Anti-SPAM ASK - Válidando remetentes por confirmação de mensagens

Autor: Patrick Brandao <contato at patrick.eti.br>
Data: 07/07/2006

Introdução

Por Patrick Brandão
http://www.patrick.eti.br
contato@patrick.eti.br

Aviso

É segunda-feira, você chega no serviço, abre o cliente e e-mail, e de repente, chove mensagem: "Viagra", "Trabalhe em casa", "Você está sendo traído", "Livre-se das multas", etc...

Depois de implementar o *SpamAssassin*, a redução é drástica, mas não total, infelizmente você corre o risco de ter uma mensagem legítima excluída e o risco aumenta a medida que você abaixa o nível, tornando o SpamAssassin mais agressivo. Programá-lo para apenas marcar as mensagens como SPAM ajuda, mas você de qualquer maneira, vai perder tempo separando algo do lixo.

Então, qual a solução?

Os spammers, pessoas desprezíveis, usam sistemas de envio de mensagens em massa, a maioria, um simples arquivo de texto com uma lista de endereços e um script que passa linha por linha enviando uma cópia do SPAM para cada um. Os mais modernos, tem sistemas com dicionários e funções de detecção de endereço de e-mail válido, sugando páginas de sites de busca, verdadeiros ROBÔS. Os mais sofisticados usam softwares que balanceiam o SPAM entre servidores de relay aberto, de forma que nem bloqueando por IP resolverá.

O detalhe interessante é que quando os SPAM´s são enviados usando remetentes inexistentes, o e-mail tende a voltar para o remetente (inventado pelo maligno), que não usa uma caixa postal válida. O resultado disso é uma fila enorme de mensagens em busca de um fim. Um dos servidores de e-mail que gerencio, certa vez chegou a ter 136 mil mensagens no queue, sendo que havia apenas 900 caixas válidas.

Bloquear o endereço do remetente é perca de tempo. Por que?
Os spammers criam strings aleatórias para o usuário no campo "From:" do SPAM e um domínio válido, e usam servidores open-relay aleatórios também, por exemplo:

From: xyz@yahoo.com.br
To: vitima@dominio.com
Subject: compre viagra, baratinho!

Assim, você bloqueia o xyz@yahoo.com.br, para que os SPAM´s sejam bloqueados, mas o próximo SPAM logo atrás dele terá o cabeçalho:

From: abc123@yahoo.com.br

To: vitima@dominio.com
Subject: compre viagra, baratinho!

Então vamos pelo assunto!
Bloqueia tudo que tiver "viagra" no assunto, e o próximo e-mail será:

From: xyz@yahoo.com.br
To: vitima@dominio.com
Subject: compre V 1 4 G R 4!

Se você bloquear o domínio yahoo.com.br, vai ter problemas de verdade, pois e-mails legítimos serão afetados.

Conclusão do texto acima: spammers não recebem retornos por e-mail, apenas usuários legítimos, os sacanas não querem um reply de seu lixo, apenas que você leia o conteúdo ou visite o link indicado. Eles são malignos, conhecem bem os anti-spam's existentes e vivem criando e-mails capazes de burlar a avaliação dos mesmos.

Nesse artigo você vai aprender como implementar, personalizar e dar suporte a um servidor de e-mail com o *anti-SPAM ASK*, cujo funcionamento é igual e superior ao anti-SPAM UOL!

O objetivo é ter na caixa de entrada, apenas endereços de e-mail de pessoas legítimas, que pretendem receber retorno das mensagens enviadas.

Algoritmo e fluxograma

Como funciona?

A mensagem parte do remetente em direção ao seu servidor de e-mail, dentro dele, a mensagem é analisada pelo MTA e entregue ao MDA (agente de entrega). É aqui que o *ASK* trabalha, no MDA, ou seja, no momento em que a mensagem está pronta para ser escrita na caixa do usuário ela entra no fluxograma do anti-SPAM.

O fluxo da mensagem é complexo, mas basicamente:

- Se é uma mensagem que retornou de um tira-teima, um código md5 é verificado para liberar a mensagem original e ela é movida para a caixa de entrada.
- Caso contrário, o remetente é verificado na lista branca (whitelist) e na lista de remetentes bloqueados (ignorelist). Se estiver permitido, a entrega é feita, se estiver bloqueado, já era. Caso contrário:
- É verificado se a palavra (ou frase) secreta se encontra na mensagem. Caso positivo, a mensagem é entregue. Caso contrário:
- A mensagem é salva em uma fila local, o tira teima é criado com um código md5 de validação e enviado para o remetente.

Fluxograma detalhado:

Servidor de e-mail

Como minha praia é *qmail*, usaremos ele para implementar o *ASK*. Esse capítulo é resumido e não é o foco do artigo.

Perguntas e dúvidas sobre o qmail devem ser evitadas para não fugir do tema aqui - ASK.

Se você leu o capítulo 2, viu que o ASK trabalha no MDA, então usaremos o genérico: *vpopmail*.

