Técnicas de combate a *spam* em servidores Linux que utilizam o *Mail Transfer Agent* Postfix.

Fábio de Oliveira Dias[1], Cristina Moreira Nunes[1]

[1]Centro Universitário La Salle – Av. Victor Barreto, 2288 – Canoas – RS – Brasil

fabio@cefetrs.edu.br, nunes@lasalle.tche.br

Resumo. *O spam tornou-se um grande problema para a comunidade internet, em virtude do aumento da demanda de recursos computacionais exigidos para suportar o volume, cada vez maior, de mensagens indesejadas. Este artigo aborda técnicas de combate ao spam em servidores Linux que fazem uso do Mail Transfer Agent Postfix. Procura, também, demonstrar que a combinação destas diversas técnicas (consulta em servidores de DNS reverso e em Realtime Blackhole Lists, utilização de listas de acesso locais e bloqueio de anexos nocivos) pode ser capaz de minimizar os efeitos decorrentes desse problema. Espera-se que, com a aplicação da metodologia desenvolvida, mais de 98% do total de mensagens indesejadas possa ser corretamente descartado.*

1. Introdução

Segundo a *United Nations Statistics Division* (Divisão de Estatísticas da Organização das Nações Unidas) [United Nations Statistics Division 2004], a internet mundial já possui mais de 600 milhões de usuários ativos, sendo que o Brasil responde por mais de quatorze milhões destes. Um dos recursos mais utilizados e que são providos por esta tecnologia é o sistema de correio eletrônico. Bilhões de mensagens trafegam diariamente pela internet levando dados de uma parte a outra do planeta em questão de segundos.

Atualmente, conforme o *Spamhaus Block List* [Spamhaus 2004], entidade de pesquisa que efetua estudos sobre o assunto, a maior parte do tráfego de mensagens de correio eletrônico pode ser classificada como UCE (*Unsolicited Commercial E-mail*, Mensagem Comercial Não-solicitada) ou, em sua designação popular, *spam*. Segundo a mesma entidade, o Brasil já é o quarto país na produção mundial de *spams*.

A prática do *spam* tem gerado preocupação e provocado muitas reações por parte dos administradores de rede e dos provedores de acesso. O *spam* gera excessiva ocupação da largura de banda, provocando congestionamentos na rede e consumo de recursos computacionais valiosos. Os usuários perdem tempo e dinheiro para abrir, ler e apagar as mensagens inúteis, podendo, ainda, ser atacados por vírus, *scams* e outras pragas enviadas em massa. Assim, a única parte que costuma se beneficiar com esse tipo de prática é o *spammer*, pois o seu meio de divulgação tem custo baixo e é extremamente eficaz, considerando as taxas de retorno de métodos tradicionais como mala-direta e *telemarketing*.

Além disso, segundo a 15ª Pesquisa Anual de Informática da Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas [Meirelles 2004], o número de servidores que utilizam o sistema operacional Linux no Brasil vem crescendo consideravelmente a cada ano, em virtude de sua confiabilidade, segurança e melhor aproveitamento de recursos. Nestes servidores, a utilização do MTA (*Mail Transfer Agent*, Agente de Transferência de Mensagens) Postfix também está em expansão, em virtude de

sua robustez e pelo histórico de vulnerabilidades de seu concorrente direto em sistemas Linux, o Sendmail.

Neste artigo, serão abordadas algumas técnicas de combate ao *spam* em sistemas Linux que utilizam o agente de transferência de mensagens Postfix. A motivação principal deste artigo é a de abordar um tema de relevância, partindo do estudo das técnicas de envio de *spam* até verificar os procedimentos que devem ser adotados para minimizar este problema. Como conseqüência, serão buscadas formas de reduzir a ocorrência de *spam* em servidores Linux que fazem uso do MTA Postfix a níveis considerados mínimos.

Na próxima seção será exposto o referencial teórico que serve de embasamento a este artigo. A seção 3 abordará a descrição metodológica desenvolvida. Já a última seção conterá as conclusões do estudo efetuado.

