

- **Éditorial**
par **J.-L. Archimbaud**
- **L'action de la CNIL**
par **L. Basse**
- **Lutte anti-spam**
par **M. Herrb**
- **Point de vue de...**
par **K. Kortchinsky**

éditorial

Spam...

Combien de temps consacrez-vous, chaque matin, à éliminer les courriers électroniques inutiles de votre boîte aux lettres? Ne serait-ce que quelques minutes, cela ne vous met pas franchement de bonne humeur pour la journée, et la perte de temps cumulée pour l'ensemble du personnel d'une organisation est énorme. C'est le résultat de l'une des déviances de l'Internet, le spam, envoi massif de courriers électroniques non sollicités.

Deux caractéristiques de la messagerie Internet ont favorisé ce phénomène : l'absence d'authentification de l'émetteur d'un message et la quasi-gratuité de service. La première fait qu'on peut vous envoyer des messages publicitaires, voire illicites, sans que vous puissiez rapidement identifier l'émetteur réel; la seconde permet au spam d'être rentable, même si un infime pourcentage des personnes est réellement accroché. L'investissement est presque nul. Ce n'est pas le cas d'autres modes de communication comme le courrier postal ou les SMS qui sont payants unitairement.

Le monde académique est particulièrement touché par ce fléau. Les collaborations internationales et les noms de domaine des universités ou des laboratoires très variés ne permettent pas une sélection facile d'adresses de confiance. Les serveurs de messagerie sont nombreux, ce qui nécessite une surveillance et des outils sur chacun. Les adresses électroniques du personnel sont souvent publiées sur le Web, donc facilement récupérables par des spammeurs.

Il n'y a pas, aujourd'hui, de solution miracle pour éradiquer totalement le phénomène. Néanmoins, deux moyens de lutte sont présentés dans ce numéro. L'un est juridique et décrit par Leslie Basse de la CNIL, l'autre est technique, présenté par Matthieu Herrb en prenant comme exemples les outils installés au laboratoire LAAS.

D'autres parades sont à l'étude dont des évolutions au niveau des protocoles entre serveurs de messagerie et dans les annuaires par exemple, mais aucune solution radicale n'a encore émergé. Sauf désaffection possible de l'utilisation de la messagerie électronique au profit d'autres modes de communication particulièrement en vogue : SMS et messageries instantanées, le spam garde encore de beaux jours devant lui. Mais les deux articles présentés ici montrent qu'il est actuellement possible de le contrer avec efficacité.

Jean-Luc Archimbaud
Directeur de l'UREC

Sécurité Informatique, orphelin?

Tous les lecteurs de *Sécurité Informatique* connaissent bien Robert Longeon, qui depuis 1996 était l'âme de ce bulletin, au titre de ses fonctions de chargé de mission SSI pour le CNRS. Robert Longeon vous avait annoncé son départ dans un numéro précédent, sans vous révéler qu'il s'envolait vers les plus hauts lieux de la sécurité des systèmes d'information, en regagnant la Direction Centrale de la Sécurité des Systèmes d'Information (au Secrétariat Général de la Défense Nationale). *Sécurité Informatique* se sent un peu orphelin, même si Robert reste présent en tant que fidèle lecteur et que nous n'hésiterons pas à le solliciter au titre de ses nouvelles fonctions. À bientôt Robert.

Joseph Illand, Fonctionnaire de Sécurité de Défense

L'action de la CNIL en matière de lutte contre le spam

par **Leslie Basse**
Juriste, CNIL

L'envahissement de la boîte aux lettres électronique des internautes par des «spams»¹ demeure un des problèmes majeurs de l'Internet. Illégal en lui-même, le spam est en outre utilisé de plus en plus pour des activités à caractère frauduleux, telles la capture d'informations financières (mot de passe et numéro de compte), le spammeur se faisant alors passer pour une société sérieuse (technique dite de «spoofing» ou de «phishing»), ou encore la diffusion de virus.

Le phénomène du spam, par son importance, sape la confiance dans l'économie numérique et menace la sécurité des réseaux.

