MECANISMOS PARA A DEFESA CONTRA *SPAMS*

Robert Mady Nunes[1], Wilmar Borges Leal Junior[1]

[1] Especialistas e Professores do Ensino Básico, Técnico e Tecnológico – IFTO; membro do Grupo de Educação, Inovação e Tecnologia do Tocantins (GEDAITT) – Dianópolis – TO – Brasil. e-mail: <robert.nunes@ifto.edu.br, wilmar.junior@ifto.edu.br>

Resumo: É fato que o recebimento de mensagens *spams*, denota um grande problema para os usuários de *webmails.* Em virtude da grande variedade de tipos e formas dificulta o trabalho dos mecanismos chamados *antispams*. Desta forma, é realizado um estudo referente aos mecanismos *antispams* e as suas ações no combate às mensagens *spams*. Assim, o objetivo do presente trabalho é analisar mecanismos *antispams* atuando individualmente ou em conjunto, junto ao servidor de *e-mail*, buscando verificar qual a forma de atuação desses mecanismos e apresentar a melhor solução, no que diz respeito à eficácia e desempenho.

Palavras–chave: a*ntispam*, e-mails, mecanismos, servidores, **s***pam*

1 INTRODUÇÃO

Com a popularização da internet e o massivo uso de sistemas de correio eletrônico, um dos principais problemas são as mensagens de e-mail não solicitadas e/ou indesejadas, a exemplo, as mensagens publicitárias, conhecidas como mensagens *spam*s (CRANOR & LAMACCHIA, 1998; TEIXEIRA, 2004). Mensagens *spam*s não prejudicam apenas aos usuários de *webmails*, dependendo da quantidade de *spams* enviadas, por dia, o usuário ficará a merce de procurar e excluir estas mensagens de suas caixas de entrada, do outro lado, prejudica também os provedores de Internet, pois, se faz necessário o aumento da capacidade de seus *links* de conexão com a Internet, dado o alto tráfego que é gerado pelas mensagens *spam* (CRANOR & LAMACCHIA, 1998; NUNES, 2007).

Para controlar, e minimizar, a quantidade de mensagens *spam*s encaminhadas para as caixas de entrada dos usuários de *webmails*, são utilizados mecanismos conhecidos como *antispams*. Existem vários tipos de mecanismos *antispams* e cada um tem sua forma específica de realizar bloquear das mensagens *spam*s. Alguns dos mecanismos mais conhecidos são baseados nas seguintes técnicas: listas bloqueio, verificação de autenticidade do remetente e filtros de conteúdos, podendo ser aplicado individual ou conjuntamente (TAVEIRA et al., 2006; OLIVIO et al., 2015; FABRE, 2005; TEIXEIRA, 2004; ANDROUTSOPOULOS et al., 2000; SCHNEIDER, 2003; RAMOS et al., 2004; JUNG, 2004).

As listas de bloqueio fazem análise dos cabeçalhos das mensagens de e-mail, tendo como objetivo, identificar endereços IP, domínios ou endereços de e-mail que sejam reconhecidamente fontes de mensagens *spam*s. O bloqueio é feito quando a mensagem recebida for enviada por um

remetente fonte de *spam*, ou seja, caso o endereço IP, domínio ou endereço de e-mail do remetente esteja presente em alguma das listas a mensagem, o mesmo será descartada (TAVEIRA et al., 2006; OLIVIO et al., 2015).

A verificação de autenticidade, reporta a autenticidade do remetente, visto que, com a utilização desse mecanismo só serão aceitas mensagens que originarem de remetentes autênticos. Desse modo, para verificar a autenticidade de um usuário remetente, é analisado o servidor de e-mail remetente, se o mesmo é, ou não, responsável pelo envio das mensagens deste usuário (FABRE, 2005).

Já os filtros de conteúdos analisam todo o conteúdo das mensagens de e-mails, englobando o cabeçalho e seu corpo, de modo que, a análise realizada destina-se a identificar padrões predefinidos, verificando palavras ou frases que estão com frequência em mensagens *spam*s, são esses os padrões que auxiliam os filtros de conteúdo na identificação de mensagens *spam*s (TEIXEIRA, 2004;OLIVIO et al., 2015).

Embora exista uma grande quantidade de mecanismos *antispams*, cada um com suas peculiaridades, há também poucos estudos que apresentem a influência desses mecanismo em servidores com resultados quantitativos de sua utilização. Além disso, é interessante apresentar uma solução em que se utilize os recursos oferecidos com eficácia e que afete minimamente o desempenho dos servidores de e-mail.

