icado 68
cnico
Dezembro, 2005
Campinas, SP

ração entre o Tipo sta e Estatísticos: cia da Embrapa ropecuária

Marcelo Gonçalves Narciso[1]
Fernando Attique Máximo[2]

iam o cabeçalho e o mo *spam* ou não. Eles anto à classificação da seus desenvolvedores. os desta linha são: vare Foundation, 2005), 2005b) e Bogofilter

wares *antispam* citados é o m o servidor de mensagens, ega deverá ser analisada pelo ser entregue, e esta análise não desprezível (de 2 a 10). Além disso, muitas vezes classificadas como *spams* por faz-se necessário um mecanismo ensagens e aviso ao remetente de oi retida, visto que estes *softwares* canismos (recuperar a mensagem e re a mensagem retida).

ocedem de maneira diferente quanto a ueles que usam do artifício de desafios tente. Uma pergunta simples, um *reply* da mensagem desafio são exemplos dos desafios que este tipo de sistema pode fazer. O mais conhecido é o *antispam* da UOL (2005) no qual o remetente lê uma palavra em uma imagem e responde uma pergunta com aquela palavra. Após isso, a mensagem é enviada ao destinatário e o usuário não mais receberá desafio. Uma versão simplificada deste *software* é o TMDA (2005a), que envia um desafio pedindo ao remetente um *reply* na mensagem desafio ou envio de mensagem vazia a um endereço descrito na mensagem do desafio.

Este trabalho apresenta uma comparação entre os filtros *antispams* estatísticos (o caso de estudo é o Spamassassin) e do tipo desafio-resposta (o caso de estudo é o TMDA), em termos de resultados e sugere soluções para combate de *spams*.

Softwares Antispams Classificatórios

Estes tipos de softwares analisam o corpo e o cabeçalho de uma mensagem e usam métodos estatísticos para classificar uma mensagem. Softwares como Bogofilter (SourceForge.Net, 2005a), Dspam (SourceForge.Net, 2005b) e Spamassassin (The Apache Software Foundation,

tação Aplicada, Pesquisador da Embrapa Informática Agropecuária, Caixa Postal 6041, Barão Geraldo - 13083-970 - Campinas, SP. cnptia.embrapa.br)
temática Aplicada e Computacional, Pesquisador da Embrapa Informática Agropecuária, Caixa Postal 6041, Barão Geraldo - 13083-970 - e-mail: fernando@cnptia.embrapa.br)

Embrapa

são exemplos deste tipo de filtros. Mais detalhes podem ser vistos em (Bayes..., 2005). A vantagem deste tipo de filtro é que ele é adaptativo, isto é, à medida que as técnicas dos remetentes de *spams* vão mudando, este tipo de filtro aprende as mudanças e continua a combater os *spams*. Para isso, o *software* é treinado com uma amostra de *spams* (geralmente 1.000 ou mais) para poder então continuar atuando eficientemente.

Neste trabalho, está sendo considerado para análise o Spamassassin, *software* mundialmente conhecido. Além de ser um filtro *antispam bayesiano* (versões mais recentes), o Spamassassin também usa um conjunto de regras para verificar se a mensagem é um *spam* ou não. Este conjunto de regras sempre se atualiza e pode ser obtido a partir do *site* (The Apache Software Foundation, 2005).

Softwares Antispams do Tipo Desafio/Resposta

Existe uma outra categoria de *software antispam* que age de forma a certificar se o remetente é válido e, desta forma, verificar se a mensagem é de origem confiável. Para isto, este sistema, ao receber uma mensagem, envia uma outra mensagem para o remetente com a finalidade de desafiá-lo a responder uma pergunta ou tomar uma outra ação que seja fácil. Caso o remetente responda corretamente, a mensagem original é entregue ao destinatário final e o endereço eletrônico do remetente vai para uma lista branca para não mais receber desafios. A seqüência de ações é:

1. o remetente envia mensagem para o destinatário;
2. caso o remetente seja desconhecido, o servidor de correio eletrônico retém a mensagem e envia uma outra ao remetente desafiando-o a responder alguma pergunta ou similar;
3. o remetente pode responder a mensagem e esta vai para o servidor de correio eletrônico;
4. se o desafio for respondido, a mensagem original é entregue ao destinatário. Se não for respondido, a mensagem fica em quarentena, isto é, pode ser recuperada pelo destinatário em uma dada quantidade de dias. Após esse prazo, a mensagem é descartada.