La loi pour la confiance dans l'économie numérique (LCEN), adoptée le 21 juin 2004, entend remédier à ce problème en renforçant les droits des internautes en matière de sollicitation commerciale par courrier électronique en instituant le consentement préalable.

Pour sa part, la Commission nationale de l'informatique et des libertés (CNIL) a choisi depuis plusieurs années de mener une politique active de lutte contre le spam, qu'il s'agisse de l'application effective de la législation anti-spam, de l'adoption de codes de bonne conduite par les professionnels, et du développement d'une forte coopération internationale.

La CNIL a, dès 1999, lors du rapport sur «Le publipostage électronique et la protection des données personnelles», considéré que le spam était une pratique illicite au regard de la loi «informatique et libertés» du 6 janvier 1978.

Par ailleurs, soucieuse d'appréhender de façon concrète le phénomène du «spam» en France, [suite page 2](#) ➔

1. La CNIL définit le spam comme l'envoi massif, et parfois répété, de courriers électroniques, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière. Constituent des spams les messages adressés à la suite d'une collecte irrégulière d'adresses de messageries électroniques soit au moyen de moteurs de recherche dans les espaces publics de l'internet, soit que les adresses aient été cédées sans que les personnes en aient été informées et sans qu'elles aient été mises en mesure de s'y opposer ou d'y consentir.

— suite de la page 1 —

la CNIL a mis en place au cours de l'été 2002 un dispositif appelé «boîte à spams» invitant les internautes à transférer par courrier électronique leurs messages non sollicités. Cette opération a trouvé immédiatement un énorme écho auprès du public, avec plus de 300000 messages reçus en trois mois.

Cette opération ponctuelle a permis à la CNIL de définir une stratégie en matière de lutte contre le spam, qui comporte un volet pédagogique et répressif. C'est ainsi que la Commission a mis en ligne sur son site Internet (www.cnil.fr) une «boîte à outils anti-spam» appelée «Halte au spam!». Réalisé après consultation des principaux acteurs concernés – fournisseurs d'accès Internet et professionnels du marketing –, ce module pédagogique a pour but d'apporter aux internautes des informations pratiques – techniques et juridiques. Il précise ainsi les démarches à effectuer pour porter plainte, ainsi que les réflexes à avoir pour se prémunir contre la réception de spams. Ce module s'adresse également aux professionnels en leur rappelant les règles à respecter à l'occasion d'une campagne d'«e-mailing».

Ce régime juridique se décline par l'application des règles suivantes:

■ La première interdit d'adresser aux personnes physiques (des individus) des messages de nature commerciale par courrier électronique, par SMS («Short Message Service») ou par MMS («Multimedia Messaging Services»), sans avoir obtenu préalablement leur consentement. Ce dernier doit être donné en pleine connaissance de cause; le fait d'accepter des conditions générales de vente ne signifie pas qu'on a donné son consentement à être prospecté.

■ La seconde prévoit une dérogation au principe du consentement préalable dans le cadre d'une relation client-entreprise existante: une personne ayant acheté un produit auprès d'une entreprise pourra recevoir des messages commerciaux de la part de cette dernière, sous réserve que la sollicitation porte sur des produits analogues. L'entreprise devra toutefois avoir mis en mesure la personne, au moment de sa commande, de s'opposer gratuitement à recevoir de la publicité de sa part.

Dans tous les cas de figure, la personne démarchée doit avoir la possibilité de demander gratuitement et à tout moment que l'envoi des messages publicitaires cesse et elle doit également être informée de l'identité de l'organisme pour le compte de laquelle le message est envoyé.

Par ailleurs, le démarchage autre que de nature commerciale, comme la prospection à caractère politique, associatif, religieux ou caritatif (par exemple, collecte de dons), n'est pas soumis au principe du consentement préalable. En effet, ce sont les règles issues de la loi — suite page 3 —

BRÈVES

(destinées principalement aux laboratoires CNRS)

Spam

Un groupe de travail technique académique s'est mis en place dont un des objectifs est de regrouper des ressources antisipam: <http://www.cru.fr/antisipam/>

Gestion de traces

● Une déclaration générique de gestion des traces (informatique et réseau) pour les laboratoires CNRS a été faite auprès de la CNIL: https://intranet.cnrs.fr/extranet/cnrs/fsd/documents/Po_gest_traces.pdf.