2. Referencial Teórico

Conforme a RFC 2505 [Lindberg 1999] e Hoepers [Hoepers 2003], os *spammers* costumam utilizar, basicamente, três técnicas para enviar mensagens não-solicitadas em massa: entrega direta (*direct delivery*), *open relay* e *open proxy*. Além disso, no caso de pragas digitais como vírus, utilizam os computadores infectados como nova fonte de envio de mensagens indesejadas para terceiros.

A entrega direta consiste na ativação (mesmo que apenas momentânea) de um servidor SMTP (*Simple Mail Transfer Protocol*, Protocolo Simples de Transferência de Mensagens) em uma determinada máquina, que servirá para enviar milhões de *spams* para qualquer parte do mundo em questão de minutos. A desvantagem desta técnica é que o endereço IP (*Internet Protocol*, Protocolo Internet) do *spammer* pode ser facilmente identificado e bloqueado.

Outras formas comuns de envio de *spam* são através dos mecanismos de *open relay* e *open proxy*. Servidores que possuem *relay* ou *proxy* abertos permitem o encaminhamento de mensagens a terceiros através de seus serviços. Assim, os *e-mails* que chegam aos destinatários contêm o endereço IP do servidor vulnerável. A desvantagem desta técnica, além da grande possibilidade de registro do endereço IP invasor nos *logs* do sistema, consiste no maior grau de conhecimento exigido para a sua implementação. Andreolly [Andreolly *et al* 2001] considera que estes fatos são considerados incidentes de segurança e devem ser reportados aos responsáveis pelos domínios envolvidos.

A RFC 821 [Postal 1982] define o protocolo SMTP. Na época de sua concepção, não foram dimensionados os problemas que alguns aspectos referentes à segurança e não contemplados poderiam ocasionar. Em 2001, a RFC 2821 [Klensin 2001] abordou novamente o protocolo SMTP, tornando obsoleta a RFC 821. Entretanto, nenhuma funcionalidade relacionada à segurança do protocolo foi alterada ou adicionada.

A fim de abrandar as deficiências explícitas da RFC 821, foi lançada a RFC 2505. Esta RFC provê algumas orientações que visam prevenir a aceitação indevida de *spam* pelos MTAs. Conforme esta RFC, quando ocorre uma conexão SMTP, três situações distintas podem ocorrer, todas relacionadas ao resultado da consulta do endereço IP de origem junto a um serviço de DNS (*Domain Name Server*, Servidor de Nomes de Domínio) reverso. São elas:

- este endereço IP não está associado a um nome de domínio FQDN (*Fully Qualified Domain Name*, Nome de Domínio Completamente Qualificado);

- o nome de domínio contido no *header* (cabeçalho) da mensagem foi forjado e não corresponde ao real domínio associado a este endereço IP;
- o endereço IP corresponde ao domínio informado no *header* da mensagem.

Na maioria dos casos, o nome de domínio do endereço de origem da mensagem é falsificado. Assim, se o resultado da comparação do endereço IP com o domínio informado pelo remetente corresponder a uma das duas primeiras situações descritas anteriormente, é muito provável que a mensagem possa ser considerada *spam*.

Mecanismos providos pelo protocolo e descritos na RFC 2821, como SMTP VRFY, SMTP EXPN e SMTP ETRN, devem ser desativados. Tais mecanismos permitem aos *spammers* confirmar, através de ataques de força bruta, por exemplo, a lista de usuários de um determinado servidor e, assim, obter novos destinatários de mensagens indesejadas.

Como forma de reforçar a segurança e evitar ao máximo a aceitação de *spams*, além das providências citadas e recomendadas pela RFC 2505, a metodologia descrita a seguir deverá também adotar um bloqueador de anexos.

Atualmente, os vírus de computador e outras pragas digitais equivalentes (*scams*, *spywares*, *trojans*, *worms*, etc) têm se propagado, basicamente, pelo repasse de *e-mails* de máquinas infectadas aos endereços constantes em seus catálogos. Na maioria dos casos, estas mensagens contêm anexos que podem ser executados com a simples visualização da mensagem. Tais anexos, que usam extensões diferentes das já tradicionais *.bat, .com, .exe*, *.dll* e *.pif*, tais como *.cpl*, *.scr*, *.reg*, entre outras, também devem ser filtrados.