O TMDA (2005a) é um *software* do tipo desafio/resposta. O desafio que o servidor envia ao remetente é que este responda à mensagem (*reply to*) simplesmente. Assim, o programa que envia *spam* provavelmente não irá responder ao desafio. Este *software* tem a vantagem de evitar perda de mensagens legítimas (*false positive*). Porém, a entrega de mensagens, quando o remetente não está na lista branca, demora algum tempo. Ao responder o desafio, o remetente não mais receberá desafios quando enviar mensagem, visto que seu endereço foi para uma lista branca do TMDA.

Uma grande vantagem do TMDA sua interface *web,* que permite ao usuário ver as mensagens que estão em quarentena, inserir endereços na lista branca ou negra, configurar quantos dias a mensagem poderá ficar em quarentena, alterar o conteúdo do desafio (personalizar) para facilitar o atendimento do remetente, etc. Esta interface gráfica é instalada no servidor de http do *site* considerado e é acessado via *browser* (Internet Explorer, Mozilla, Opera, etc.). A Fig. 1 mostra a página inicial doTMDA. Observe que as mensagens cujos remetentes não estejam na lista branca ficam armazenadas esperando a resposta do desafio ou ainda que o usuário libere a mensagem (basta clicar no botão *release* ou *whitelist,* sendo que a última opção também insere o endereço do remetente na lista branca). Observe que existem no lado esquerdo as opções Pending (mostra as mensagens pendentes), Filters (configura a localização das listas branca e negra), Lists (possibilita o usuário inserir endereços nas listas branca e negra), Settings (configuração geral do TMDA), Info (informações gerais sobre o TMDA) e Logout. Mais detalhes sobre esta interface estão em TMDA (2005b).

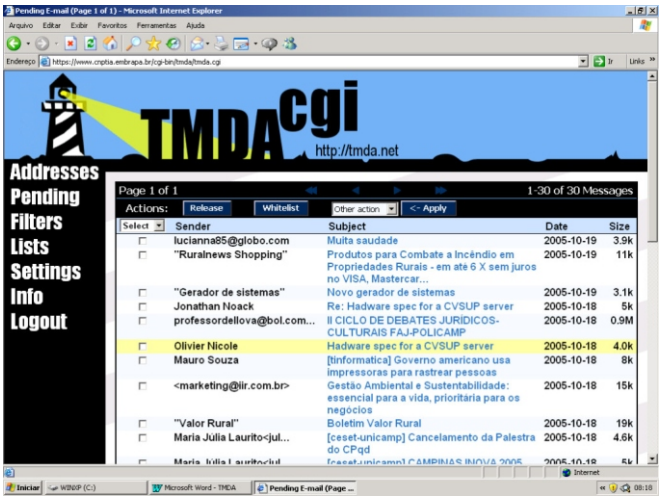

Fig. 1. Página de abertura do TMDA.

Resultados - Comparação entre as Duas Técnicas Apresentadas

O sistema de *mail* na Embrapa Informática Agropecuária, para efeito de comparação, será descrito a seguir. O Mail Transfer Agent (MTA) utilizado foi o *sendmail* (Sendmail Consortium, 2005), o qual usava o *procmail* (Procmail Org., 2005) para entrega de mensagens locais. O *procmail* tem um arquivo de configuração, cujo nome é *procmailrc*, no qual são invocados o Spamassassin, TMDA ou outros filtros *antispams.* Assim, cada *mail* local que era entregue passava pelos filtros configurados em *procmailrc*. Neste arquivo, estavam configurados, na ordem:

- filtros para análise de extensões de arquivos anexos a *mail*. Não eram permitidos arquivos que continham anexos executáveis ou que pudessem trazer algum dano (exe, .bat, .scr, .pif, etc.). Mais detalhes sobre estes filtros podem ser vistos em Narciso (2005);
- se o *mail* era proveniente da Embrapa Informática Agropecuária ou do domínio embrapa.br e outros domínios com relacionamento com a Embrapa (Unicamp, INPE, CenPRA, CNPq, FAPESP, etc.) , então a mensagem era entregue. Era analisado se o IP do servidor de *mail* do remetente, no cabeçalho da mensagem, correspondia ao domínio de onde a mensagem vinha;
- após isto, eram chamados filtros internos do *procmailrc*, por serem mais rápidos de serem executados e também por terem eficácia em muitos casos de *spams*. Mais detalhes sobre estes filtros podem ser vistos em Narciso (2005) ou em (Procmail Org., 2005b);

- o Spamassassin ou o TMDA eram então chamados para analisar as mensagens provenientes de domínios não previstos (configurados) anteriormente.

