Projeto e Desenvolvimento de um Sistema de Controle e Acompanhamento de Notificações de Spam

Cristine Hoepers
cristine@nic.br

Klaus Steding-Jessen
jessen@nic.br

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

NIC BR Security Office – NBSO
Comitê Gestor da Internet no Brasil

Roteiro

- Motivação
- Objetivos do Sistema
- Arquitetura
- Implementação
- Resultados
- Conclusões

Motivação

- grupos de resposta a incidentes recebem um grande volume de reclamações
  - é preciso triagem
  - reclamações de spam contém informações sobre problemas de configuração e abusos
- o NBSO recebe cerca de 8.500 emails/dia de reclamações de spam
- cerca de 90% são enviados pelo SpamCop

Objetivos do Sistema

- processar reclamações de spam provenientes do SpamCop
- agrupar por responsáveis pelas redes e tipo de abuso
- gerar notificações para os responsáveis pelas redes
- gerar estatísticas sobre:
  - tipo de abuso notificado
  - redes sendo abusadas

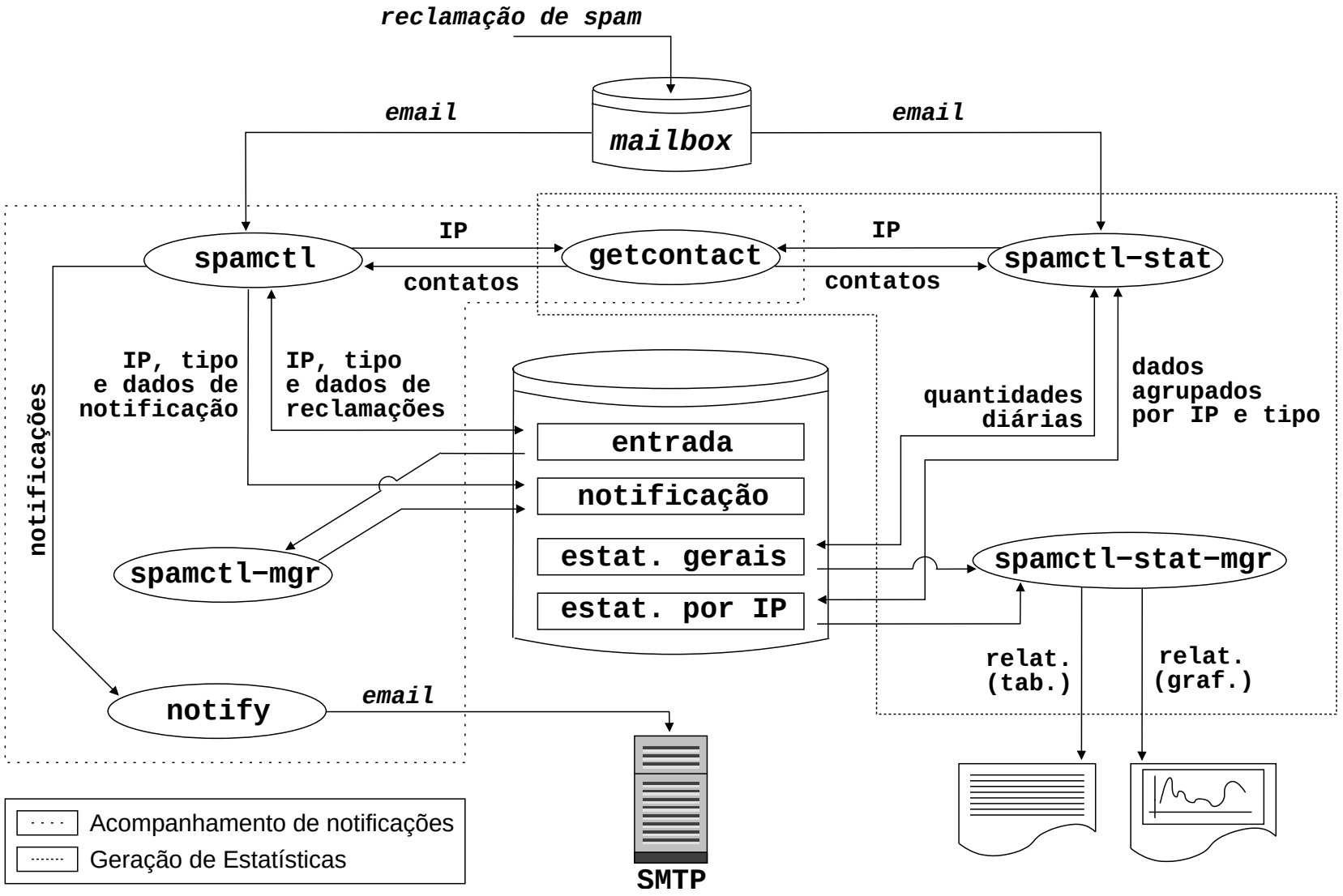
Reclamações Processadas

- 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

Arquitetura

- Acompanhamento de Notificações
  - agrupa dados de reclamações e envia mensagens de notificação para os responsáveis pelas redes envolvidas
- Geração de Estatísticas
  - contabiliza e armazena informações utilizadas na geração de estatísticas sobre as reclamações de spam

