This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

Recommandation MAAWG
Gestion du port 25 appliquée à l'espace IP dynamique ou résidentiel
Pourquoi l'adopter ? Que risque-t-on à ne rien faire ?

Introduction

Virus et logiciels espions sont de plus en plus utilisés par les spammeurs et autres criminels pour prendre le contrôle de nombreux ordinateurs personnels. La hausse continue du nombre d'ordinateurs ayant une connexion permanente (DSL, câble ou réseau d'entreprise) augmente le nombre de cibles et le risque de subir d'importants dégâts. Quelques modifications techniques, associées à une sensibilisation des utilisateurs, qui encouragerait ces derniers à utiliser des logiciels antivirus et des pare-feu, permet d'améliorer le contrôle d'un fournisseur de service de messagerie électronique sur le trafic néfaste qui pourrait être émis depuis les ordinateurs de ses propres clients. Une meilleure gestion des messages électroniques expédiés depuis les ordinateurs personnels permettrait ainsi aux fournisseurs de réduire leurs coûts opérationnels, de mieux satisfaire leurs clients et de diminuer le nombre d'utilisations abusives de l'Internet associées à leur service.

Flux de courrier électronique : menaces et abus

Le fait de pouvoir accéder en permanence depuis un ordinateur personnel à des serveurs de messagerie (envoi de messages électroniques) qui ne sont ni gérés ni contrôlés par le fournisseur de services de messagerie augmente le risque à la fois pour le fournisseur et pour ses clients d'être victimes de personnes malveillantes ou de logiciels « véreux ». Les ordinateurs personnels contrôlés par des tiers non autorisés à l'insu de leur propriétaire, communément appelés « zombies », permet aux spammeurs qui les utilisent pour se connecter à des serveurs de messagerie (MX) et à des relais SMTP non protégés de garder l'anonymat et d'envoyer ainsi encore plus de spams et de virus. Pas moins de 80 % des spams transitent par ces ordinateurs « zombies » sans que leur propriétaire n'ait donné leur autorisation ou n'en soit informé.

Ne rien faire : quels sont les risques ?

Les effets négatifs pour les propriétaires de ces ordinateurs détournés sont immédiats et importants. Souvent, les utilisateurs constatent une baisse des performances de leur ordinateur pendant de longues périodes, en particulier lorsqu'ils utilisent l'Internet. À leur insu, un spammeur peut saturer la largeur de bande en amont et réduire aussi considérablement la largeur de bande disponible en aval.

Le fournisseur d'accès auquel ordinateur est connecté remarquera peut-être à peine qu'une largeur de bande additionnelle est utilisée, mais en règle générale, les effets seront néfastes pour lui aussi. En effet, le client concerné risque d'appeler le service technique, ce qui peut représenter un coût équivalent à un mois de recettes, voire plus, pour l'opérateur. Le client peut aussi simplement estimer que les services logiciels, commutés ou large bande du fournisseur ne sont pas assez performants et décider d'en changer.

Tant que le client continuera de se connecter à l'Internet via son accès infecté, le fournisseur accumulera les plaintes des destinataires des spams émis par l'ordinateur infecté. Les coûts induits par les plaintes reçues par le service client, le service des fraudes ou le service d'exploitation de réseau du fournisseur peuvent devenir considérables, même si le réseau ne compte qu'un petit nombre d'ordinateurs « zombies ». Le fournisseur peut

également s'apercevoir que tout son réseau se retrouve sur une liste noire, ou ne peut envoyer de messages à des destinataires habituels, en raison du nombre élevé de spams émis. Bien évidemment, à chaque spam émis correspond un spam reçu. Rester passif face à ce genre d'abus nuit à tous les utilisateurs Internet et à tous les fournisseurs d'accès et n'encourage pas le consommateur à utiliser l'Internet comme outil de communication, de commerce ou de divertissement.

