



Sobre Graylist

Uma visão rápida a respeito de Graylist e seu funcionamento aplicado a técnica anti-spam
Uniwares Anti-Spam Lab

Copyright © 1996-2007 Uniwares Ltda.

Uniwares é marca registrada de Uniwares Ltda. Todos os direitos reservados.

Todos os produtos ou serviços mencionados nessa publicação são marcas registradas de seus respectivos proprietários.

Versão desse documento: 1.2

Índice


Índice	2
Introdução	3
Como surgiu a idéia?	4
Método de ação	5
Graylist em diversas “cores”	6
Principais problemas do uso de Graylist	7
Você pode perder mensagens	7
Atraso no recebimento	7
Problemas com Mailing Lists	7
Problemas com grandes provedores	7
Conclusão	8

Introdução

O mecanismo conhecido como Graylist consiste em recusar uma conexão no momento em que a mesma é estabelecida. Dessa forma, espera-se que a conexão seja aberta novamente o que é uma característica comum dos servidores de e-mail. Já os softwares de spammers, em sua grande maioria, não tentam novamente.

Graylist é apenas um mecanismo auxiliar para combate ao spam e sua eficácia como mecanismo único é extramente baixa e questionável.

Nesse documento iremos explorar um pouco mais a respeito do funcionamento das Graylists e suas características aplicadas a spam e também a mensagens legítimas. Falaremos ainda sobre como o mercado tem adotado sua prática.

 *Nota: Para usuários do Leon Anti-Spam Server:*

O Leon possui mecanismo de Graylist desde o lançamento de sua primeira versão. Para habilitá-lo, basta assinalar a opção contida em Standard | Connections | Reject first-time connections with temporary error (Rejecting 'Stranger').

Como surgiu a idéia?

Desde o primeiro spam até os dias atuais sabemos que grande parte de seu volume é enviada por spamware. Basicamente, uma estação é infectada – muitas vezes, por um spam recebido com os mais diversos tipos de apelo que levam o usuário a clicar em determinado link o qual acaba por instalar o spamware em seu computador – nesse momento, o computador da vítima torna-se um “soldado”.

Um único computador não causaria grandes estragos e por isso a idéia dos spammers é infectar o maior número possível de computadores. Uma vez que já tenham uma quantidade razoável, podem utilizar os “soldados” para formar um verdadeiro exército e, estrategicamente, atacar diversos alvos.

Todas às vezes que a conexão com a Internet é detectada as estações infectadas informam a um ou vários servidores que estão prontas para o trabalho. O servidor envia uma mensagem principal e uma lista de destinatários para o qual a estação deve enviar spam. Por esse motivo, muitas vezes o internauta percebe que seu computador está lento – mesmo que ele esteja utilizando apenas um editor de texto. O fato é que estar conectado a Internet é tudo que o spammer precisa para utilizar um computador infectado.

Nesse momento devemos considerar que:

- A maioria esmagadora dessas infecções é feitas em computadores domésticos
- Conexões domésticas são geralmente por meio de DSL, Wireless, Cabo e dial-up – sim, ainda existe acesso discado
- Quase 100% dos endereços IPs designados a essas conexões são IPs dinâmicos
- Os spamwares são aplicações simples, sem qualquer respeito às RFCs ou qualquer política de boas práticas

Método de ação

O mecanismo de Graylist entra em ação no momento em que a conexão com o servidor de e-mail é estabelecida. Nesse momento, ao saber que se trata de uma conexão nova e desconhecida, o servidor responde com um erro com código 4xx, ou seja, erro temporário. Um mecanismo de blacklist recusaria a conexão com erro permanente 5xx e o whitelist aceitaria a conexão com mensagem 2xx. Daí vem o Graylist que é um meio termo, pois, ao enviar um erro temporário não está recusando definitivamente a conexão e simplesmente solicitando que tente mais tarde; a mesma coisa acontece quando o servidor está ocupado, com problemas temporários ou em manutenção e não pode aceitar mais conexões.

