Controle de SPAM baseado em pré-detecção da vulnerabilidade de Mail Relay

ISSN 1518-5974

Andrey Vedana Andreoli <andrey@penta.ufrgs.br>
Leandro Márcio Bertholdo <berthold@penta.ufrgs.br>
Liane Margarida Rockenbach Tarouco <liane@penta.ufrgs.br>

Ponto de Presença da RNP no Rio Grande do Sul (PoP-RS)
Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul
Computer Emergency Response Team of RS (CERT-RS)

Resumo

Este artigo descreve as atividades desenvolvidas junto ao CERT-RS / POP-RS no tratamento de ocorrências de SPAM. Como metodologia de ação, buscou-se criar um sistema de pré-detecção de hosts vulneráveis a mail relay que são os maiores amplificadores de SPAM por toda a Internet. Relatam-se aqui as experiências e resultados obtidos ao longo de um ano de utilização deste sistema.

^

1. Informações gerais

Desde os primórdios da Internet o leque de serviços utilizados na rede tem aumentado consideravelmente. Nesse contexto, alguns destes serviços têm sido amplamente utilizados e, hoje, já são comuns à maioria dos usuários desta rede mundial. Alguns exemplos que podemos citar como serviços bastante popularizados são a world wide web e o e-mail, entre outros. Neste artigo, será dado enfoque ao serviço de e-mail, com um panorama geral deste serviço em relação a problemas enfrentados atualmente, em especial o caso do SPAM e suas formas de prevenção nos grandes backbones.

Logo no surgimento deste serviço, o número de usuários com endereço eletrônico era muito pequeno e era possível enviar mensagens contendo apenas texto. Em seguida, conforme foram feitas extensões que permitiam o envio de arquivos binários, áudio e vídeo, entre outros, este serviço apresentou um crescimento com velocidade muito maior que o esperado. Pode-se dizer que, conforme a praticidade do serviço foi aumentando, ele foi se tornando mais popular e mais difundido a toda a comunidade da Internet. No Ponto de Presença RNP do Rio Grande do Sul (PoP-RS), o tráfego de e-mail representa algo em torno de 5% do total utilizado pelas instituições conectadas.

Este dado é obtido mediante a utilização do recurso do Netflow [(1)] , presente nos equipamentos de rede do POP-RS.