3. Descrição Metodológica

A adoção de medidas que buscam minimizar o *spam* deve agir de duas maneiras, procurando se certificar que o servidor não está sendo utilizado como *relay* não-autorizado e evitando a entrada de mensagens indesejadas.

Em um primeiro momento, devem ser tomadas atitudes que impeçam a utilização do MTA como propagador de *spam*, através de *open proxy* ou *open relay*.

Como os serviços *proxy* fogem ao escopo deste artigo, será assumido que eles estão corretamente configurados ou simplesmente desativados. Serviços *proxy* abertos e mal-configurados permitem que o *spammer* envie uma requisição HTTP com alvo na porta 25 (SMTP) do *host* de destino [Hambridge and Lunde 1999]. Criado este caminho, é por aí que poderão ser enviadas as mensagens com os mais variados destinos. O endereço IP que constará nas mensagens será o do *host* possuidor do serviço *proxy* que está sendo abusado.

Como parte da correta configuração do MTA Postfix, deve-se certificar que o *relay* só poderá ser efetuado por *hosts* situados nas faixas de rede que possuem permissão para tanto. Isso é feito com a adição das seguintes linhas no arquivo */etc/posfix/main.cf* [Venema 1999]:

```
mynetworks_style = subnet
mynetworks=192.168.0/24, 192.168.1/24, IP/máscara...
```

A seguir, as seguintes linhas também devem ser adicionadas ao arquivo */etc/posfix/main.cf*, de forma a atender as recomendações da RFC 2505 e solicitar que sejam efetuadas as consultas ao serviço de DNS reverso:

```
smtpd_client_restrictions =
permit_mynetworks,reject_non_fqdn_sender,reject_non_fqdn_recipient,
```

```
reject_unknown_sender_domain,reject_unknown_recipient_domain,
hash:/etc/postfix/access,reject_unknown_client
smtpd_sender_restrictions =
permit_mynetworks,check_sender_access hash:/etc/postfix/access,
reject_unknown_sender_domain,check_relay_domains
smtpd_recipient_restrictions =
permit_mynetworks,reject_invalid_hostname,reject_non_fqdn_sender,
reject_non_fqdn_recipient,reject_unknown_sender_domain,
reject_unknown_recipient_domain,reject_unauth_pipelining,
reject_unauth_destination,permit
```

Cabe salientar que após cada alteração no arquivo */etc/posfix/main.cf*, o comando '*postfix reload*' deve ser executado para que as alterações tenham efeito.

O arquivo */etc/postfix/access*, citado em algumas das linhas acima, refere-se ao mecanismo que gerencia listas brancas e listas negras, respectivamente, e que permite um ajuste fino à técnica adotada. Este ajuste busca evitar que ocorra bloqueio ou aceitação de mensagens de forma indevida. Em alguns poucos casos, há servidores de DNS que não efetuam a correta correspondência de seu DNS reverso. Entretanto, isto é apenas um sinal de que o servidor está mal-configurado. Não significa que e-mails provenientes destes lugares possam ser classificados como *spam* e devam ser rejeitados. Por outro lado, há também servidores utilizados para o envio de *spam* que possuem o DNS reverso corretamente configurado.

O conteúdo deste arquivo deve ser inserido ou editado, de maneira que ele siga o seguinte formato:

```
aaa.bbb.ccc.ddd      OK
zzz.bbb.ccc.ddd      550 Spam permanentemente negado
```

A primeira linha informa ao MTA que este deve aceitar mensagens provenientes do endereço *aaa.bbb.ccc.ddd*. A segunda linha diz que o código de erro permanente 550, seguido da mensagem '*Spam permanentemente negado*', deve ser retornado, na eventualidade da ocorrência de conexões por parte do IP *zzz.bbb.ccc.ddd*.

Cada alteração no arquivo */etc/postfix/access* requer a execução do comando *postmap /etc/postfix/access*, para que as mesmas façam efeito.