● Une décision à ce sujet est parue au Bulletin officiel du CNRS: <http://www.dsi.cnrs.fr/BO/2004/12-04/4111-bo1204-dec04p014dsi.htm>.

● Une note de J. Illand (datée du 16 février) a été envoyée à tous les directeurs de laboratoires, sous couvert des délégués régionaux, pour la mise en conformité des unités par rapport à la déclaration faite à la CNIL.

● Une démarche similaire est en cours dans les universités.

Incidents récents

Deux types d'attaques ces derniers mois:

● **Compromission de serveurs web dynamiques.**

Recommandations:

Appliquez tous les correctifs de sécurité que vous conseille le CERT Renater.

Interdisez (ou limitez) les rebonds entre le serveur web situé dans la zone semi-ouverte et les machines situées dans la zone interne.

Définissez des méthodes de programmation strictes de vos sites web.

● **Attaque par force brute de serveur ssh.**

Recommandations:

Privilégiez l'authentification par clef.

Si ce n'est pas possible, vérifiez la solidité des couples nom d'utilisateur/mot de passe.

Surveillez votre serveur ssh, point d'entrée important.

Veille technologique UREC

Afin de donner des conseils validés aux utilisateurs CNRS, nous sommes en train de mener des tests sur trois catégories de produits: la voix/ip (skype, msn...), le chiffrement (prim'x, msi...), les VPN SSL (openvpn...).

Phishing

Pour en savoir plus sur le Phishing: <http://www.hsc.fr/ressources/presentations/rs05-phishing/index.html>

Sur le plan répressif, l'opération «boîte à spams» a conduit la CNIL à dénoncer à la justice cinq entreprises à l'origine du plus grand nombre d'envois de messages non sollicités. À cette occasion, des contacts réguliers ont été pris avec les parquets concernés et les services de police spécialisés en la matière, afin de les informer et de les sensibiliser sur l'ampleur des préjudices causés par le spam. Si le bilan des actions judiciaires intentées par la CNIL n'a pas encore à ce jour rencontré les résultats escomptés², ce constat ne remet pas en question l'action de la CNIL, compte tenu notamment de l'évolution de la législation.

La France a désormais une législation spécifique interdisant le spam, à savoir la loi du 21 juin 2004 pour la confiance dans l'économie numérique

Le principe essentiel posé dans la loi est celui du consentement préalable (consécration du principe dit de l'«opt-in»). Son article 22 subordonne ainsi l'utilisation de courriers électroniques dans les opérations de prospection commerciale au consentement préalable des personnes concernées.

2. Plusieurs dénonciations ont été classées sans suite faute d'identification du spammeur. S'agissant de la dénonciation ayant fait l'objet de poursuites pénales, le tribunal correctionnel de Paris a, par un jugement du 7 décembre 2004, décidé de relaxer le dirigeant de cette société qui était poursuivi pour collecte déloyale de données nominatives. Il a été fait appel par le parquet de Paris de ce jugement, ce dont se félicite la CNIL qui a toujours considéré que le fait de collecter des adresses électroniques sur Internet à l'insu des intéressés à des fins commerciales constituait un délit.

— suite de la page 2 —

«informatique et libertés» qui s'applique; à savoir une information préalable sur l'utilisation de son adresse électronique à de telles fins et le droit de s'opposer à cette utilisation.

Les codes de déontologie de l'«e-mailing»

Dans le prolongement de l'adoption de la LCEN, la CNIL a engagé un travail de concertation avec les professionnels du marketing direct afin de définir les modalités pratiques d'application du nouveau régime juridique.

Ce travail a abouti à l'adoption de deux codes de déontologie de l'«e-mailing» présentés respectivement par l'UFMD (Union française du marketing direct) et le SNCD (Syndicat national de la communication directe), qui représentent la quasi-majorité des acteurs du marketing en France. En application de l'article 11 de la loi du 6 janvier 1978, la CNIL a reconnu ces deux codes conformes aux exigences légales et à ses préconisations. Ces codes proposent ainsi des exemples de mentions de recueil du consentement des personnes concernées, telle l'aposition d'une case à cocher sur chaque formulaire de collecte, ce qui constitue une préconisation constante de la CNIL. Véritables guides pratiques, ces codes permettent d'assainir et d'encadrer la prospection par «e-mailing».

