**Usurpation d’adresse électronique et serveur SMTP ouvert**

Un **serveur relais ouvert** est un serveur SMTP configuré de telle sorte que n’importe qui sur Internet peut s’en servir pour envoyer un mail, qui ne se limite pas à du courrier électronique destiné à ou provenant d’utilisateurs connus. De nombreux serveurs de courrier électronique étaient par défaut configurés de cette manière ; en fait, c’est sous cette forme qu’Internet a été instauré au départ, mais les internautes se sont détournés des serveurs relais ouverts qui étaient vulnérables aux spams et aux vers. Nombre d’entre eux ont été fermés ou placés sur liste noire par d’autres serveurs.

Vers le milieu des années 1990, le spam étant en plein essor, les spammers se sont résignés à transférer leurs mails via des serveurs de tierces parties pour éviter d’être détectés et exploiter les ressources supplémentaires de ces serveurs relais ouverts. Ainsi, ils envoyaient un mail au relais ouvert et inclure une longue liste de destinataire en copie blind, et le relais ouvert relayait le spam à toute la liste. Cela réduisait certes grandement les besoins en bande passante pour les spammers alors que les connexions Internet étaient limitées, mais en revanche, chaque spam devait être une copie exacte, ce qui le rendait donc facile à détecter.

Les relais ouverts ne faisant rien pour authentifier l’expéditeur d’un mail, ils sont vulnérables à l’usurpation d’adresse.

**L’usurpation d’adresse mail** consiste à créer des messages mails avec une fausse adresse d’expéditeur créée de toute pièce.

Les protocoles centraux de la messagerie électronique n’ayant pas de mécanisme d’authentification, les mails de spam et de hameçonnage utilisent couramment l’usurpation d’adresse pour tromper le destinataire quant à l’origine du message.

Quand un courrier SMTP est envoyé, la connexion initiale fournit deux informations concernant l’adresse :

* **MAIL FROM:** - généralement présenté au destinataire comme l’en-tête *Return-Path:*, mais qui n’est en principe pas visible pour l’utilisateur final, et par défaut aucun contrôle n’est effectué pour s’assurer que le système expéditeur est autorisé à envoyer au nom de cette adresse ;
* **RCPT TO:** - spécifie à quelle adresse mail le mail a été envoyé, normalement n’est pas visible pour l’utilisateur final *mais* peut être présente dans les en-têtes dans l’en-tête « Received: ».

Ces deux informations ensemble constituent ce que l’on appelle parfois l’enveloppe d’adressage, par analogie avec une enveloppe traditionnelle papier et, à moins que le serveur destinataire du message ne signale qu’il a un problème avec l’une ou l’autre de ces informations, le système expéditeur envoie la commande « DATA », et en général envoie plusieurs éléments d’en-tête, notamment :

* **From:** Joe Q Doe <joeqdoe@example.com> - l’adresse est visible par le destinataire mais, là encore, par défaut aucun contrôle n’est effectué pour savoir si le système expéditeur est autorisé à envoyer au nom de cette adresse.
* **Reply-to:** Jane Roe <Jane.Roe@example.mil> - non contrôlé non plus.

Et parfois :

* **Sender:** Jin Jo <jin.jo@example.jp> - là non plus, sans contrôle

Le destinataire du mail reçoit donc son mail comme si celui-ci avait été envoyé depuis l’adresse indiquée dans l’en-tête *From:* ; il arrive que l’on puisse trouver l’adresse *MAIL FROM ;* et si l’on répond au mail, celui-ci sera acheminé soit vers l’adresse de l’en-tête *From:,* soit vers celle de *MAIL FROM ;* or, en général, ni l’une ni l’autre ne sont fiables, de sorte que les messages de renvoi automatiques peuvent générer un phénomène de rétrodiffusion.

Même si la technique d’usurpation de l’adresse mail est efficace pour créer une fausse adresse mail, l’adresse IP de l’ordinateur d’où a été envoyé le mail peut en général être identifiée à partir des lignes « Received » dans l’en-tête du mail. Il est fréquent qu’il s’agisse d’un tiers innocent infecté par un maliciel (malware) qui envoie le mail sans que le propriétaire de l’ordinateur n’en soit averti.

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