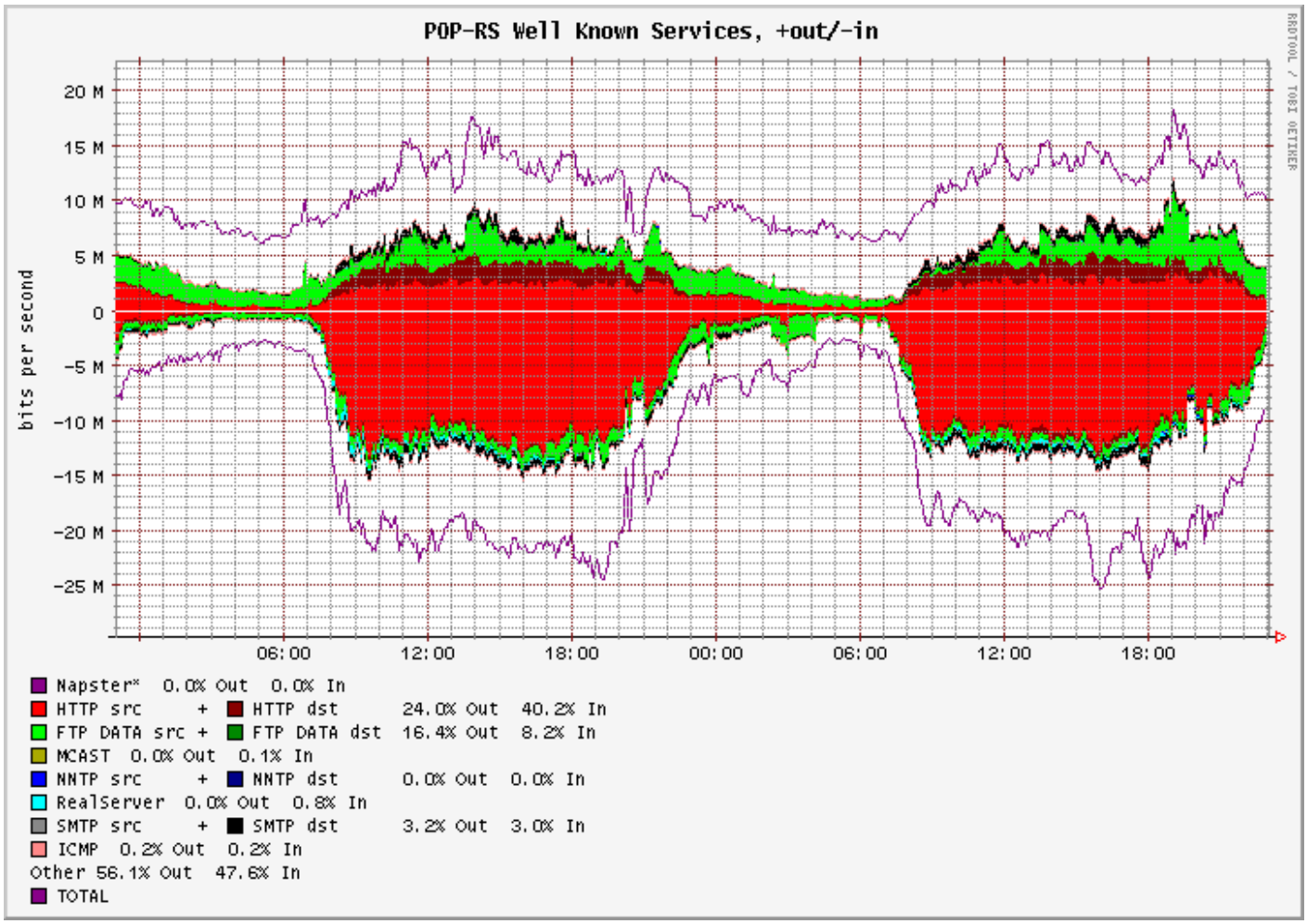

Figura 1 - Gráfico do tráfego do PoP-RS gerado pelo Netflow

Os usuários deste serviço começaram a divulgar seus endereços, tornando-os comuns em homepages ou em cartões de visita. Essa informação passou a ser usada como mais uma forma de contato, sendo muitas vezes até identificada como mais eficiente que o próprio serviço de correio comum. Neste ponto, começou a surgir o popular SPAM, versão eletrônica da disseminada e discutível prática de envio propagandas e mala-direta via correio convencional. Diversos motivos facilitam o encaminhamento deste tipo de propaganda via e-mail e não via correio postal, dentre eles:

- custo praticamente zero para envio de milhares de mensagens;
- facilidade na obtenção de vastas listagens de e-mails de usuários por toda a Internet;
- existência de programas que automatizam a tarefa de envio de e-mails "em massa";
- existência de servidores SMTP com *relay* aberto, permitindo que sejam utilizados para envio de mensagens a partir de qualquer host na Internet.

A ocorrência de SPAM tem sido cada vez maior e tem se tornado mais inconveniente. Alguns dados que reforçam a gravidade da situação são, por exemplo, que cada usuário da Internet recebeu em média 571 e-mails não solicitados durante o ano de 2001 e a projeção é de que esse número suba para 1500 em 2006, de acordo com a empresa de pesquisa Jupiter Media Metrix, de Washington/EUA. Outro dado é que as empresas da Inglaterra vêm perdendo cerca de 4,8 bilhões de dólares devido a problemas com SPAM e pornografia. Essa conclusão baseia-se no fato de que pelo menos 42% da força de trabalho britânica trabalha com equipamentos computacionais e que são perdidos cerca de 10 minutos diários para se livrar de e-mails inúteis não solicitados em meio a mensagens que realmente são pertinentes.

Tudo isso está se tornando tão problemático que o governo federal norte-americano, por exemplo, pretende ir pela primeira vez atrás dos "*spammers*", como são chamados os responsáveis pela disseminação de SPAM.

Com as primeiras ocorrências de SPAM, estas tentativas começaram a ser tratadas como incidentes de segurança, sendo encaminhados aos grupos de segurança responsáveis pelos domínios envolvidos. Isso quer dizer que, ao enviar milhares de e-mails, o servidor SMTP origem pode ser facilmente descoberto e serem tomadas as devidas providências para evitar que novos SPAMs sejam enviados. Infelizmente, as implementações de softwares de SMTP mais antigas não trataram de evitar uma vulnerabilidade conhecida atualmente como *mail relay*, descrita a seguir.