O esquema do procmailrc descrito vale para outros MTA (postfix, qmail, exim) desde que esses usem o *procmail* para a entrega de mensagens locais. Caso não seja usado o *procmail,* existem outras formas de se chamar o Spamassassin ou TMDA, usando-se o *.forward.*

Desta forma, os *spams* eram analisados pelo Spamassassin ou TMDA após sofrerem uma triagem, evitando-se analisar todas as mensagens. Assim, a entrega da maioria das mensagens válidas era mais rápida, pois não era necessário passar pelos *softwares antispams*. Após esta breve introdução de como era o sistema de *mail*, tem-se então a comparação dos dois *softwares*, representando os filtros estatísticos (Spamassassin) e os filtros do tipo desafio-resposta (TMDA).

Em novembro de 2003 foi instalado o Spamassassin. Em princípio, reduziu pela metade a quantidade de *spams* que os usuários recebiam. Embora o Spamassassin fosse treinado para capturar *spams*, com amostras de *spams* que ele deixava passar, e tinha uma série de análises estatísticas sobre a mensagem para verificar se ela é um *spam* ou não, os resultados obtidos não foram a redução de 90 a 95% de *spams*, prometido pelo *site* do Spamassassin (The Apache Software Foundation, 2005) na época. O que era verificado é que o treinamento não melhorava o desempenho do *software* como era de se esperar. Chegou-se à conclusão de que outros filtros *antispams* deveriam ser usados em conjunto com o Spamassassin para melhorar o desempenho do sistema como um todo. Outro detalhe importante era quanto ao bloqueio de mensagens legítimas, conhecido por falso positivo. Infelizmente, cerca de 5% das mensagens bloqueadas eram falso positivo. Esse problema trouxe insatisfação aos usuários, mas foi resolvido com o tempo, inserindo-se endereços na lista branca do Spamassassin (o *site* não dizia como fazer isso, que foi descoberto analisando-se o código do *software*) e também criando mensagens, no arquivo *procmailrc,* notificando o usuário que tivesse seu *mail* retido. Por um lado, a adoção do Spamassassin melhorou a segurança de entrega de mensagens, mas ainda assim muitos *spams* não eram retidos pelo Spamassassin.

Visto que o Spamassassin não conseguia reter os *spams* e também bloqueava mensagens legítimas, filtros baseados em expressões regulares (Procmail Org., 2005b) para bloquear mensagens foram inseridos no arquivo *procmailrc.* À medida que os filtros foram sendo colocados para analisar o cabeçalho da mensagem e também palavras-chaves do corpo da mensagem, o Spamassassin foi ficando cada vez menos solicitado, visto que os filtros feitos com expressões regulares (Procmail Org., 2005b) eram mais rápidos e também mais eficazes. Visto que estes filtros vinham antes do Spamassassin, os *spams* eram retidos mais rapidamente,o Spamassassin demorava para analisar as mensagens.

Os filtros do tipo estatístico, como dspam e bogofilter, tal como o Spamassassin, também prometem diminuir consideravelmente volume de *spams*. Porém, esses filtros têm os mesmos problemas que o Spamassassin: falso positivo e uma boa quantidade de *spams* passam por esses filtros. Entretanto, esses *softwares* reduzem em razoável quantidade o volume de *spams*. Eles devem ser usados com o cuidado de inserir uma lista branca para evitar análises desnecessárias de mensagens e também notificar os usuários sobre o fato do *mail* ter sido retido, devido ao problema de falso positivo.

Em setembro de 2004 foi feito um levantamento dos *spams* retidos pelo Spamassassin e pelos filtros internos definidos em *procmailrc*. Os dados estão na Tabela 1.

Tabela 1. Quantidade de *spams* retida pelo sistema mensagens em setembro de 2004.