Diante do exposto, este trabalho tem como objetivo implantar e analisar mecanismos *antispams*, atuando individualmente ou em conjunto, de forma a verificar a eficácia e sua influência no desempenho dos servidores de e-mail, apresentando assim, uma solução para os administradores utilizarem em seus servidores de e-mail.

2. METODOLOGIA

O presente trabalho apresenta estudos sobre correio eletrônico, *spam*s e principalmente sobre mecanismos *antispams*. O estudo é realizado com o objetivo de conhecer os mecanismos *antispam*s existentes, selecionar e compreender cada um dos mecanismos *antispam*s utilizados nos testes.

Em paralelo ao levantamento bibliográfico, é realizada a configuração de dois servidores de e-mail, para a realização dos testes práticos, com a finalidade de analisar a eficácia dos mecanismos *antispam*s, atuando em conjunto ou individualmente.

Após a conclusão e configuração dos servidores de e-mail, será realizado um estudo detalhado sobre os mecanismos *antispam*s onde serão definidos os critérios a serem utilizados nos testes em laboratório.

Após a realização dos testes em laboratório, será determinada a melhor forma de utilização dos mecanismos *antispams,* demonstrando a eficácia em ambiente real.

2.1 Critérios para a Seleção de Mecanismos *antispam*s

Para a seleção de mecanismos *antispams*, os critérios utilizados, baseiam-se na ideia de seleção de mecanismos *antispams* utilizado no trabalho de Fabre (2005), são eles:

- **Classificação em número de *downloads*:** mecanismos que são amplamente utilizados e difundidos;
- **Classificação em satisfação na utilização:** mecanismos que são bem avaliados, por sua eficácia;
- **Opções por gratuidade:** mecanismos gratuitos;
- **Utilização de ferramentas para coleta de dados:** escolha de mecanismos multiplataforma.

3. RESULTADOS E DISCUSSÕES

Com a realização dos testes é possível verificar a eficácia dos mecanismos *antispams*, atuando de forma conjunta ou individualmente no enfrentamento as massivas mensagens *spams,* apresentando considerável sobrecarga no servidor de e-mail.

Ao final dos testes e das análises realizadas, será apresentada uma possível solução para utilização em ambiente de produção.

3.1 Software para envio de e-mails

Para a realização dos testes práticos é utilizado um *socket* cliente de SMTP que realiza o envio de e-mails em massa automáticamente (NUNES, 2007). As mensagens utilizadas para os testes são coletadas do repositório particular de domínio publico, Untroubled (1998), que contém várias mensagens de *spams armazenadas* individualmente em arquivos de texto, disponível em <*http://untroubled.org/spam*/>.

3.2 Testes de Eficácia

Os testes realizados, têm como objetivo a verificação da eficácia dos mecanismos *antispam*s, atuando individual ou conjuntamente com outro mecanismo. Nos testes, a eficácia é analisada de acordo com a quantidade de mensagens falso-positivo (mensagens *spam* na caixa de entrada) e/ou falso-negativo (mensagens não *spam* na caixa *spam*). Sendo que as situações testadas são:

- Atuação individual da verificação de reverso do DNS;
- Atuação individual das listas legras;
- Atuação individual do Filtro *bayesiano*;
- Atuação em conjunto de listas negras e filtro *bayesiano*.

3.3 Verificação de Reverso do DNS

O mecanismo de verificação de reverso do DNS analisa se o servidor de e-mail remetente possui reverso configurado, rejeitando mensagens vindas de servidores sem reverso configurado ou com problemas e aceitando mensagens originadas de servidores que possuem reverso configurado corretamente (RAMOS et al., 2004; JUNG, 2004).

3.4 Listas negras

As listas negras são mecanismos *antispam*s que analisam os cabeçalhos das mensagens de e-mail, com o intuito de identificar endereços IP e domínios de e-mail que sejam reconhecidamente fontes de mensagens *spam*s (RAMOS et al., 2004; JUNG, 2004).

3.5 Filtro *bayesiano*

Filtros *bayesiano*s são mecanismos que analisam todo o conteúdo das mensagens de e-mail objetivando identificar padrões textuais, buscando determinar o que é ou não uma mensagem *spam* (ANDROUTSOPOULOS et al., 2000; SCHNEIDER, 2003). Para a análise de filtro *bayesiano* foi utilizada a ferramenta *bogofilter*.

3.6 Listas negras e filtro *bayesiano*

Para os testes de eficácia utilizando mecanismos de lista negra conjuntamente com filtros *bayesianos,* é utilizada a mesma coleção de mensagens *spams* enviadas nos testes anteriores.