Para que o MTA Postfix faça consultas em RBLs mantidas por entidades que combatem o *spam*, algumas configurações devem ser efetuadas ao arquivo */etc/postfix/main.cf*. O exemplo a seguir demonstra como seria solicitada a consulta em três RBLs distintas:

```
maps_rbl_domains = sbl.spamhaus.org, relays.ordb.org
```

Além disso, a seguinte linha deve ser acrescentada às seções *smtpd_client_restrictions* e *smtpd_recipient_restrictions*:

```
reject_maps_rbl
```

Para que ocorra o bloqueio de anexos potencialmente nocivos, o Postfix deve ser configurado para que faça a análise de conteúdo dos *headers* e do corpo das mensagens. Essa checagem é efetuada através da avaliação de expressões regulares e necessita que o módulo PCRE (*Perl Compatible Regular Expression*, Expressões Regulares Compatíveis Perl) esteja instalado. Para que a verificação seja efetuada, as seguintes linhas devem ser adicionadas no arquivo */etc/postfix/main.cf*:

```
header_checks = pcre:/etc/postfix/header_checks
mime_header_checks = $header_checks
nested_header_checks = $header_checks
body_checks = pcre:/etc/postfix/body_checks
body_checks_size_limit = 51200
```

Os arquivos */etc/posfix/header_checks* e */etc/postfix/body_checks* (referenciados nas linhas acima) devem conter, linha por linha, as expressões regulares que devem ser avaliadas e as ações que devem ser tomadas em casos positivos. Diversas características das mensagens podem ser validadas, tais como assunto, conteúdo, remetente, destinatário e anexos. Assim, cada mensagem que entra no servidor é verificada e pode ser rejeitada, caso não se enquadre nas regras pré-estabelecidas. A linha a seguir demonstra o conteúdo que estes arquivos devem apresentar para que ocorra o bloqueio de anexos com extensões executáveis potencialmente nocivas (como, por exemplo, *.bat*, *.com*, *.cpl, .dll*, *.exe*, *.pif*, *. reg* e *.scr*,) e o retorno que deve ser fornecido ao remetente.

```
/^Content-Type|Disposition):.*(file)?name=.*.(bat|com|cpl|dll|
exe|pif|reg|scr) / REJECT Mensagem rejeitada devido à presença
de um arquivo .${3} anexado.
```

As técnicas abordadas até aqui se referem às relacionadas diretamente ao MTA Postfix. Entretanto, a sua aplicação isolada não é suficiente, tendo em vista a variação das técnicas utilizadas por *spammers*. Deve ser fortemente cogitada a possibilidade de combinar à metodologia um filtro estatístico bayesiano. Há diversas ferramentas GPL disponíveis, dentre as quais se destaca o SpamAssassin, que se encontra disponível nas versões mais atuais do sistema operacional Linux. É bastante recomendável, ainda, a combinação de um sistema antivírus, como o Amavis.

4. Conclusões

De acordo com a RFC 2505, o *spam* é considerado extremamente prejudicial à estrutura da internet e a seus usuários pelos seguintes motivos:

- ocorre em grande volume, isto é, as pessoas recebem grande quantidade de *e-mails* inúteis em suas caixas postais;
- não há relação direta entre eventuais áreas de interesse do destinatário e o *spam* enviado;
- há a geração de um grande custo financeiro para os provedores de acesso e corporações, que têm de manter estruturas robustas (como alta largura de banda e servidores e discos de alta capacidade e desempenho) para comportar o tráfego intenso; e,
- ocorre a utilização de *relays* não-autorizados como forma de propagar o *spam*. Ao evitar que seja exposta a verdadeira origem, o *spammer* também demonstra que possui consciência de que seus atos são prejudiciais.

Portanto, a metodologia descrita neste artigo busca, através da união de diversas técnicas, minimizar a ocorrência de *spam* em MTAs Postfix. As técnicas abordadas (verificação de DNS reverso, uso de RBLs, bloqueio de anexos, etc) possuem desvantagens que se tornam menos evidentes quando combinadas.