A teoria é que um verdadeiro MTA (Mail Transport Agent) irá fazer uma nova tentativa ao passo que para um spamware é mais vantajoso ganhar em volume e assim partir para outro servidor ao invés de tratar mensagens de erros. Certamente alguns spamwares mais sofisticados vão tentar a conexão novamente e, nesse caso, acabam driblando o Graylist.

Graylist em diversas “cores”

A atitude de desenvolver esse mecanismo foi totalmente independente e já foi desenvolvida diversas vezes. Embora a idéia principal seja de certa forma a mesma, alguns detalhes de implementação fazem com que um mecanismo de Graylist possa ser diferente de outro afetando sua eficiência e desempenho.

Ao analisar o funcionamento desses mecanismos ligeiramente (ou não) diferentes, devemos levantar primeiro a questão: de que forma o Graylist deve ser aplicado?

Existem diversas formas que devemos considerar. Embora exija um trabalho manual, o uso de whitelist em conjunto com Graylist pode ser uma boa saída, mas que ainda assim pode ter uma boa variação de produto para produto. Por exemplo: quais serão os dados utilizados para whitelist? Você pode optar com o Leon Anti-Spam Server - apenas como referência – por uma séria de dados para whitelist como:

- IP do remetente
- Domínio
- Rementete
- Destinatário
- Name Server (origem)

Outro fator importante que obsevamos é que os administradores têm configurado o intervalo de conexão do Graylist a seu próprio gosto, ou seja, alguns aceitam que a conexão seja feita novamente imediatamente enquanto outros solicitam 10, 15, 60, 90 minutos e até mais tempo. O fato concreto que é que é impossível para o servidor MTA entender essas mensagens de erro (que seguem junto com o erro 4xx). O aconselhável é que se permita a conexão novamente de acordo com tempo definido pelas tentativas RFC's.

E por falar em mensagens de erro, é incrível a miscelânea de mensagens de servidores SMTP. Senhores administradores, por favor, o e-mail é uma coisa global e mensagens que descrevam erros ou informações (2xx,3xx,4xx,5xx) em inglês já ajudaria bastante.

Principais problemas do uso de Graylist

O uso de um conjunto de regras anti-spam depende sempre de uma política e existem alguns pontos que devem ser considerados por aqueles que desejam utilizar o mecanismo de Graylist:

Você pode perder mensagens

A perda de mensagem pode acontecer quando, ao receber o código 4xx de erro temporário, o servidor remetente não tente a conexão novamente. Para se ter uma idéia, até meados de 2005, o Yahoo não tentava a entrega novamente – não se sabe ao certo se por política, bug ou problemas de desempenho. Felizmente essa situação já foi resolvida, mas não sabemos quantos MTAs ainda possuem essa limitação.

Atraso no recebimento

Graylist pode gerar atraso no recebimento de mensagem, podendo ser um atraso insignificante ou um atraso mais que inconveniente.

Problemas com Mailing Lists

Ao adotar o uso de Graylist, tenha em mente que poderá ter problemas com Mailings que utilizam VERP (Variable Envelop Return Paths) e BATV (Bounce Address Tag Validation) que ao modificarem, a cada envio, informações de remetente e destinatário, o mecanismo de whitelist não funcionará baseado nessas duas informações.

Problemas com grandes provedores

Algumas implementações de Graylist exigem vários fatores que devem ser iguais em cada tentativa de envio como o IP do MTA, remetente e destinatário. Este método não funciona com muitos provedores de grande porte porque na maioria das vezes eles têm diversos servidores de saída e cada tentativa pode ser feita de um servidor diferente.

Conclusão

Um planejamento adequado pode reduzir consideravelmente o número de mensagens legítimas perdidas. Se você tem diversos servidores MX, considere, por exemplo, centralizar sua base de novas conexões. Dessa forma, vai evitar que o MTA receba mensagens 4xx diversas vezes de servidores diferentes de sua rede.

Discuta com sua equipe a respeito da adoção desse mecanismo, tentem chegar a uma conclusão se possui mais benefícios que malefícios e não deixe de escrever a decisão do grupo em sua política anti-spam.

Em suma, seja prudente ao escrever a sua política e escolha o produto certo.