3.7 Solução indicada

Com base nos testes de eficácia, observa-se que: o filtro *bayesiano* é muito preciso em determinar o que é mensagem *ham* (não *spam*) e mensagem *spam*; as listas negras não rejeitam mensagens *hams*, mas, apresenta uma quantidade significativa de falsos-negativos; e, o verificador de reverso de DNS é bastante eficaz na rejeição de mensagens *spam*s.

Nos testes, é possível verificar uma desvantagem apresentada pelo mecanismo de verificação de reverso do DNS, o mesmo gerou mensagens de e-mails falso-positivos, em um ambiente de produção, haveria sobrecarga desnecessária nos servidores.

Assim, de acordo com os resultados dos testes, a escolha da melhor solução a ser utilizada em um ambiente real fica entre a utilização dos mecanismos de listas negras e filtros *bayesiano*s, atuando individualmente ou em conjunto.

A tabela 1, abaixo, apresenta a comparação dos resultados entre testes realizados com os mecanismos de listas negras e filtro *bayesiano*, atuando individual ou conjuntamente.

Tabela 1: Comparativo entre mecanismos

	Rejeitadas	Caixa de *spam*	Caixa de Entrada
Lista negra	11	0	89
Filtro *bayesiano*	0	95	5
Lista negra e Filtro *bayesiano*	11	84	5

De acordo com os resultados obtidos, a técnica de lista negra se mostra satisfatória no bloqueio de mensagens *spam*s, de modo que, este mecanismo necessita do auxílio de outros mecanismos no combate às mensagens *spam*s.

Os resultados do filtro *bayesiano* também obteve uma satisfação desejável, em razão da quase totalidade de eficácia. Consequentemente, este mecanismo pode atuar com bastante precisão em um ambiente real e sem a necessidade de utilização de outros mecanismos.

E por fim, o resultado da combinação entre listas negras e filtro *bayesiano*s atingem o mesmo percentual de acertos do filtro *bayesiano,* atuando individualmente, visto que 11% das mensagens *spam*s são rejeitadas pelas listas negras, antes de serem analisadas pelo filtro *bayesiano*.

Diante disso, essa solução diminui o processamento do servidor de e-mail, tendo em vista que, com as mensagens rejeitadas por listas negras, reduz o número de mensagens *spam*s a serem analisadas pelo filtro *bayesiano*, o que diminui o processamento do servidor, melhorando consideravelmente o seu desempenho.

Contudo, ao contrário das listas negras, o funcionamento ideal dos filtros *bayesiano*s depende muito do treinamento, o qual deve ser feito pelo administrador das redes tendo como base uma grande quantidade de mensagens *hams* e *spam*s. Desta forma, o resultado poderia ser menos satisfatório do que os apresentados nesse trabalho, caso o treinamento não seja realizado adequadamente.

E por fim, após os testes realizados, a solução mais adequada é a utilização dos mecanismos de listas negras combinado com o filtro *bayesiano.* Método que apresenta boa relação eficácia/desempenho. Apesar do ótimo resultado, em se tratando de ambiente de produção, poderá ser um pouco diferente, tendo em vista que, diariamente surgem novas mensagens *spam*s. Logo, é sempre bom lembrar da necessidade de atualização constante das bases de dados dos mecanismos *antispam*s com vistas ao melhor resultado.

3.8 Trabalhos Futuros

Com base em todo o trabalho é possível compreender a existência de várias técnicas para o combate aos *spams,* as quais podem ser utilizadas e analisadas atuando de forma integrada ou não às outras técnicas. Baseado nisso, como sugestões de trabalhos futuros, pode-se testar mais técnicas *antispams* atuando integradas, com a finalidade de mais precisão na definição de falsos-positivos e falsos-negativos. Sendo que, outra sugestão de trabalho futuro é o desenvolvimento de uma ferramenta *antispams* utilizando a técnica, de Inteligencia artificial, redes *bayesianas*, a qual utiliza a análise probabilística para a classificação de mensagens *spam.*

5 CONSIDERAÇÕES FINAIS

Este trabalho tem como objetivo testar e analisar a eficácia de mecanismos *antispam*s existentes, indicando a melhor solução no combate aos *spam*s, com utilização dos mesmos, individualmente ou conjuntamente. Para a decisão da solução a ser indicada é levado em consideração, dentre outros, o tempo que os mecanismos *antispam* gastam para fazer a análise das mensagens, objetivando a menor carga de desempenho no servidor de e-mail, reduzindo assim, o desnecessário processamento.