Dia	*Spamassassin*	*Filtros internos do Procmail*	*% de retenção pelo Spamassassin*
15.09.04	1.537	460	76,97
16.09.04	1.688	123	93,21
17.09.04	1.831	433	80,87
18.09.04	1.409	640	68,77
19.09.04	1.309	618	67,93
20.09.04	1.920	382	83,41
21.09.04	1.754	421	80,64
22.09.04	1.253	400	75,80

Pelos dados da Tabela 1, considerando-se uma média de 80 usuários que existem na Embrapa Informática Agropecuária, tem-se uma média de 25 *spams*/dia/usuário que o sistema consegue reter, isto é, se os *spams* citados passassem, cada usuário receberia em média 25 *spams*/dia a mais.

Após a coleta dos dados da Tabela 1, em setembro, outros filtros usando expressões regulares (Procmail Org., 2005b) foram criados e assim a quantidade de *spams* que iam sendo retidos aumentava, visto que os filtros novos, à medida em que eram criados, retinham mais *spams*. Uma amostra deste comportamento pode ser vista na Tabela 2.

Tabela 2. Quantidade de *spams* retida pelo sistema de mensagens em abril de 2005.

Dia	*Spamassassin*	*Filtros internos do Procmail*	*% de retenção pelo Spamassassin*	*% de retenção pelos filtros internos do Procmail*
01.04.05	199	1.881	9,57	90,43
02.04.05	36	2.460	1,44	98,56
03.04.05	18	2.027	0,88	99,12
04.04.05	72	2.189	3,18	96,82
05.04.05	74	2.490	2,89	97,11
06.04.05	88	1.979	4,26	95,74
07.04.05	103	2.352	4,20	95,80
08.04.05	101	2.418	4,01	95,99

Pelos dados da Tabela 2, considerando-se uma média de 80 usuários que existem na Embrapa Informática Agropecuária, tem-se uma média de 29 *spams*/dia/usuário que o sistema consegue reter, isto é, se os referidos *spams* passassem, cada usuário receberia em média 29 *spams*/dia a mais.

Observe que os filtros internos do *procmail*, conforme a Tabela 2, retinham mais de 90% das mensagens, melhorando assim o desempenho do sistema, visto que mais *spams* foram retidos, em comparação com a Tabela 1, e menos processos do Spamassassin eram necessários para reter *spams*, visto que a maioria destes eram retidos agora pelos filtros do *procmail*.

Embora o número de *spams* retidos tenha aumentado, o número de *false positive* também, principalmente devido a *sites* mal configurados (problemas de DNS), que tinham erros nos cabeçalhos das mensagens ou ainda devido a *sites* legítimos que estavam nas listas negras de *sites* sobre o assunto (relays.ordb.org, dnsbl.sorbs.net, sbl.spamhaus.org, sbl-xbl.spamhaus.org e outros). Chegou-se à conclusão que filtros para análise de mensagens tem suas limitações. Além de, por várias razões, reterem mensagens legítimas, não conseguem reter os *spams* totalmente. Além disso, sempre é necessária a intervenção do suporte computacional para configurar novas regras ou recuperar mensagens retidas indevidamente.

Devido ao comportamento do Spamassassin e dos filtros citados anteriormente, buscou-se outras alternativas de bloqueio de *spams*. Um ótima alternativa foi a instalação de um gray list (Dreifus, 2005). A idéia deste *software* é rejeitar a mensagem na primeira vez que esta chega ao servidor, emitindo uma mensagem do tipo "451 4.7.1 Please try again later (TEMPFAIL)". A maioria das aplicações que enviam *spams* em massa não tentarão enviar novamente a mensagem. Assim, uma grande quantidade de *spam* é retida pelo *software* de grey list sem gerar *false positive*. Se a mensagem for legítima, o servidor de mensagens do remetente deverá tentar enviar a mensagem novamente. Quando assim o fizer, a mensagem não será mais bloqueada pelo *software* de grey list e então continuará no processo de envio ao destinatário. Este *software* pode ser usado com qualquer MTA (Postfix, Sendmail, Exim, Qmail) e os resultados obtidos na Embrapa Informática Agropecuária foram muito bons, diminuindo em grande quantidade o número de *spams* que ainda passavam. Este sistema foi instalado em maio de 2005 e seus resultados podem ser vistos na Tabela 3.

