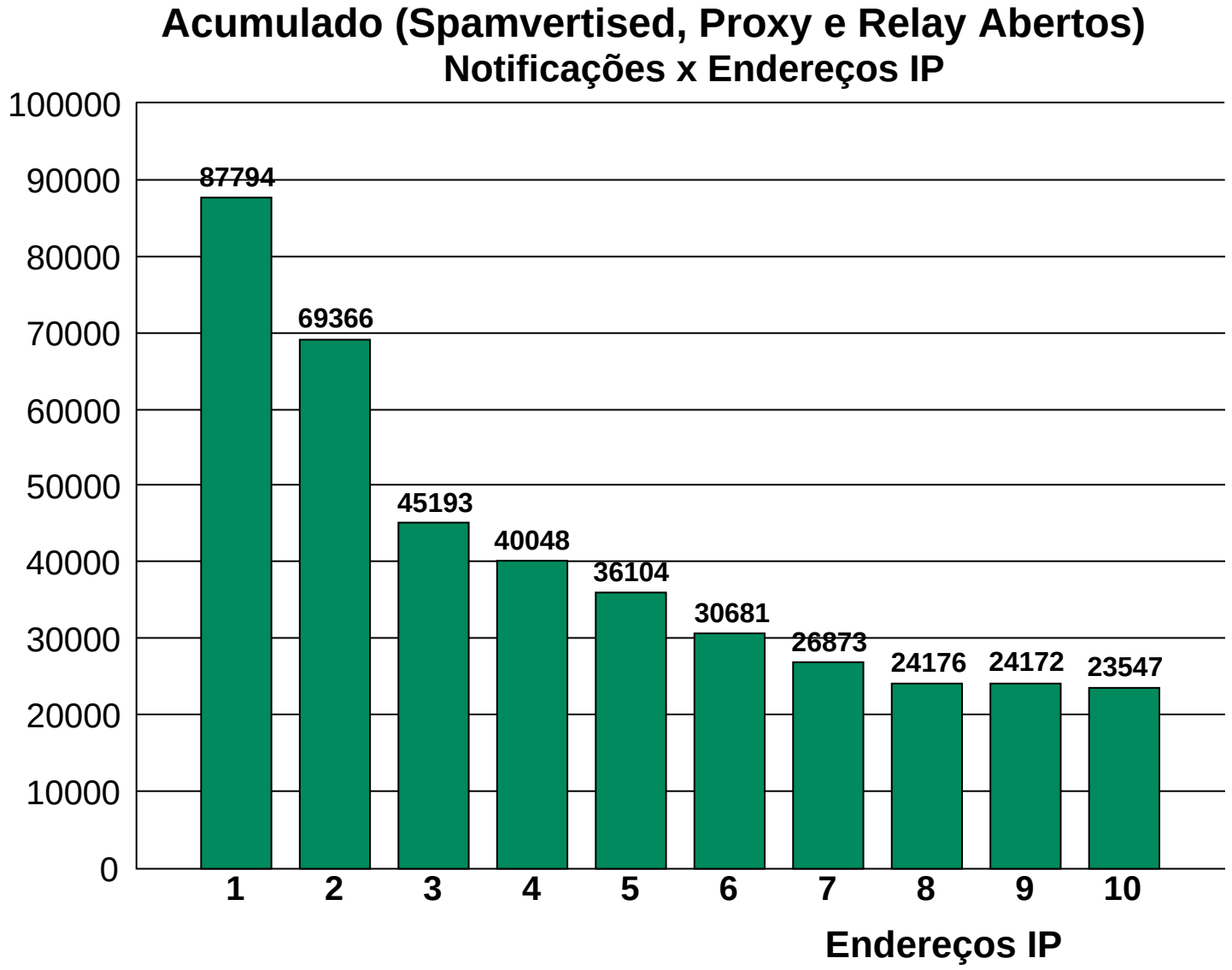
1	200.141.76.227
2	200.204.118.235
3	200.222.209.196
4	200.161.16.159
5	200.171.183.248
6	200.171.213.234
7	200.173.110.137
8	200.168.0.78
9	200.171.100.214
10	200.207.168.9

Endereços IP (cont.)



