Date: Jeudi 18 août 2005 à 13:43:50
Sujet: 3 Sécurité et Hacking

Qu'est-ce que le mail-bombing ?

Le Mail Bombing consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires.

Le Mail Bombing consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires., dans le but de saturer le serveur de mails, la bande passante du serveur et du ou des destinataires, ou même de rendre impossible aux destinataires de continuer à utiliser l'adresse électronique !!

L'attaque

Il est nécessaire pour l'auteur de l'attaque de se procurer un logiciel permettant de réaliser le mail bombing, des logiciels qui permettent à l'utilisateur de choisir :

* l'adresse qu'il veut faire apparaître en tant qu'émetteur du message;
* le sujet du message,
* le nombre de messages à envoyer,
* le serveur de mail à partir duquel les messages seront émis, (bien souvent si les administrateurs de serveurs mails ne se protègent pas assez, des serveurs "innocents" servent de relais sans le savoir, et le danger pour leurs propriétaires est de se retrouver "black listés" c'est à dire voir son fournisseur d'accès internet lui couper sa connexion),
* le corps du message,
* l'adresse email de la victime.

La possibilité d'y attacher une pièce jointe est une sérieuse menace, puisqu'elle permet à l'expéditeur d'insérer virus et troyens dans les messages. Une fois de plus, rappelons qu'il faut impérativement éviter d'ouvrir une pièce jointe ayant pour extension .com, .bat, .pif ou .exe...

Comment réagir à ces attaques ?

Avant de prendre le risque d'avoir une adresse électronique inutilisable mieux vaut prendre ses précautions :

* Si vous avez une adresse personnelle à laquelle vous tenez, ne la communiquez qu'aux personnes dignes de confiance,
* Créez vous un second compte de messagerie, pour tout ce qui est mailing list par exemple et groupe des discussion, ainsi, vous ne craignez pas de perdre d'informations vitales. Si ce compte est attaqué vous pourrez sans difficulté reprendre une autre adresse et vous ré-abonner.
* Utilisez eremove (voir les téléchargements / utilitaires) pour éviter les mail bombers.

Lancement de Eremove :

1. Face au premier écran, vous allez maintenant pouvoir commencer la configuration en tapant sur next.

2. Sur l'écran suivant, vous devez rentrer les identifiants de votre messagerie, votre mot de passe, le serveur de votre FAI ainsi que le port utilisé (par défaut c'est généralement le 110). Pour les personnes disposant de plusieurs comptes de messagerie différents, il est nécessaire de passer par le mode avancé de configuration. Cliquer sur "Advance".

2.1. ADVANCE : L'onglet Account permet de donner les indications sur tous les comptes de messagerie que vous souhaitez protéger. A chaque fois que vous cliquez sur Add vous trouverez un écran similaire à celui que vous avez vu pour votre compte principal. Vous pouvez entrer autant de comptes que vous le désirez.

2.2. ADVANCE : L'onglet Programs vous permet de déterminer quel est le type de Boîte aux Lettres que vous utilisez (Eudora, Outlook, etc ...).

2.3. ADVANCE : L'onglet Others vous permet de déterminer si le programme se connecte directement à votre boite aux lettres à son lancement. Vous pouvez aussi spécifier un fichier de logs.

3. Ensuite, lorsque vous lancez eremove, le programme vous montre le nombre de messages, ainsi que la taille de chacun et l'émetteur. Il vous suffit ensuite de sélectionner le ou les messages que vous ne souhaitez pas recevoir et ils seront directement détruits sur le serveur de messagerie.

Vous pouvez au préalable vérifier le contenu du message en faisant un clic gauche avec la souris sur le message. Cela vous donnera des éléments sur le corps du message et sur l'expéditeur.

Vous avez été attaqué :

Si vous avez été victime d'un mail bombing, il est parfois possible de remonter jusqu'à l'émetteur.
En effet, il existe des informations dans chaque message qui donnent des informations sur leur auteur.
Voici un exemple de propriétés de message :

* Return-Path: Ici vous trouvez l'email de l'émetteur
* Received: from hotmail.com (f88.law14.hotmail.com [64.4.21.88]) by servertoto.pourexemplejenevaispsvousmonserveur.net (8.9.3/8.9.3-NoSpam-Rbl-ORBS) with ESMTP id PAA19370 Ici vous trouvez le serveur par lequel l'attaquant à envoyé les messages. Si la personne débute il se peut que ce serveur soit réel et il vous faut vous rapprocher de son propriétaire pour vous plaindre.
* For commercial@securiteinfo.com; Sat, 22 Dec 2001 15:45:34 +0100 Ici vous trouvez normalement votre adresse de messagerie ainsi que des indications horaires

Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
Sat, 22 Dec 2001 06:33:00 -0800
Received: from XXX.XXX.XXX.XXX by lw14fd.law14.hotmail.msn.com with HTTP;
Sat, 22 Dec 2001 14:33:00 GMT

* X-Originating-IP: [XXX.XXX.XXX.XXX] Ici vous trouvez les indications sur l'IP d'où sont partis les messages. Attention, il est possible mais assez rare que l'adresse IP soit modifiée
* From: "Eyrill ROMOS" De nouveau l'émetteur
* To: De nouveau le destinataire
* Subject: =?iso-8859-1?B?UHJvcHJp6XTpcyBkJ3VuIG1lc3NhZ2Ug?= Le sujet du message encodé
* Date: Sat, 22 Dec 2001 15:33:00 +0100 Date et heure
* Mime-Version: 1.0 Version Mime utilisée pour l'encodage du message
* Content-Type: text/plain; charset=iso-8859-1; format=flowed Type de contenu
* Message-ID: Identifiant interne du message
* X-OriginalArrivalTime: 22 Dec 2001 14:33:00.0561 (UTC) FILETIME=[8E825010:01C18AF5] Heure et date d'arrivée du message

Si vous retrouvez des informations comme l'adresse email ou le serveur qui ont permis l'arrivée des messages, il est important de se plaindre auprès du fournisseur d'accès. En effet, dans la plupart des cas les fournisseurs d'accès n'apprécient pas ce type de procédés via leurs serveurs et prennent toutes les mesures nécessaires pour empêcher les auteurs de recommencer.

Conclusion :

Le mail bombing n'est, à priori, pas illégal. Il n'existe pas de limite légale déterminant le nombre maximum de messages à envoyer à un internaute. Cependant, les fournisseurs d'accès à Internet n'apprécient pas ce type de procédés. En effet, cela leur cause des soucis de bande passante et la saturation de leurs serveurs de messagerie. En conséquence, n'hésitez surtout pas à les solliciter si vous êtes victime d'une telle attaque. Ils réagissent généralement rapidement pour éviter que leurs abonnés recommencent. Par ailleurs, prendre le temps d'installer eremove est indispensable si l'on désire éviter tout soucis et ne pas se retrouver contraint à changer d'adresse électronique. Une fois installé vous pouvez en toute quiétude ne plus craindre les attaques par mail bombing !!!

URL de cette publication
http://www.zmaster.fr/modules.php?name=News&file=article&sid=114