Estratégias de controle de envio de e−mail para ISPs

Danton Nunes (danton@inexo.com.br)
InterNexo Ltda., São José dos Campos, SP

março de 2003

Apresentado à 15ª reunião do GTER, São Paulo, SP

O Problema

O envio massivo de mensagens não solicitadas e impertinentes (SPAM) virou uma praga que pode comprometer seriamente todo o serviço de correio eletrônico.

Apesar de extremamente ineficiente do ponto de vista de retorno, o SPAM é tão barato que acaba sendo compensador para quem o envia.

O SPAM é antipático e quem o envia procura se esconder de várias formas, com endereços forjados, usando retransmissores (relays) abertos, etc.

Os ISPs comerciais não tem ou mal praticam políticas de inibição dessa prática predatória.

A mala direta convencional (em papel, pelo correio), tem o custo bancado por quem a envia. Porisso ela precisa ser bem dirigida.

O SPAM tem a maior parcela de seu custo bancado pelos destinatários e pelos provedores de serviços (que em última análise recai nos usuários). Porisso o envio indiscriminado é economicamente viável.

Atualmente as estratégias de combate ao SPAM se baseiam em filtragem pelo endereço de origem (listas negras) ou conteúdo (p.ex. as abordagens Bayesianas). De qualquer forma:

- **o ônus da filtragem cai no destinatário;**
- **não é possível evitar falsos positivos;**
- **os spammers vão se adaptando aos filtros, a guerra se torna permanente, como no caso dos vírus.**

Este trabalho tece estratégias para mudar o foco do combate ao SPAM do destinatário para o provedor de serviços que hospeda o possível spammer.

As estratégias estudadas vão nas linhas:

1. **Tarifação do correio eletrônico, instituindo o equivalente a um selo postal;**

2. **Limitação da quantidade de mensagens enviadas;**

3. **Bloqueio ao uso de retransmissores abertos.**

Evidentemente procuramos causar pouco ou nenhum impacto nos usuários lícitos de correio eletrônico, inclusive marketing direto não indiscriminado (opt−in, com gerenciadores de listas).

Tarifação do correio eletrônico

Antes da introdução do selo postal no século XIX, o custo do cor−reio convencional era bancado pelo destinatário. O selo provocou uma revolução que viabilizou o serviço postal moderno.

O correio eletrônico vive ainda no período pré−Vitoriano porém sem as limitações técnicas de então. Imagine se você tivesse que pagar pela propaganda que recebe pelo correio! pois é isso que acontece com o SPAM.

A solução é atacar o SPAM em seu ponto fundamental, o custo.

O ISP passa a cobrar por mensagem enviada, mais propriamente por RCPT. Pode haver uma franquia de modo que quem enviar menos mensagens do que o número franquiado não paga.

Tarifação do correio eletrônico

O problema é como implementar a bilhetagem dos RCPTs. Seria fácil se toda a mensagem que saísse da rede do ISP passasse por um servidor centralizado, pois nesse caso a análise do log seria suficiente.

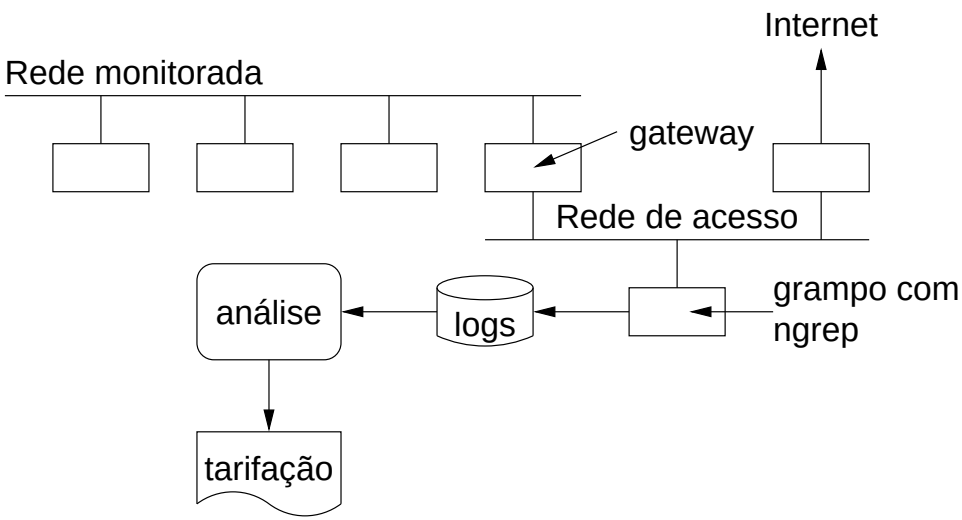
No entanto, os usuários são geralmente livres para enviar mensagens diretamente de suas estações de trabalho ou servidores corporativos.