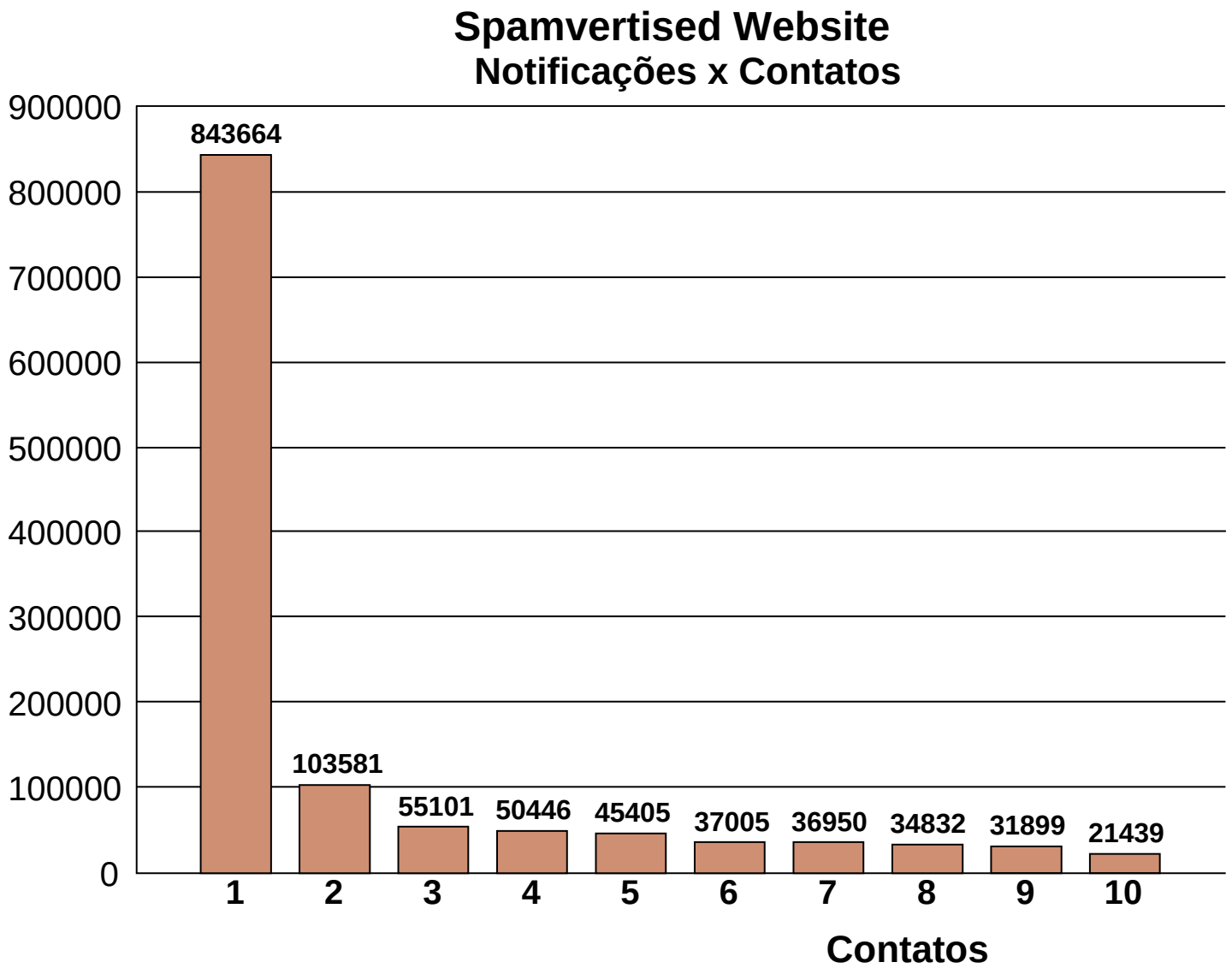
1	200.207.152.131
2	200.171.185.185
3	200.206.192.179
4	200.168.189.151
5	200.206.138.6
6	200.162.224.137
7	200.252.143.12
8	200.206.159.188
9	200.195.53.1
10	200.204.124.77

Endereços IP (cont.)