Arquitetura (cont)



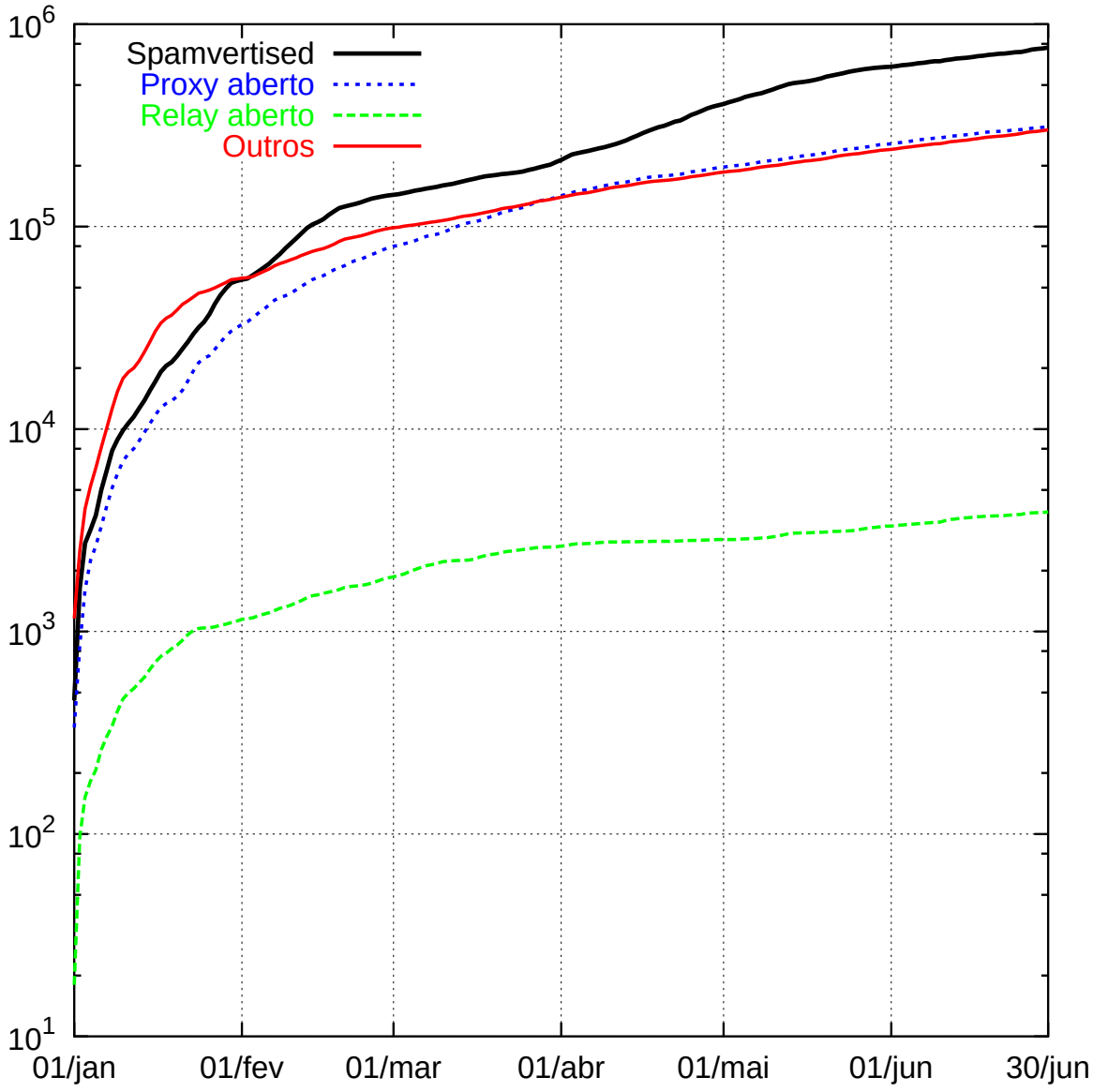
Implementação

- escrito em Perl
- utilização de *hashes* em memória e disco
- preocupações com programação segura
  - manipula dados potencialmente não confiáveis
  - *taint mode*
  - auditoria de código via RATS

Resultados

Mês	*Spamv.*	*Proxy*	*Relay*	Outros
jan	53.843	31.670	1.127	55.165
fev	88.732	47.058	712	42.822
mar	65.511	60.837	779	40.021
abr	189.851	56.050	225	46.448
mai	216.824	59.981	471	55.138
jun	152.521	56.197	583	60.991
Total	767.282	311.793	3.897	300.585

Resultados (cont)



Conclusões

- Automatização permite tratar um volume muito grande de *emails*
- As estatísticas mostram as redes com maiores problemas
- Espera-se que estas redes utilizem esses dados para direcionar esforços

Referências

- SpamCop

  http://spamcop.net/

- Estatísticas geradas pela ferramenta

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