A solução é monitorar o tráfego que saia para qualquer lugar na Internet pela porta 25/TCP.

O correio eletrônico sobre SSL (porta 465/TCP) não é muito significativo em termos de tráfego e não é possível acessar seus estados. Ainda assim poderia ser cobrada uma taxa por sessão, mas não por RCPT ou por mensagem.

Tarifação do correio eletrônico

Esquema do Experimento



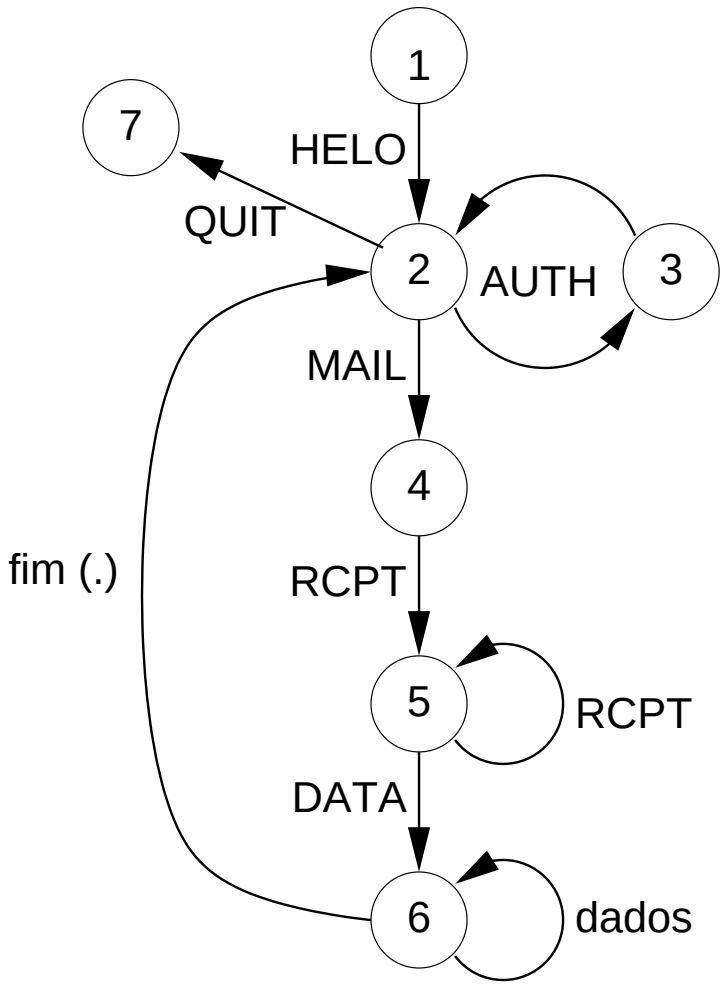
Um grampo transparente foi instalado à jusante do gateway

O grampo usa o programa ngrep, sobre o tráfego para porta 25 de endereços externos.

As linhas relevantes são capturadas em um log.

O log é processado por uma máquina de estados para identificar o número de destinatários, produzindo um relatório que associa IP de origem, destinatário e horário.

Tarifação do correio eletrônico




```
220 quasar.inexo.com.br ESMTP
ehlo cara-palida
250-quasar.inexo.com.br
250-AUTH=LOGIN
250-PIPELINING
250 8BITMIME
auth login
334 VXNlcm5hbWU6
ZGFudG9uI3BvbGktbmF2YWwtNzYuZW5nLmJy
334 UGFzc3dvcmQ6
bGh1ZmFz
235 go ahead
mail from: <danton@inexo.com.br>
250 ok
rcpt to: <danton@poli-naval-76.eng.br>
250 ok
rcpt to: <danton@telar.com.br>
250 ok
data
354 go ahead
Subject: exemplo para o GTER

esta linha não deve ser contada:
rcpt to: <danton@telar.com.br>
.
250 ok 1047417618 qp 8166
quit
221 quasar.inexo.com.br
```

Tarifação do correio eletrônico

Conclusões

É relativamete fácil estabelecer pontos de controle na rede onde o tráfego de correio eletrônico pode ser monitorado e posteriormente bilhetado.

O processo de monitoramento é totalmente passivo e não interfere com o funcionamento normal do correio eletrônico.

Todas as mensagens saintes são monitoradas, qualquer que tenha sido o cliente usado.

Para completar a bilhetagem é necessário associar endereço e horário com o usuário, mas supostamente é para isso que serve a autenticação!