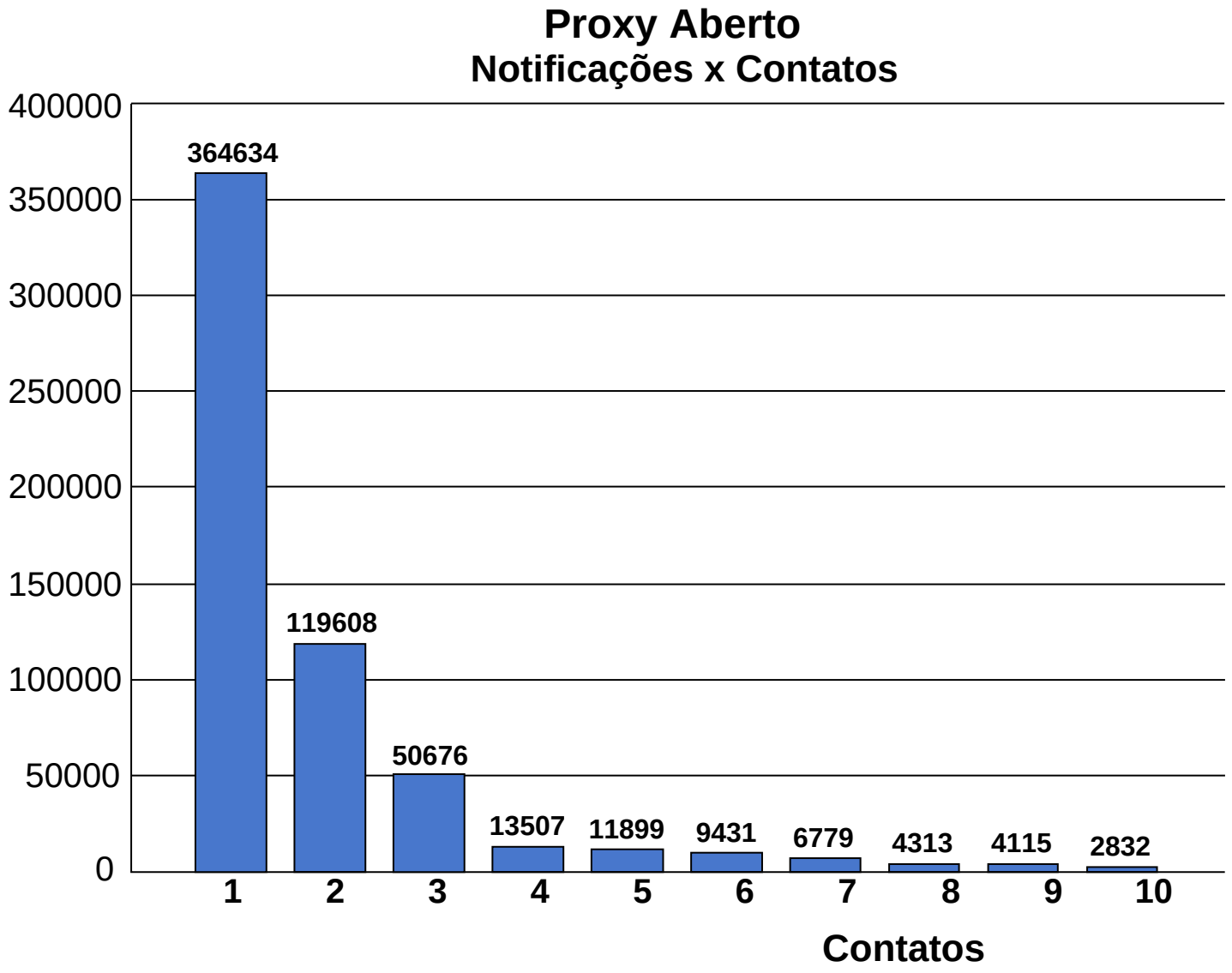
1	200.232.77.20
2	200.206.185.136
3	200.206.191.247
4	200.168.14.44
5	200.206.185.198
6	200.206.185.105
7	200.194.216.108
8	200.206.186.34
9	200.206.193.190
10	200.232.78.100