1 - Netflow é um aplicativo presente em equipamentos de rede, como roteadores Cisco, que permite examinar, logar e contabilizar pacotes segundo os dados contidos no seu cabeçalho. O gráfico em questão é gerado pelos softwares cflow [CFL01], flowscan, netflow [NET01] e RRDTool [RRD01].

^

2. A vulnerabilidade de mail relay

O seguinte fluxo de mensagens caracteriza a exploração da vulnerabilidade de *mail relay*:

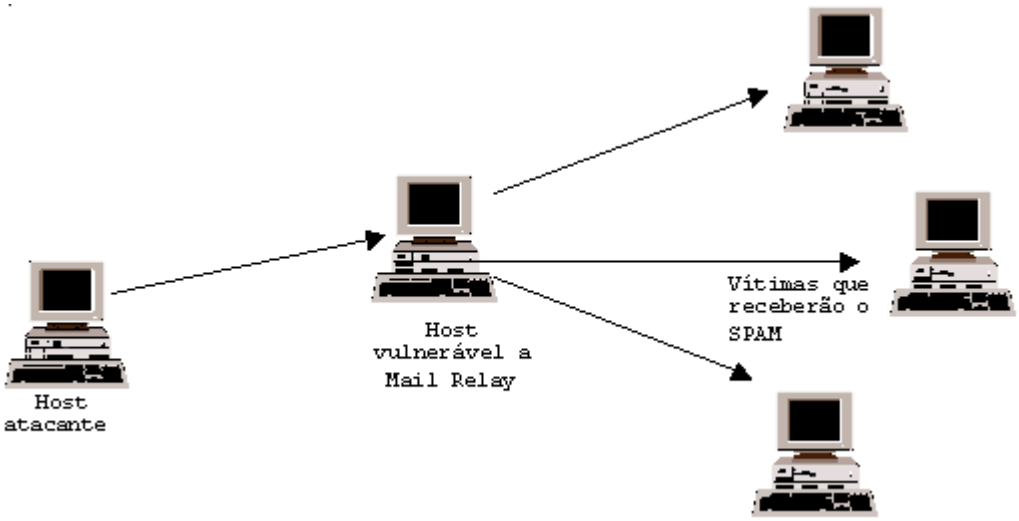

Figura 2 - Representação de envio de SPAM utilizando a vulnerabilidade de *mail relay*

Como pode ser visto na figura, ao invés do *spammer* (host atacante) fazer o envio a partir do servidor SMTP do seu domínio, ele utiliza um servidor de outro domínio (no caso, a vítima) ou, ainda, utiliza em paralelo *n* servidores a fim de enviar a todos os destinatários o que ele desejar. Se o atacante tiver domínio sobre o servidor SMTP do domínio da vítima, o envio será ainda maior se o host tiver um link rápido e recursos de CPU disponíveis. Infelizmente, esta situação acaba não somente gerando problemas aos destinatários das mensagens de SPAM, mas também à vítima do servidor SMTP utilizado que, além de ter seus recursos usados para o ataque, terá que responder por todas as reclamações provenientes do envio dos SPAMs, pois a origem do envio destas mensagens será o servidor SMTP da vítima, e não do atacante.

Uma forma de proteção contra o recebimento a partir destes *hosts* foi a criação de bases de dados on line que possuem uma listagem de todos os *hosts* que tiveram reclamações de SPAM. Estas bases de

dados são utilizadas por uma grande faixa de servidores na Internet para bloquear e-mails vindos de hosts que já tiveram registros de reclamações de SPAM. Isso pode gerar problemas muito maiores. Por exemplo, no caso de um servidor corporativo que possui esta vulnerabilidade, todos os e-mails, inclusive os enviados por usuários legítimos, seriam recusados.

Atualmente, os pacotes já oferecem recursos para, facilmente, fazer esse controle de *relay*. Isso muda um pouco a situação anterior, decorrente das próprias limitações dos pacotes. Agora surge uma nova responsabilidade do administrador do servidor, que deve fazer corretamente esta configuração e fazer bom uso destes recursos. Esse fato não diminuiu a incidência de SPAMs de forma muito significativa. O problema, aqui, é que nem todos os administradores se conscientizaram da necessidade de efetuar as devidas correções e planejamentos para evitar a exploração desta vulnerabilidade.