Com a finalidade de obter alguns resultados preliminares, foi efetuada uma pequena experimentação. Foram analisadas, através dos *logs* do sistema, 458 mensagens recebidas no período de 48 horas, entre os dias 07 e 08 de junho de 2004, pelo servidor *mail.cefetrs.edu.br* (onde foi implantada a metodologia descrita). Dentre as mensagens aceitas, 218 eram desejadas (95,19%) e 11 consideradas *spam* (4,81%). Entre as bloqueadas, 225 eram consideradas *spam* (98,25%) e 4 desejadas (1,75%). Apesar do caráter meramente ilustrativo da experimentação, seus resultados podem ser considerados satisfatórios. Cabe salientar que testes mais apurados deverão ser efetuados.

A rejeição de 100% de mensagens indesejadas é uma meta que surge como inalcançável, em virtude das variações de técnicas utilizadas pelos *spammers* e da vasta quantidade de servidores mal-configurados e que podem sofrer explorações de *relay*. No entanto, a adoção de algumas medidas que combatam o *spam* pode amenizar os inúmeros danos ocasionados por este problema.

O correio eletrônico já é um meio de comunicação consagrado e extremamente difundido em virtude de sua simplicidade, agilidade e eficiência. Entretanto, o *spam* é uma grande ameaça ao futuro desta ferramenta. Assim, cada membro da comunidade internet deve auxiliar, de alguma forma, no combate a essa enorme quantidade de lixo eletrônico que é propagada diariamente. O *spam* só ocorre porque há um bom retorno financeiro decorrente desta prática. A primeira forma de combate deve ser, portanto, o boicote às suas inúmeras ofertas. Caso não ocorra algum viés na tendência do aumento da remessa de mensagens indesejadas, dentro de pouco tempo não haverá mais condições para a execução de nenhuma tarefa útil – apenas a de apagar *spams*.

5. Referências Bibliográficas

Androutsopoulos, Ion *et al* (2000) "An Experimental Comparison of Naive Bayesian and Keyword-Based Anti-Spam Filtering with Personal E-mail Messages", National Center for Scientific Research 'Demokritos', Athens, Greece, disponível em http://portal.acm.org/citation.cfm?id=345569& dl=ACM&coll=GUIDE e em http://adsabs.harvard.edu/cgi-bin/nph-bib_query? 2000cs.....8019A, março.

Andreoly, A. *et al* (2001) "Controle de SPAM baseado em pré-detecção da vulnerabilidade de Mail Relay", Computer Emergency Response Team (CERT-RS/UFRGS), disponível em http://www.rnp.Br/newsgen/0207/mail_relay.htm, abril.

Hambridge S. and Lunde A. (1999) "RFC 2635: Don't spew – A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam)", disponível em http://www.ietf.org/rfc/rfc2635.txt, março.

Klensin J. (2001) "RFC 2821: Simple Mail Transfer Protocol", disponível em http://www.ietf.org/rfc/rfc2821.txt, março.

Lindberg G. (1999) "RFC 2505: Anti-Spam Recommendations for SMTP MTAs", disponível em http://www.ietf.org/rfc/rfc2505.txt, março.

Meirelles, F. (2004) "Pesquisa Anual de Administração de Recursos de Informática – Sumário de Resultados da Pesquisa", 15ª edição, Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas, disponível em http://www.fgvsp.br/cia/pesquisa/Pesq04GV.pdf, abril.

Postal, J. (1982) "RFC 821: Simple Mail Transfer Protocol", disponível em http://www.ietf.org/rfc/rfc821.txt, março.

Spamhaus Block List (2004) "Top 10 Spam Countries – April 2004", Disponível em http://www.spamhaus.org, abril.

United Nations Statistics Division (2004) "Internet Users (ITU estimates 2003)", Disponível em http://unstats.un.org/unsd/mi/mi_series_results.asp? rowID=608&fID= r15&cgID=, março.

Venema, W. (1999) "Postfix Documentation", disponível em http://www.postfix. org/documentation.html, março.