MTA - qmail
MDA e gerente de contas - vpopmail

Na instalação do qmail e vpopmail, você encontrará tudo que precisa nos links abaixo:

Scripts:

- http://www.patrick.eti.br/software/scripts/lifewithqmail.sh
- http://www.patrick.eti.br/software/qmail/vpopmail-install

Sites:

- http://www.lifewithqmail.org
- http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=1468
- http://www.qmailrocks.com

Vou considerar que:

- qmail instalado em /var/qmail, como um domínio;
- vpopmail instalado em /home/vpopmail domínio virtual adicionado: intranet.br.

Se você já tem um servidor, próximo capítulo...

Download e instalação

Procedimentos:

* Verifique se você tem o pacote python instalado, o *ASK* invoca o interpretador de comandos a partir de /usr/bin/python.

1. baixe o ASK:

- http://prdownloads.sourceforge.net/a-s-k/ask-2.5.2.tar.gz?download

2. Instalação:

 # tar -xvzf ask-2.5.2.tar.gz
 # mv ask-2.5.2 /usr/share/ask
 # chown root.root /usr/share/ask -R
 # chmod +rx /usr/share/ask
 # chmod +r /usr/share/ask -R

Isto basta. Próximo passo, ativar ASK em uma conta.

5. Ativando ASK em uma conta:

Primeiramente, criemos uma conta:

 # /home/vpopmail/bin/vadduser contato@intranet.br senhasecreta

Vá até a pasta do domínio intranet.br, caso não saiba onde é, digite:

 # /home/vpopmail/bin/vdominfo intranet.br -d

Como vamos trabalhar com o usuário "contato" do domínio "intranet.br", na pasta do domínio crie o arquivo:

.qmail-contato

Esse arquivo receberá as mensagens do qmail, que serão processadas pelos comandos contidos nesse arquivo. Para que a mensagem seja simplesmente entregue, o seguinte conteúdo basta:

| /home/vpopmail/bin/vdelivermail " bounce-no-mailbox

Porém, para usar o ASK, é necessário:

| preline /usr/share/ask/askfilter --loglevel=5 --logfile=/var/log/ask/contato_intranet.br.log
--home=/home/vpopmail/domains/intranet.br/contato

O usuário vpopmail DEVE conseguir ler este arquivo, portanto:

 # chown vpopmail.vchkpw /home/vpopmail/domains/intranet.br/.qmail-contato

Vamos estudar os parâmetros:

- --loglevel: define o nível de sensibilidade do log, de 1 a 10;
- --logfile: arquivo onde os eventos serão registrados, é necessário que o usuário que executa a entrega (normalmente, vpopmail uid 89) tenha permissão de escrita;
- --home: diretório do usuário, para descobrir, digite:

  # /home/vpopmail/bin/vuserinfo contato@intranet.br -d

Ainda não está pronto, é necessário criar o arquivo de configuração e as subpastas do ASK trabalhar.

Dentro do diretório do usuário contato@intranet.br (/home/vpopmail/domains/intranet.br/contato), execute:

 # mkdir .ask
 # cd .ask
 # cp /usr/share/ask/templates . -R
 # mkdir queue
 # mkdir tmp
 # touch ignorelist.txt
 # touch whitelist.txt
 # chown vpopmail.vchkpw /home/vpopmail/domains/intranet.br/contato/.ask -R
 # chmod 600 /home/vpopmail/domains/intranet.br/contato/.ask -R

Resultado na pasta do usuário contato:

 # find

```
- contato
..|+Maildir/
..| - .ask/
........| --- queue/
........| ---- tmp/
........| ---+templates/
........| ---- whitelist.txt
........! ---- ignorelist.txt
```

As mensagens esperando por confirmação do remetente permanecerão no diretório "queue", arquivos temporários serão trabalhados em "tmp", remetentes conhecidos deverão estar cadastrados em "whitelist.txt" e remetentes bloqueados em "ignorelist.txt".

O mais importante aqui é que o usuário (uid) responsável pela entrega (vpopmail) seja capaz de escrever nesses diretórios.

O arquivo de configuração. Quando definimos "--home=/home/vpopmail/domains/intranet.br/contato" no comando *askfilter*, fizemos com que o ASK procure nessa pasta o arquivo *.askrc*, esse arquivo contém as configurações do ASK específicas para a conta em que vamos usá-lo. Crie o arquivo ".askrc" no diretório especificado e no conteúdo coloque:

```
#------------------- inicio da configuração
[ask]
rc_mymails = contato@intranet.br
rc_myfullname = Contato Intranet
rc_mymailbox = /home/vpopmail/domains/intranet.br/contato/Maildir/
rc_mailkey = ContatoImediatoSecreto
rc_md5_key = mamamiaASK

rc_remote_cmd_enable = on
rc_remote_cmd_htmlmail = off
rc_basic_headers = From:,To:,Cc:,Bcc:,Date:,Subject:,Return-Path:,Received:,Message-ID:
rc_max_attach_lines = 0
rc_askdir = ${HOME}/.ask
rc_msgdir = %(rc_askdir)s/queue
rc_tmpdir = %(rc_askdir)s/tmp
# Templates Padrão para Todos
rc_confirm_dirs = /usr/share/ask/templates
rc_whitelist_on_mailkey = true
rc_confirm_langs = ptbr
rc_whitelist = %(rc_askdir)s/whitelist.txt, %(rc_askdir)s/whitelist-local.txt
rc_ignorelist = %(rc_askdir)s/ignorelist.txt, %(rc_askdir)s/ignorelist-local.txt
rc_mta_command = /usr/sbin/sendmail -t < MAILFILE
```