Assim sendo, algo deve ser feito afim de que o número de SPAMs seja minimizado e que, de alguma forma, esta situação seja revertida. Um dos recursos utilizados, que tem ajudado na entrada de SPAMs em domínios, é a implementação de filtros, que acabam bloqueando mensagens com determinados tipos de arquivos anexados ou por algum campo das mensagens de e-mail, como *sender* e subject, entre outros. Esta solução tem auxiliado muito nos resultados para minimizar o RECEBIMENTO de SPAMs no próprio domínio. Mas o objeto principal deste artigo é relatar a experiência feita na prevenção do ENVIO de SPAMs, ou seja, na ocorrência de *relays* abertos em grandes backbones.

^

3. Prevenção desta vulnerabilidade em grandes backbones

Como contexto dessa experiência apresentamos a Rede Tchê, que é a rede estadual do Rio Grande do Sul, constituída por instituições acadêmicas, públicas e escolas, totalizando mais de 40 grandes instituições interconectadas, com links entre 512Kbps e 100 Mbps. Pensou-se que além de sugerir que as instituições implementassem filtros, como os descritos acima, poderia ser feito algo para evitar que *hosts* pertencentes a esta rede fossem utilizados indevidamente para *relay*. Tratando-se de um conjunto de cerca de 60.000 IPs (se forem contabilizados todos os blocos alocados), surgiu a idéia de fazer um controle PREVENTIVO de *relays* abertos e não apenas aguardar que os incidentes fossem acontecendo para tomar as providências e acertar as configurações.

Para o teste de *hosts* individuais, já existem scripts e sites que o executam de forma simples e prática. Mas o desafio, neste caso, foi de pensar em uma solução que fizesse essa análise em todos os *hosts* da Rede Tchê, de forma automatizada e periódica.

^

4. Implementação da Ferramenta para testes

Depois de identificar os módulos e funcionalidades necessárias, partiu-se para a implementação da solução nas linguagens C [SCH96] e PERL [PER01] para plataformas UNIX. Tudo foi dividido em módulos para tornar cada parte reutilizável em outros testes. A estrutura de módulos ficou definida da seguinte forma.

- **Módulo de entrada de dados:**

Responsável pela análise das faixas *classfull* ou *classless* pertencentes a cada instituição e geração dos IPs de cada faixa, como demonstrado abaixo:

Exemplo de arquivo de entradas hipotético:

Universidade A
192.168.10.240/28

Exemplo dos arquivos de saída deste módulo:

Universidade_A.tmp

192.168.10.240
192.168.10.241
192.168.10.242
192.168.10.243
...

- **Módulo de teste de ping:**

  Responsável por verificar todos os IPs pertencentes a cada faixa atribuída para cada instituição e, através do teste de ping, descobrir quais *hosts* "ativos" devem ser testados posteriormente. Esse módulo pode ser visto como um otimizador, já que ele poderia até ser excluído desta solução. Mas sua importância justifica-se, já que reduz o número de testes apenas aos hosts que estão ativos na rede. Dependendo da ocupação de cada faixa, esse módulo pode tornar a execução muito mais eficiente. Para executar tal tarefa, foi utilizado o programa de domínio público chamado FPING que faz a tarefa de teste de ping em paralelo, tornando a execução muito mais rápida. Para ser implementado neste módulo, foram feitas algumas adaptações no arquivo de saída deste programa para uma correta interpretação nos próximos módulos.

- **Módulo de teste da vulnerabilidade de *Mail Relay*:**

  Este é o módulo mais importante do teste, pois é nele que é feito de fato o teste de *mail relay*. Para o teste em um único *host*, foi obtido um pacote de segurança no site http://www.freeBSD.org que inclui um script em PERL que faz a conexão com determinado *host* na porta 25 (SMTP), faz o teste de *relay* e exibe na tela os eventos do teste de forma detalhada [BSD01]. Este script sofreu algumas modificações em sua implementação para criar um arquivo de log de teste se o *host* for vulnerável e para não criar nenhum arquivo de log se o teste tivesse algum resultado diferente (não conseguir estabelecer conexão na porta 25, o host não apresentar vulnerabilidade, entre outros.). Sabendo que este teste seria repetido para milhares de *hosts*, e não apenas para alguns poucos, implementou-se uma rotina que dispara um teste para cada *host* de forma paralela. Esse paralelismo pode ser previamente configurado para disparar *n* testes a cada segundo, onde *n* varia de acordo com os recursos de CPU e memória disponíveis no *host* que será usado para os testes.