Contatos



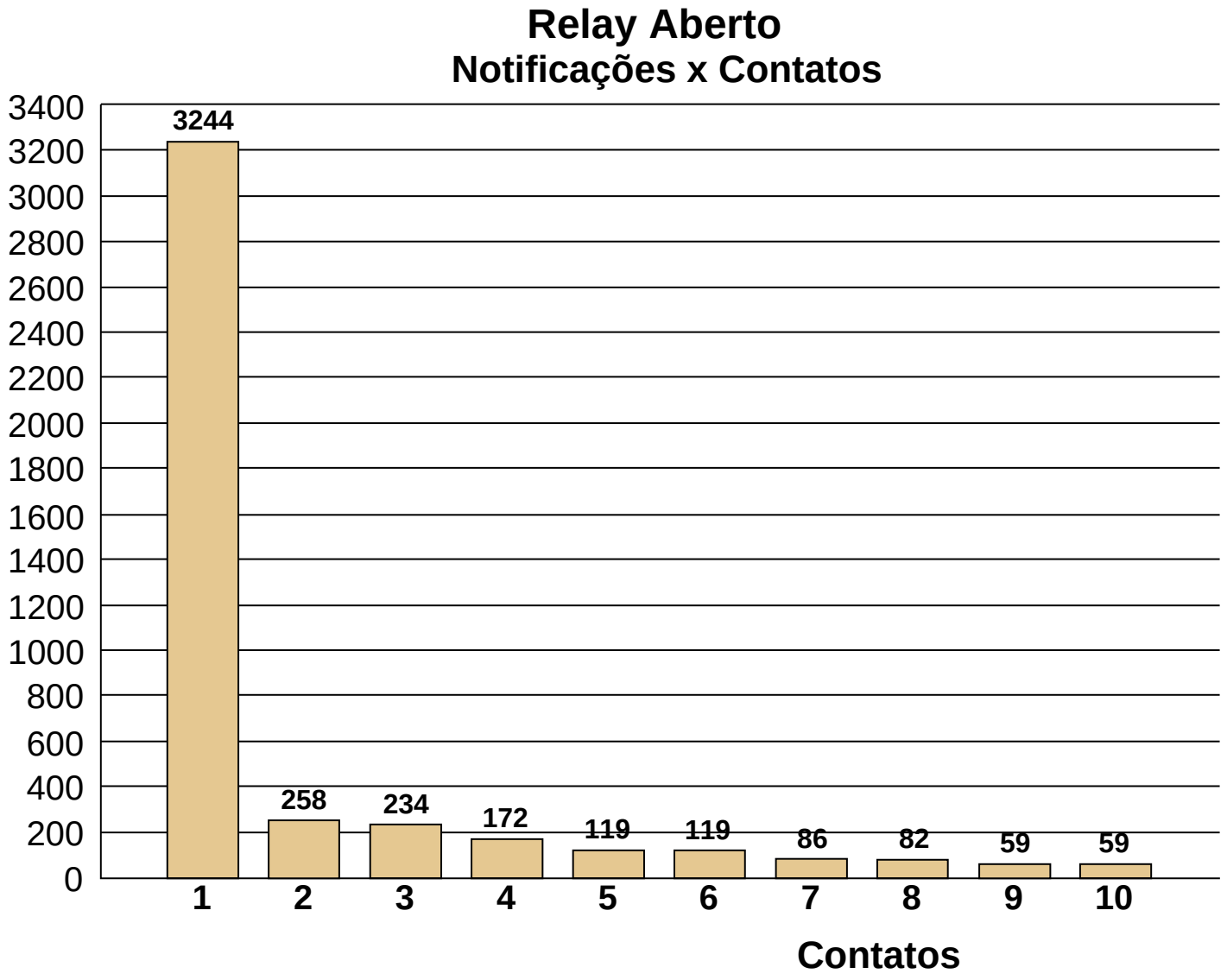
1	telefonica
2	telemar
3	impsat
4	tbline
5	diveo
6	ajato
7	embratel
8	comdominio
9	e-hosting
10	ctbctelecom

Contatos (cont.)