Dada a existência de vários mecanismos *antispams*, baseados nas técnicas estudadas, selecionamos apenas alguns mecanismos para serem implementados e estudados em profundidade, os quais são: listas negras, verificação de reverso do DNS e filtro *bayesiano*.

A partir dos testes com a verificação de reverso do DNS conclui-se que este mecanismo é bastante eficaz no combate às mensagens *spam*s, entretanto, gera uma quantidade considerável de mensagens falso-positivos, o que se tornaria inviável para um ambiente de produção.

Os resultados dos testes com as listas negras mostram que este mecanismo não gera mensagens falso-positivo, entretanto, gera grandes quantidades de mensagens falso-negativo, todavia, este mecanismo necessita ser combinado com outro mecanismo para combater as mensagens *spam*s.

Os resultados dos testes com o filtro *bayesiano* mostram que este mecanismo é o mais completo dentre todos os utilizados, sendo bem treinado, não gera mensagens falso-positivos e obtêm quase 100% de eficácia no combate às mensagens *spam*s.

Em relação à eficácia, os testes com listas negras atuando conjuntamente com os filtros *bayesiano*s obteve-se os mesmos resultados do bloqueio de mensagens *spam*s utilizando filtro *bayesiano* atuando individualmente.

Conclui-se, com os dados apresentados, que, a solução mais indicada a ser utilizada em um ambiente de produção é a combinação do mecanismo de listas negras e filtro *bayesiano* visto que, o bloqueio inicial feito pelas listas negras reduz o número de mensagens de e-mail a serem analisadas pelo filtro *bayesiano*, consequentemente reduz o processamento do servidor de e-mail, dado que menos mensagens de e-mail serão processadas pelos filtros *bayesiano*s tendo um ganho de desempenho.

E por fim, é possível sugestões de trabalhos futuros, com a utilização de mais técnicas *antispams* e o desenvolvimento de um mecanismo baseado em redes *bayesianas*, para melhor filtro de *spams*.

REFERÊNCIAS

ANDROUTSOPOULOS, Ion et al. **An evaluation of naive bayesian anti-spam filtering**. arXiv preprint cs/0006013, 2000.

CRANOR, L.F., and LAMACCHIA, B.A. **“Spam!”**, Communications of ACM, 41(8):74–83. 1998.

FABRE, Recímero César. **Métodos Avançados para Controle de** *spam***.** 81 p. Trabalho Final (Mestrado Profissional) – Instituto de Computação, Universidade Estadual de Campinas, São Paulo. 2005. Disponível em: <http://www.las.ic.unicamp.br/paulo/teses/20050215-MP-Recimero.Cesar.Fabre-Metodos.avancados.para.controle.de.*spam*.pdf>. Acessado em: 22/07/2017.

JUNG, Jaeyeon; SIT, Emil. **An empirical study of spam traffic and the use of DNS black lists.** In: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement. ACM, p. 370-375. 2004.

NUNES, Robert Mady. **Solução para a defesa contra spams: utilização dos principais mecanismos existentes**. Trabalho de Conclusão de Curso em Sistemas de Informação – Centro Universitário Luterano de Palmas. 97 p. 2007.

OLIVO, Cleber K.; SANTIN, Altair O.; OLIVEIRA, Luiz Eduardo S. **Abordagens para Detecção de Spam de E-mail.** XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2015.

RAMOS, Gustavo R. et al. **Análise de Desempenho de Políticas de Segurança em Servidores de Correio Eletrônico**. In: Proceedings of the 3rd I2TS-International Information and Telecommunication Technologies Symposium. Carlos, SP, Brazil. 2004.

SCHNEIDER, Karl-Michael. **A comparison of event models for Naive Bayes anti-spam e-mail filtering**. In: Proceedings of the tenth conference on European chapter of the Association for Computational Linguistics-Volume 1. Association for Computational Linguistics, 2003. p. 307-314.

TAVEIRA, Danilo Michalczuk et al. **Técnicas de Defesa Contra Spam.** Rio de Janeiro. 2006. 49 p. cap. 5. Disponível em:<http://www.lee.eng.uerj.br/~rubi/TechReports/TMRD06.pdf>. Acessado em: 18/07/2017.

TEIXEIRA, Renata Cicilini. **Combatendo o** ***spam*****: Aprenda como Evitar e Bloquear E-mails Não-solicitados.** 1. ed. São Paulo: Novatec Editora Ltda. 2004.

UNTROUBLED. *spam* **Archive**. 1998. Disponível em: <http://untroubled.org/*spam*//>. Acessado em 25/07/2017.