Tarifação do correio eletrônico

Problemas e Questões Abertas

Escalabilidade: quais são os requisitos de um sistema como este para redes de alto tráfego?

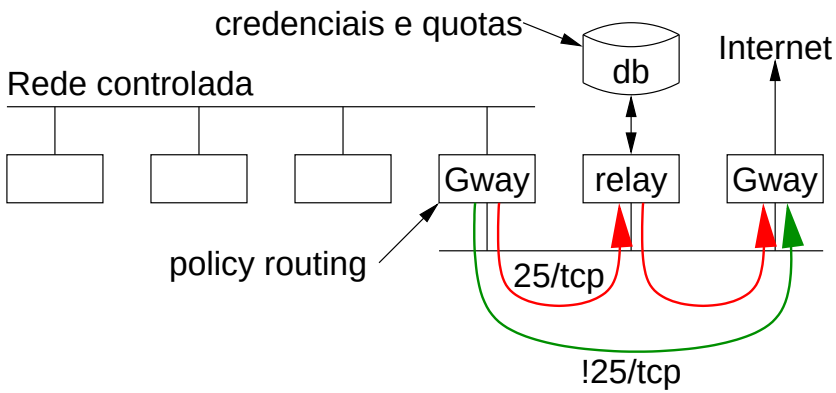
Distributividade: em redes complexas seria viável ter a tarifação distribuida em vários pontos de controle? Em redes estruturadas como árvores certamente isso não é problema.

Este esquema dificilmente funcionaria em provedores gratuitos.

Não previne abusos de retransmissores abertos na própria rede monitorada. Provavelmente nenhum método passivo previna.

Limitando a Quantidade de Mensagens

Esta estratégia se baseia em forçar o tráfego de correio através de um retransmissor semi−aberto.



O roteador que liga a rede controlada à internet é programado para desviar o tráfego 25/TCP para um retransmissor.

No retransmissor é possível:

IMPORTANTE!

− exigir autenticação do usuário;

− contabilizar as mensagens e destinatários;

− limitar o número de mensagens, recusando as que excederem à quota.

Solução adaptada aos provedores gratuitos.

Limitando a Quantidade de Mensagens

Pontos positivos

A quantidade de mensagens ou destinatários pode ser limitada, independente de tarifação (ideal para provedores gratuitos).

Requerer autenticação no retransmissor tem duas virtudes:
− identifica de forma inequívoca quem está transmitindo e
− resolve o problema de associar endereço IP ao usuário (isto é, tudo se resolve na camada de aplicação).

O uso de retransmissores abertos dentro da rede controlada é evitado. As mensagens retransmitidas não passarão pelo retransmissor por causa da autenticação. Mesmo que passem, o estrago será limitado pela quota.

Limitando a Quantidade de Mensagens

Pontos negativos

Requer mais recursos que o monitoramento passivo (mas nada estratosférico pois cache de Web é feito de forma semelhante e é bem viável).

O MTA do retransmissor tem que ser configurado com muito cuidado para não se tornar ele mesmo um retransmissor aberto (quem conhece sendmail.cf sabe com quantos paus se faz uma canoa).

Não estão claras as interações deste esquema com clientes e outros MTAs. Nossos testes se limitaram a: elm, pine, sendmail, qmail e telnet 25.

Bloqueio ao Uso de Retransmissores Abertos

Um efeito colateral do esquema proposto para limitação do número de mensagens enviadas é o bloqueio de retransmissores abertos.

A mensagem que seria enviada por um retransmissor aberto na Internet é interceptada e enviada para nosso retransmissor controlado.

Este determina o servidor de destino pelo DNS (processo normal do MTA), enviando a mensagem diretamente para o destinatário, isto se ela passar pelo mata−burro da autenticação.

Conclusão: o esquema proposto inviabiliza o uso de retransmis−sores abertos mesmo que não se exija autenticação.

Comparação entre as estratégias

Critério	Monitoração Passiva	Retransmissor Forçado
Contabiliza as mensagens?	SIM	SIM
Exige autenticação?	NÃO	SIM
Impede o uso de ´open relay´ externo?	NÃO	SIM
Impede o uso de ´open relay´ interno?	NÃO	SIM
Facilidade de instalação e configuração?	ALTA	BAIXA
Presta-se a provedor gratuito?	NÃO	SIM

Conclusão: com a tecnologia corrente e um pouco de boa vontade os ISPs podem tarifar e controlar o envio de correio eletrônico de modo a tornar o SPAM pouco atraente sem prejudicar os remetentes lícitos.

É possível matar o dragão no ninho!