**E-mail de falsificação e servidor SMTP aberto**

Uma **retransmissão de e-mail aberta** ocorre com um servidor SMTP configurado de forma a permitir que qualquer pessoa, na Internet, envie um e-mail por meio dela, não apenas e-mails destinados a ou provenientes de utilizadores conhecidos. Esta costumava ser a configuração padrão em muitos servidores de e-mail; na verdade, foi a forma como a Internet foi inicialmente configurada, mas a retransmissão de e-mail aberta tornou-se impopular devido à sua exploração por spammers e worms. Muitos retransmissores foram fechados ou colocados em listas negras por outros servidores.

Em meados da década de 90, com o aumento do spam, os spammers recorreram ao reencaminhamento dos seus e-mails através de servidores de e-mail de terceiros para evitar a deteção e para explorar os recursos adicionais destes servidores de retransmissão aberta. Assim, os spammers enviavam um e-mail para o retransmissor aberto e (efetivamente) incluiam uma lista grande de cópias ocultas e, então, o retransmissor aberto retransmitiria este spam para toda a lista. Embora este processo reduzisse bastante a largura de banda disponível para os spammers (numa época histórica em que as ligações com a Internet eram limitadas), por outro lado, cada cópia de mensagem (spam) era uma cópia exata da original e, portanto, mais fácil de detetar.

Como os retransmissores de e-mail abertos não fazem nenhum esforço para autenticar o remetente de um e-mail, os retransmissores de e-mail abertos são vulneráveis a falsificações de endereço.

**Falsificação de e-mail** é a criação de mensagens de e-mail com um endereço de remetente falso.

Como os principais protocolos de e-mail não possuem nenhum mecanismo para autenticação, é comum que os e-mails de spam e phishing utilizem esta falsificação para enganar o destinatário sobre a origem da mensagem.

Quando um e-mail SMTP é enviado, a ligação inicial fornece duas informações de endereço:

* **E-MAIL DE:** - geralmente apresentado ao destinatário como o cabeçalho *Caminho de retorno:* mas normalmente não visível para o utilizador final e, por predefinição, não são realizadas *nenhumas verificações* se o sistema de envio está autorizado a enviar em nome desse endereço.
* **RCPT PARA:** - especifica em que endereço de e-mail o e-mail é entregue, normalmente não é visível para o utilizador final, mas *pode* estar presente nos cabeçalhos como parte do cabeçalho "Recebido:".

Em conjunto, estes são algumas vezes referidos como o endereço "envelope", por analogia com um envelope de papel tradicional, e a menos que o servidor receba sinais de que tem problemas com qualquer um destes itens, o sistema de envio envia o comando "DATA" e envia vários itens de cabeçalho, incluindo:

* **De:** Joe Q Doe <joeqdoe@example.com> - o endereço visível para o destinatário; mas, novamente, por predefinição, não é feita nenhuma verificação de que o sistema de envio está autorizado a enviar em nome desse endereço.
* **Responder a:** Jane Roe <Jane.Roe@example.mil> - igualmente não verificado

e às vezes:

* **Remetente:** Jin Jo <jin.jo@example.jp> - também não verificado

O resultado é que o destinatário do e-mail vê o e-mail como tendo vindo do endereço no cabeçalho *De*: e, se responder ao e-mail, ele irá para o endereço apresentado no cabeçalho *De:* ou *Responder a:* - mas nenhum destes endereços é geralmente fiável, portanto, as mensagens de retorno automáticas podem gerar retrodifusão.

Embora a falsificação de e-mail seja eficaz ao forjar o endereço de e-mail, o endereço IP do computador que envia o e-mail geralmente pode ser identificado nas linhas "Recebido:" no cabeçalho do e-mail. Em muitos casos, é provável que seja um terceiro inocente infetado por malware que está a enviar o e-mail sem o conhecimento do proprietário.

*Fonte: https://en.wikipedia.org/wiki/Open\_mail\_relay; https://en.wikipedia.org/wiki/Email\_spoofing.*