Nos testes feitos adotou-se *n* = 2, ou seja, 2 testes disparados por segundo, totalizando 120 *hosts* analisados por minuto, fazendo pelo menos 7200 testes em uma hora, executando até 120 processos simultâneos no *host*. O paralelismo foi implementado usando os recursos de FORK da linguagem PERL. Por não ser uma aplicação leve, exige-se que, esses testes sejam feitos a partir de um *host* com recursos de CPU generosos e memória RAM de pelo menos 512 MB, já que para cada instância do teste disparada é carregado na memória o interpretador PERL. Nos testes feitos na Rede Tchê, foi utilizada uma estação R-50 IBM com 1GB de memória RAM.

- **Módulo de apresentação de resultados e logs:**

  Uma vez aplicados os testes em todos os *hosts* da rede, é necessário que seja gerada uma listagem dos *hosts* vulneráveis de cada instituição, juntamente com o log comprovando o teste e a exploração do serviço. Essa saída é gerada em formato pré definido no site do CERT-RS em um diretório cujo acesso é restrito aos administradores das instituições da Rede Tchê. Essa restrição de acesso é feita com o intuito de evitar o vazamento de informações e uma possível exploração mal intencionada das redes em questão.

  Um exemplo de log de teste cujo host se mostrou vulnerável é mostrado abaixo:

  Connecting to xxx.yyy.zzz.xxx. ...
  <<< 220 SMTP.dominio.tche.br ESMTP Sendmail 8.8.8/8.8.8; Thu, 12 Jul 2001 16:19:48 -0300 (EST)
  >>> HELO beta.pop-rs.rnp.br
  <<< 250 SMTP vitima.com.br Hello atacante.com.br [xxx.xxx.xxx.xxx], pleased to meet you
  >>> MAIL FROM:
  <<< 250 ... Sender ok
  >>> RCPT TO:
  <<< 250 ... Recipient ok
  >>> DATA
  <<< 354 Enter mail, end with "." on a line by itself
  >>> (message body)
  <<< 250 QAA09785 Message accepted for delivery
  >>> QUIT
  <<< 221 SMTP vitima.com.br closing connection
  rlytest1.20: relay accepted - final response code 221

As informações de IP e nome do *host* testado foram omitidas para evitar a exposição do *host* vulnerável.

^

5. Acompanhamento pós-testes dos hosts vulneráveis

Uma vez que os testes foram feitos e os resultados disponibilizados, foi feito um contato direto com os administradores das redes que possuíam *hosts* vulneráveis a fim de esclarecer dúvidas e dar orientações sobre a configuração que deveria ser feita. A maioria dos administradores acabou fazendo as devidas configurações e novos testes eram feitos até verificar que a configuração tinha sido corrigida.

No caso da vulnerabilidade não ser corrigida dentro do prazo especificado, alguns *hosts* foram filtrados nos roteadores de distribuição até que as devidas providências fossem tomadas.

^

6. Resultados obtidos na utilização da ferramenta em 2001

Durante o ano de 2001 foram feitos testes periódicos. Grande parte deles foi aplicada entre períodos de 3 meses. Abaixo pode-se verificar, pela figura 3, o gráfico que mostra o número total de *hosts* vulneráveis a *Mail Relay* detectados em cada teste:

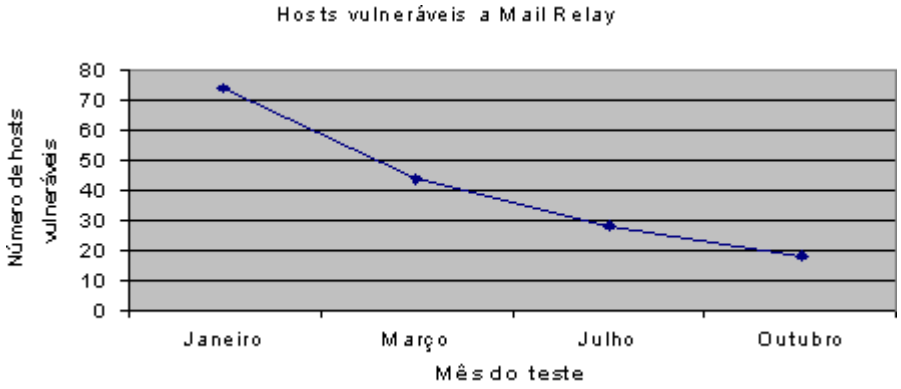

Figura 3 - *Hosts* vulneráveis a *mail relay* durante o ano de 2001

Como se pode verificar no gráfico, o número de *hosts* vulneráveis a *mail relay* diminuiu consideravelmente com a implantação deste sistema de prevenção a esta vulnerabilidade.