Envoi de messages électroniques : les meilleures pratiques

Le moyen le plus efficace de combattre les abus en ce qui concerne l'envoi de messages électroniques illégitimes est de laisser le secteur se réguler lui-même. L'ampleur du problème appelle des mesures immédiates. Les organismes publics du monde entier ont été très clairs sur ce point : sans action immédiate et sans résultats, le secteur s'expose à plus de surveillance et plus de régulation. C'est pourquoi le MAAWG recommandent les Meilleures pratiques pour les fournisseurs de services Internet et de messagerie électronique en matière de gestion du port 25 suivantes :

1. Assurer les services d'envoi de messages électroniques via le port 587, comme indiqué dans la norme RFC 2476 ;

2. Exiger une authentification pour l'envoi des messages, comme indiqué dans la norme RFC 2554 ;

3. Ne pas gêner la connectivité avec le port 587 ;

4. Configurer la messagerie électronique du client de sorte qu'elle utilise le port 587 et demande l'authentification pour envoyer des messages électroniques ;

5. Bloquer l'accès au port 25 pour tous les clients du réseau, sauf pour ceux que les fournisseurs ont expressément autorisés à exécuter des fonctions de relais SMTP. Il s'agira a priori de vos propres serveurs de messagerie et éventuellement des serveurs légitimes de vos clients responsables ;

6. Bloquer tout trafic à destination de votre réseau en provenance du port 25, ce qui évitera de potentiels abus de la part de spammeurs qui utilisent un routage asymétrique et usurpe les adresses IP sur votre réseau.

Ces pratiques ont été adoptées par des fournisseurs de toutes tailles, y compris par bon nombre des plus grands fournisseurs dans le monde et par beaucoup de membres du MAAWG, sans qu'ils aient à subir de réduction sensible de leur clientèle.

Pourquoi adopter ces meilleures pratiques

L'authentification obligatoire et le regroupement des messages électroniques envoyés sur le relais SMTP présentent les précieux avantages suivants pour le fournisseur de services Internet :

- identifier le client à l'origine des messages ;
- filtrer les spams, les virus et les autres utilisations abusives de la charge utile liée à l'envoi de messages ;
- surveiller et limiter le nombre de messages envoyés par client et/ou total;
- appliquer des politiques et des conditions générales d'utilisation du service de messagerie acceptables.

En outre, le fournisseur de services Internet retire les avantages concurrentiels suivants :

- remise plus efficace des messages légitimes due à une diminution du risque d'être placé sur une liste noire par le fournisseur de services Internet et de messagerie du destinataire ;
- diminution des coûts pour les services d'assistance en cas d'abus, le service clientèle et le service d'exploitation du réseau ;
- possibilité d'offre de services de premier choix aux clients ayant un besoin légitime d'exploiter des serveurs de messagerie électronique avec un accès direct au port 25 ;
- réduction des coûts d'infrastructure due à la diminution de l'utilisation des ports et de la consommation de largeur de bande ;
- rôle proportionnel du destinataire dans la baisse du nombre de spams.

Une fois ces mesures mises en place, les ordinateurs infectés ne peuvent plus être vecteur d'anonymat. Ils peuvent être rapidement identifiés et mis en quarantaine le temps que leur propriétaire se rende compte du problème et le résolve. Ce faisant, les clients prennent conscience des menaces de sécurité et sont encouragés à mieux se protéger. Chacun de ces changements améliore la sécurité et la confidentialité pour tous les utilisateurs finals.

Sensibiliser les clients

Le MAAWG n'insistera jamais assez sur l'importance d'informer les clients et de les sensibiliser à ces menaces, aux mesures prises pour les éliminer et au rôle que les propriétaires d'ordinateurs doivent jouer dans la mise en place d'un mécanisme plus sûr pour envoyer des messages électroniques. Les fournisseurs de services Internet et de messagerie doivent informer leurs clients de ce qu'ils font, pourquoi ils le font, et pourquoi, pour la plupart d'entre eux, cela sera transparent. Tous les fournisseurs de services de messagerie sont vivement encouragés à adopter ces pratiques technologiques le plus vite possible, à reprendre le contrôle du port 25 et à mener en permanence des programmes de sensibilisation de leurs clients en protégeant leurs services contre les utilisations abusives.

À lire sur le même thème :

SMTP Service extension for authentication, J. Meyers, Mars 1999 (http://www.ietf.org/rfc/rfc2554.txt)

Message submission, R. Gellens and J. Klensin, Décembre 1998 (http://www.ietf.org/rfc/rfc2476.txt

Operation spam zombies, Federal Trade Commission, Mai 200 (http://www.ftc.gov/bcp/conline/edcams/spam/zombie/)

Anti spam technical alliance technology and policy proposal, anti spam technical alliance, 11 juin 2004 (http://www.postmaster.aol.com/asta/proposal_html.html)

Freinons le pourrriel, Créer un Internet plus fort et plus sécuritaire, Industrie Canada, Avril 2005 (http://e-com.ic.gc.ca7epic/internet/inecic-ceac.nsf/en/gv00329e.html)