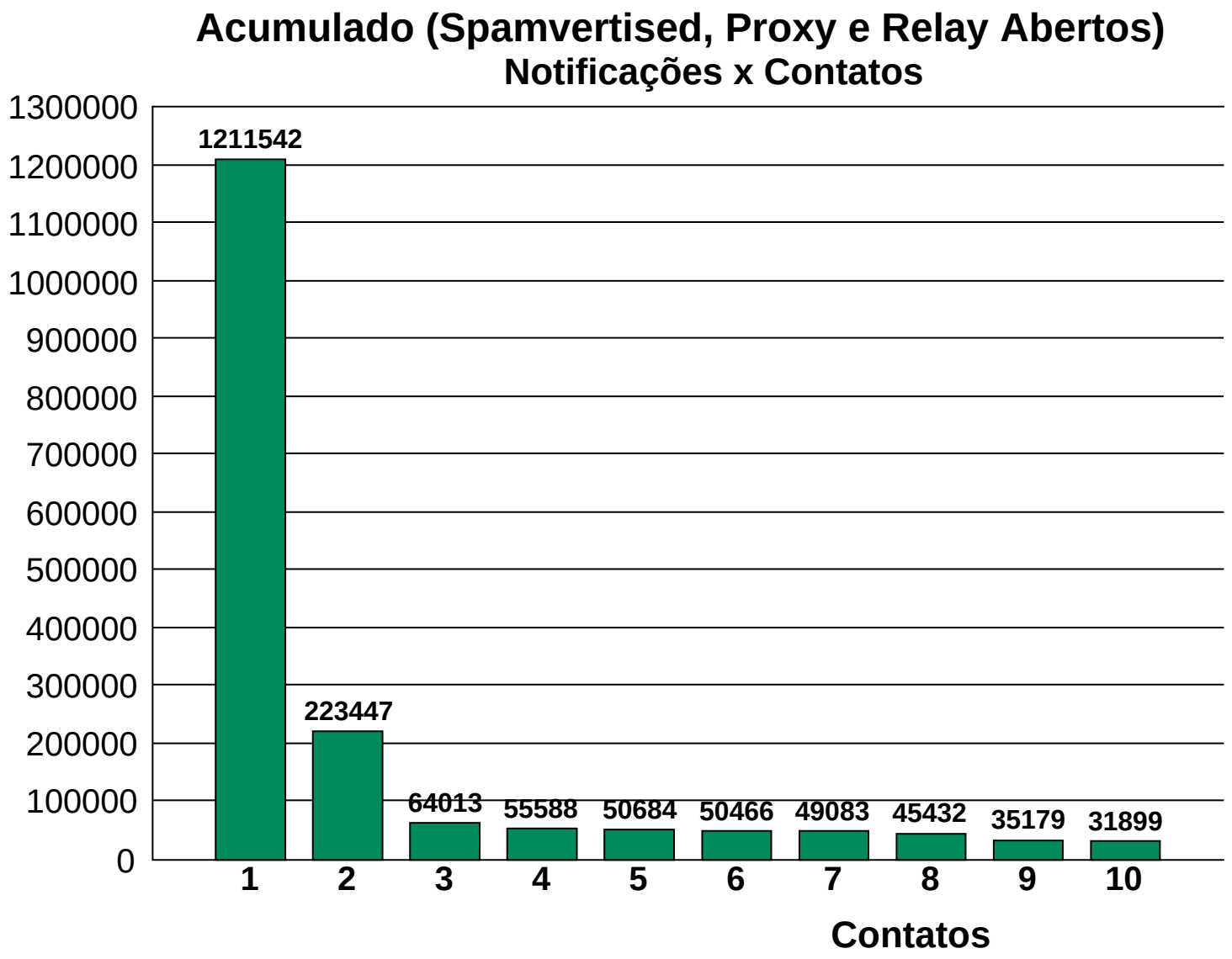
1	telefonica
2	telemar
3	brasiltelecom
4	ajato
5	embratel
6	telepar
7	terra
8	globocabo
9	horizoncable
10	linkexpress

Contatos (cont.)



1	telefonica
2	telemar
3	embratel
4	ajato
5	brasiltelecom
6	telepar
7	intelignet
8	copel
9	diveo
10	edificiovarig

Contatos (cont.)



1	telefonica
2	telemar
3	brasiltelecom
4	impsat
5	ajato
6	tbline
7	embratel
8	diveo
9	comdominio
10	e-hosting

Recomendações

- Reduzir proxies ou relays abertos
  - filtragem
  - educação dos usuários/administradores
- Possuir políticas de uso aceitável
- Prever em contrato abusos relacionados a spam
  - essencial para o caso de *spamvertised website*

Referências

- Material desta apresentação

  http://www.nbso.nic.br/docs/ssi2003/

- SpamCop

  http://spamcop.net/

- Documentação sobre Segurança e Administração de Redes

  http://www.nbso.nic.br/docs/seg-adm-redes/

- Documentos, RFCs e sites relacionados

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