Entre 1998 e 2001, o CERT-RS - responsável pelo tratamento de incidentes de segurança da Rede Tchê - recebeu diversas notificações sobre utilização de *hosts* na rede estadual que estavam sendo utilizados para *relay* de terceiros. A figura 4 ilustra o número de ocorrências de incidentes notificados ao final de cada ano, ressaltando que os testes foram iniciados durante o ano de 2001.

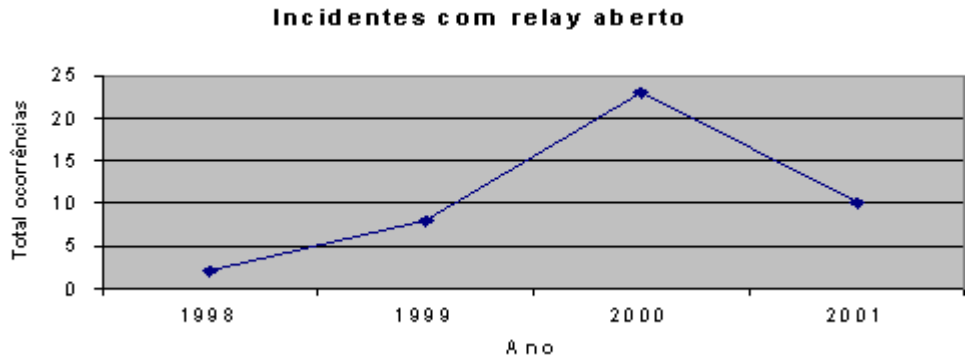

Figura 4 - Total de incidentes com *relay aberto* entre 1998 e 2001

Um dado importante destes incidentes é que em 80% dos casos de *hosts* vulneráveis, baseados nos testes feitos durante o ano de 2001, os sites utilizados para envio de SPAM já haviam sido alertados e divulgados como possuindo *hosts* vulneráveis com pelo menos um mês de antecedência pelo CERT-RS. Os demais 20% de *hosts* vulneráveis não foram contemplados já que a vulnerabilidade foi explorada

logo após a abertura indevida do *relay*. Isso poderia ser resolvido aplicando testes com mais frequência, aumentando com isso a granularidade dos resultados.

Em relação ao ano de 2000, comparando o total de incidentes envolvendo *relay* abertos ao final de cada ano, observou-se que ocorreu uma diminuição de 50% nos casos de utilização de *relays* abertos por terceiros.

^

7. Conclusões

Como pontos positivos destes dados, pode-se destacar que a maioria dos *hosts* vulneráveis é identificada antes de um ataque externo ou utilização indevida, com isso facilitando sua manutenção por parte dos administradores responsáveis. Isso significa que, uma vez descoberto o *relay* aberto, com uma rápida ação de reparo em sua configuração, dificilmente algum host será usado por terceiros para *relay*. Se em todos os grandes backbones isso também for atingido, os usuários somente conseguirão utilizar os servidores SMTP de seus próprios domínios para SPAM , estes serão muito mais facilmente detectados e haverá maiores chances de punir os responsáveis.

^

8. Próximos passos do projeto

Como próximos passos deste *scan*, espera-se que neste ano de 2002 seja feito um acompanhamento mais rígido com os administradores dos *hosts* vulneráveis a fim de obter uma ação mais rápida no fechamento de *relay*. Também estão sendo criadas políticas rígidas de filtragem no caso de demora excessiva no tratamento desse incidente. Outra possibilidade é o aumento da freqüência dos testes e expansão para outras redes, dependendo de um acordo prévio. O aumento da freqüência de testes de uma peridiocidade trimestral para mensal certamente evitará ações rápidas de spammers.