#------------------- fim da configuração

Salve e garanta que o usuário *vpopmail* conseguirá ler este arquivo:

 # chown vpopmail.vchkpw .askrc
 # chmod g-rwx .askrc

Vamos ver a função de algumas opções:

* rc_mymails = contato@intranet.br

Define os endereços de email que passarão pelo ASK com destino ao mesmo diretório definido em rc_mymailbox, caso haja mais de um, coloque:

rc_mymails = contato@intranet.br , diretoria@intranet.br

Separando por espaço-virgula-espaço.

* rc_myfullname = Contato Intranet

Define o nome do responsável pela conta, essa informação é usada no campo "From:" do e-mail de tira-teima, portanto, coloque um nome assimilativo, a maioria dos clientes de e-mails coloca o nome do campo "From" no catálogo de endereços quando uma mensagem é respondida.

* rc_mymailbox = /home/vpopmail/domains/intranet.br/contato/Maildir/

Define o diretório onde as mensagens serão gravadas para que os softwares servidores (POP3, IMAP) possam entregá-las ao usuário. A presença do barra ("/") no final define o tipo de entrega como Maildir. Caso fosse em mailbox, defina o caminho para o arquivo, sem o barra no final.

* rc_mailkey = ContatoImediatoSecreto

Esse recurso é interessante: define a frase ou palavra secreta. Caso este segredo esteja presente no corpo da mensagem, ela é considerada válida será entregue diretamente, sem tira-teima. Procure colocar algo não muito óbvio, como seu nome! O sobrenome é uma boa idéia, haja visto que apenas seus conhecidos sabem.

* rc_md5_key = mamamiaASK

Define a palavra ou frase usada para gerar o código MD5. Esse código é enviado no assunto da mensagem de tira-teima.

* rc_remote_cmd_enable = on

Habilita/desabilita comandos remotos.

* rc_remote_cmd_htmlmail = off

Habilita/desabilita comandos remotos em mensagens com formato html

* rc_basic_headers = From:,To:,Cc:,Bcc:,Date:,Subject:,Return-Path:,Received:,Message-ID:

Define cabeçalhos usados para verificações.

* rc_askdir = ${HOME}/.ask

Diretório onde as sub-pastas (tmp/, queue/, templates/) foram instalados.

rc_msgdir = %(rc_askdir)s/queue

Diretório onde as mensagens aguardarão por confirmação.

rc_tmpdir = %(rc_askdir)s/tmp

Diretório para manipulação de arquivos temporários.

rc_confirm_dirs = %(rc_askdir)s/templates

Diretório onde estão os templates (modelos) para envio do tira-teima, esses templates pode ser personalizados, assim você coloca aqui a mensagem que deseja enviar para o remetente avaliado.

* rc_whitelist_on_mailkey = true

Se definido como "true", adiciona automaticamente na lista branca (whitelist.txt) o remetente que informou a frase/palavra secreta no conteúdo da mensagem. É necessário que o usuário responsável pela entrega (vpopmail) consiga escrever nesse arquivo.

* rc_confirm_langs = ptbr

Linguagem usada na mensagem de tira-teima, esse valor define os arquivos em templates/ que serão usados.

* rc_whitelist = %(rc_askdir)s/whitelist.txt, %(rc_askdir)s/whitelist-local.txt

Define os arquivos de lista branca, quando um remetente retorna o tira-teima, o endereço de e-mail dele é adicionado no primeiro arquivo definido. Assim, o usuário responsável pela entrega (vpopmail) deve ter privilégios de escrita nesse arquivo. Use o segundo parâmetro (opcional) para definir uma lista global, ou criar grupos de listas: use a imaginação!

* rc_ignorelist = %(rc_askdir)s/ignorelist.txt, %(rc_askdir)s/ignorelist-local.txt

Define os arquivos de lista negra.

* rc_mta_command = /usr/sbin/sendmail -t < MAILFILE

MUITO IMPORTANTE. Define o comando a ser executado para enviar a mensagem de tira-teima. No caso do qmail, /usr/sbin/sendmail deve ser um link simbólico para /var/qmail/bin/sendmail

Prontinho!

Envie uma mensagem para o usuário que está usando ASK e verifique o resultado. Caso erros ocorram, o ASK procura o primeiro diretório acima do diretório do usuário para escrever um arquivo ASK-XXXXX contendo os erros.

Ajuda e referências

O artigo atualizado será mantido no site www.lifewithqmail.com.br.

Caso deseja se aprofundar no *ASK*, aconselho que visite a página do autor e do ASK:

- http://www.paganini.net
- http://www.paganini.net/ask

Procure não fazer perguntas sem antes reler o artigo ou consultar a versão atualizada!

Grato, espero que gostem.

---

http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=2083

Voltar para o site