Tabela 3. Quantidade de *spams* retida pelo sistema de mensagens em junho de 2005.

Dia	*Mensagens retidas pelo Spamassassin*	*Mensagens retidas pelos filtros internos do Procmail*	*% de retenção pelo Spamassassin*
01.06.05	32	1.272	2,45
02.06.05	41	1.072	3,68
03.06.05	93	1.310	6,63
04.06.05	60	791	7,05
05.06.05	45	828	5,15
06.06.05	54	910	5,60
07.06.05	95	1.058	8,24
08.06.05	75	946	7,35

Observe que os *spams* retidos pelos filtros do *procmail* e pelo Spamassassin diminuíram, mostrando assim a validade de se usar o *software* de grey list, isto é, uma quantidade razoável de *spams* já é retida antes mesmo de passar pelos filtros citados (Spamassassin, TMDA, filtros do *procmail*, etc.). A média de *spams* que iriam para o usuário, caso o Spamassassin e os filtros do *procmail* não funcionassem seria 14 *spams*/dia/usuário a mais, considerando-se 80 usuários.

Em junho de 2005, foi instalado o *software* TMDA. Este *software* foi configurado em *procmailrc* e era chamado antes dos filtros usando expressões regulares e o Spamassassin. Assim, poderia ser quantificado quão eficiente é a ação do TMDA analisando a quantidade de *spams* que os filtros que usam expressões regulares e o Spamassassin conseguem reter, os quais são invocados após o TMDA.

O resultado da Tabela 4 indica que algumas mensagens ainda passam pelo TMDA sem serem retidas. Com os dados citados, a média de *spams* é de 111/1 dia/80 usuários, isto é, 1,4 *spams*/dia/usuário. Desta forma, o desempenho do TMDA foi muito bom, visto que sozinho o TMDA conseguiu reter a grande maioria dos *spams* e, desta forma, trouxe satisfação ao usuário.

Tabela 4. Quantidade de *spams* retida pelo sistema de mensagens em agosto de 2005.

Dia	*Mensagens retidas pelo Spamassassin*	*Mensagens retidas pelos filtros internos do Procmail*	*% de retenção pelo Spamassassin*
25.08.05	0	200	0,0
26.08.05	0	147	0,0
27.08.05	0	53	0,0
28.08.05	0	238	0,0
29.08.05	0	51	0,0
30.08.05	0	56	0,0
31.08.05	0	99	0,0
01.09.05	0	43	0,0

Foram colhidas opiniões dos usuários sobre esta combinação (Grey List + TMDA) e foi unânime a opinião de que o número de *spams* abaixou sensivelmente, levando a crer que o TMDA também reteve *spams* que os filtros que usam expressões regulares e o Spamassassin não barravam. Desta forma, o número de *spams* por usuário caiu sensivelmente.

Um detalhe muito importante sobre o TMDA é que o próprio usuário pode inserir endereços nas listas branca e negra, e também recuperar as mensagens legítimas. Para isso o usuário deve usar a interface *web* do TMDA, ilustrada na Fig. 1. Isso trouxe um grande benefício e satisfação ao usuário visto que o número de *spams* por usuário diminuiu muito e também que o usuário sempre pode intervir no sistema, não dependendo mais dos administradores de rede para recuperar mensagens ou inserir endereços eletrônicos nas listas branca ou negra. O usuário também pode fazer suas operações fora da unidade, desde que o serviço (acesso ao TMDA pela *web*) esteja configurado para ser acessado externamente.

Para os administradores de rede, o TMDA facilitou o serviço, evitando esforços com demanda de usuários quanto à recuperação de mensagens, inserção de endereços em lista branca ou negra.

Conclusões

É extremamente difícil acabar com os *spams*, mas existem maneiras para atenuar consideravelmente o número deles por usuário. Na experiência que tivemos na Embrapa Informática Agropecuária, observou-se que a solução para combate aos *spams* é um conjunto de medidas. Assim, a união da lista cinza (Grey List) com o TMDA, e também com outros filtros (expressões regulares, se estiver usando o *procmail,* ou regras para o arquivo main.cf se estiver usando o MTA postifx ou outros filtros específicos para cada MTA) diminui consideravelmente a quantidade de *spams* entregues por dia aos usuários.