^

9. Esclarecimentos técnicos sobre a vulnerabilidade de mail relay

Como foi relatado no início deste artigo, qualquer servidor de e-mail pode fazer uso de uma lista que, em tempo real, fornece a listagem de *hosts* com *relay* aberto. Esta listagem é conhecida como RBL e pode ser encontrada em http://mail-abuse.org/rbl/. O mesmo recurso pode ser utilizado em http://work-rss.mail-abuse.org/rss/index.html. Adicionalmente, existem outros sites, como http://www.ordb.org/, que possuem outras modalidades de listas.

Também existe a possibilidade de efetuar o teste de *relay* para alguma máquina ou algum servidor específico. Uma das formas é pela URL: http://www.abuse.net/relay.html ou ainda em http://www.ordb.org/submit/. No Brasil, o site AntiSPAM/BR (http://www.spambr.org/) oferece informações sobre como denunciar SPAMs; técnicas de bloqueio em roteadores Cisco e Cyclades, bem como no Sendmail e MS Exchange; além de links para programas e materiais sobre o assunto.

Por fim, a própria home page do CERT-RS oferece, em http://www.cert-rs.tche.br/docs_html/relay/, um material, em português, sobre o assunto.

No caso de inclusão de um servidor nestas listas on line, depois de acertar as devidas configurações para fechamento de *relay*, em alguns casos é necessário contato via telefone ou e-mail para solicitar a remoção do *host*. Este é o caso da lista RBL - REALTIME BLACKHOLE LIST - cujo acesso às informações necessárias pode ser feito a partir de: http://www.mail-abuse.org/rbl/removal.html. Em outros sistemas, como é o caso do ORDB (Open Relay Database), é necessário acessar o site e submeter o *host* vulnerável a fila de testes e, no caso do sistema detectar que o *host* não está mais vulnerável, a remoção da lista é feita automaticamente.

Outro recurso interessante que tem sido amplamente utilizado é o SPAMCOP (http://spamcop.net). Trata-se de um mecanismo que permite o envio automatizado de reclamações de recebimento de SPAM aos domínios envolvidos. Neste caso, a mensagem recebida, juntamente com seu *header*, pode ser submetida e é feita uma análise desse conteúdo pelo próprio sistema, que fornece dados como e-mail dos responsáveis pelo domínio e cria um texto base relatando a reclamação, solicitando ao usuário apenas a confirmação do envio da reclamação. Também são fornecidos outros serviços, alguns deles comerciais.

^

10. Download da ferramenta

A ferramenta encontra-se disponível no site do CERT-RS, na seção Tools (http://www.cert-rs.tche.br/tools). Existe também no site um Manual de Utilização que busca dar orientações e esclarecimentos sobre a instalação e utilização da ferramenta. A leitura do manual é obrigatória já que a ferramenta depende da correta configuração de parâmetros de acordo com o teste desejado. Problemas, sugestões, esclarecimentos poderão ser enviados para teste-relay@pop-rs.rnp.br.

^

Referências bibliográficas

[RFC01] LINDBERG, G. *Anti-Spam Recommendations for SMTP MTAs*. RFC 2505, fev. 1999. Disponível em: <http://www.ietf.org/rfc/rfc2505.txt?number=2505>. Acesso em 2002.

[NET01] CISCO. Cisco - Cisco IOS; Technologies - NetFlow. Disponível em> <http://www.cisco.com/warp/public/732/Tech/netflow/>. Acesso em 2002.

[CFL01] CISCO. Cisco Content Flow Monitor. Disponível em: <http://www.cisco.com/warp/public/cc/pd/wr2k/cflow/index.shtml>. Acesso em 2002.

[RRD01] RRD TOOL. - About RRDtool. Disponível em: <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>. Acesso em 2002.

[CER01] MAPAS TSI: Anti-relay: O que é usar a retransmissão de mail por terceiros? [Artigo sobre a vulnerabilidade de Mail Relay]. Disponível em: <http://www.cert-rs.tche.br/docs_html/relay>. Acesso em: 2002.

[BSD0] FreeBSD Ports. [Programa de teste de teste da vulnerabilidade de Mail Relay]. Disponível em: <http://www.freeBSD.org/ports>. Acesso em 2002.

[SCH96] SCHILDT, Herbert. *C Completo e Total*. São Paulo: Makron Books, c1997. 827 p.

[PER01] Perl Mongers. [Tutoriais sobre a linguagem PERL]. Disponível em: <http://www.perl.org/>. Acesso em 2002. HYPERLINK.

^