Quanto à comparação do TMDA com o Spamassassin, observa-se que o TMDA é muito superior, tanto em termos de resultado, conforme demonstrado nas Tabelas citadas, quanto em termos de gerenciamento por parte do usuário, visto que o TMDA tem uma interface *web* que permite inserir endereços na lista branca ou negra, recuperar mensagens cujos remetentes não responderam ao desafio, alterar parâmetros do funcionamento do TMDA (como, por exemplo, o número de dias que a mensagem fica de quarentena, o conteúdo da mensagem que vai como desafio para o remetente, etc.). O TMDA também facilita a vida do administrador de sistemas, diminuindo o trabalho de administração, que é transferido para o usuario.

O problema relativo a falsos positivos trouxe insatisfação para o usuário e trabalho extra para o suporte computacional. O TMDA eliminou os falsos positivos e trouxe satisfação para o usuário, que analisa as mensagens pendentes (aquelas cujos remetentes não responderam ao desafio) para recuperar mensagens legítimas e assim elimina o trabalho do suporte computacional de recuperar mensagens (e também de ficar inserindo endereços em listas branca e negra).

Sobre o Spamassassin, este tem como vantagem o fato do usuário não ter que configurar nada, porém, ele é limitado quanto à capacidade de reter *spams*. Além desta limitação, o Spamassassin retém mensagens legítimas. Desta forma, sobra para o suporte computacional a tarefa do gerenciamento de *spams*, visto que ele tem que procurar soluções para reter razoável quantidade de *spams* que o Spamassassin deixa passar e também tem que ficar recuperando mensagens retidas indevidamente (falsos positivos), causando transtornos para o suporte computacional e também para o usuário, visto que este depende do suporte para a recuperação das mensagens.

Referências Bibliográficas

THE APACHE SOFTWARE FOUNDATION. **The Apache SpamAssassin Project**. Disponível em: <http://spamassassin.apache.org/>. Acesso em: set. 2005.

BAYES e o spam. Disponível em <http://www.propus.com.br/articles/alt/1/1.html>. Acesso em: out. 2005.

DREYFUS, E. **Milter-greylist home page**. Disponível em: <http://hcpnet.free.fr/milter-greylist/>. Acesso em: out. 2005.

NARCISO, M. G. **Uma solução para melhoria de desempenho para servidores de correio eletrônico com antispam**. Campinas: Embrapa Informática Agropecuária, 2005. 5 p. (Embrapa Informática Agropecuária. Comunicado Técnico, 65). Disponível em: <http://www.cnptia.embrapa.br/modules/tinycontent3/content/2004/comtec65.pdf>. Acesso em: out. 2005.

PROCMAIL ORG. **Procmail home page**. Disponível em: <http://www.procmail.org>. Acesso em: set. 2005a.

PROCMAIL ORG. **Procmail tips**. Disponível em: <http://pm-doc.sourceforge.net/pm-tips.html>. Acesso em: out. 2005b.

SENDMAIL CONSORTIUM. **Sendmail home page**. Disponível em <http://www.sendmail.org>. Acesso em: set. 2005.

SOURCEFORGE.NET. **Bogofilter home page**. Disponível em <http://bogofilter.sourceforge.net/>. Acesso em: out. 2005a.

SOURCEFORGE.NET. **SourceForge.net**: DSPAM anti-spam agent. Disponível em: <http://sourceforge.net/projects/dspam>. Acesso em: out. 2005b.

TMDA. **Tagged Message Delivery Agent (TMDA) homepage**. Disponível em: <http://tmda.net>. Acesso em: set. 2005a.

TMDA. **TMDA-CGI**: what is it? Disponível em: <http://tmda.net/tmda-cgi/>. Acesso em: set. 2005b.

UOL. **UOL - o melhor conteúdo**. Disponível em: <http://www.uol.com.br>. Acesso em: out. 2005.

Comunicado Técnico, 68

Ministério da Agricultura, Pecuária e Abastecimento

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Embrapa Informática Agropecuária
Área de Comunicação e Negócios (ACN)
Endereço: Caixa Postal 6041 - Barão Geraldo
13083-970 - Campinas, SP
Fone: (19) 3789-5743
Fax: (19) 3289-9594
e-mail: sac@cnptia.embrapa.com.br

1ª edição on-line - 2005