Les actions de coopération de la CNIL avec le secteur privé

Elles portent également leurs fruits, comme en témoigne le jugement prononcé le 5 mai 2004 par le tribunal de commerce de Paris condamnant un «spammeur» à 22000 € de dommages et intérêts. Dans cette affaire, la CNIL a prêté son concours à l'action judiciaire engagée par deux entreprises, en leur transmettant, après les avoir rendus anonymes, tous les éléments relatifs aux plaintes enregistrées auprès d'elle concernant cet émetteur de courriers électroniques non sollicités.

La pratique du «spamming»

Elle peut être sanctionnée sur la base d'autres fondements juridiques. Ainsi, le fait de pratiquer une opération de «spamming» qui, par l'ampleur du nombre de messages envoyés, provoque un blocage des serveurs ou de la bande passante (on parle alors de «mailbombing») est constitutif du délit d'entrave au fonctionnement d'un système de traitement automatisé de données prévu à l'article 323-2 du Code pénal. Il est également interdit d'envoyer un courrier électronique à des fins de publicité mensongère, de tromperie ou d'escroquerie (exemple: le réseau d'escroquerie du «scam»³ nigérian), ou encore d'envoyer un courrier électronique en méconnaissance des règles contractuelles ou des usages (exemple: violation du contrat de service de messagerie électronique).

Enfin, rappelons que des condamnations exemplaires ont été prononcées en dehors de nos frontières, à l'instar de celle prise aux États-Unis par la cour de l'État de Virginie qui a sanctionné un spammeur par une peine de neuf ans d'emprisonnement⁴.

La multiplication des initiatives en matière de lutte contre le spam tant au niveau national, européen que mondial

En France, la CNIL participe au groupe de concertation et d'action contre le spam lancé par le gouvernement le 10 juillet 2003. Ce groupe, animé par la Direction du développement des médias (www.ddm.gouv.fr), réunit les acteurs publics et privés de la lutte contre le spam (autorités de régulation, organisations représentatives, personnalités qualifiées, représentants des administrations mobilisées).

La Commission européenne, afin de faciliter et de coordonner les échanges d'information et les meilleures pratiques en matière de traitement des plaintes relatives au spam, a créé un groupe en ligne informel réunissant les autorités européennes chargées de la

répression du spam dont la CNIL a été pilote en 2004. Une procédure de coopération définissant les conditions d'échange d'informations sur les plaintes reçues en matière de spam a été adoptée par ce groupe en décembre 2004.

Enfin, au niveau international, la CNIL suit l'ensemble des travaux menés au sein des instances internationales. Leur foisonnement atteste que la lutte contre ce fléau est devenue une véritable priorité pour les gouvernements et les organisations internationales telles que l'OCDE ou l'Union internationale des télécommunications. La CNIL entretient également des contacts réguliers avec le Département du commerce américain («Federal Trade Commission»), qui veille au respect de la législation «antispam» dit «Can Spam Act», adoptée le 1^{er} janvier 2004. La commission s'est toutefois fixé comme principal objectif d'assainir le marché français avant de poursuivre ses efforts au niveau mondial.

Conclusion

Il est nécessaire de rappeler que le spam ne concerne qu'une partie du publipostage électronique; celui qui est répréhensible car contraire à la loi, et non pas l'ensemble du marketing électronique. Il y a trop souvent confusion entre spams et communications électroniques. Pour les expéditeurs de spam établis en France, la CNIL va continuer son action en utilisant notamment les pouvoirs de sanction dont la nouvelle loi «informatique et libertés» l'a dotée. Enfin, s'agissant d'expéditeurs établis à l'étranger, la coopération internationale et l'intervention de tous les acteurs concernés sont les deux éléments, compliqués à réunir en pratique, mais indispensables au succès.

3. Forme de spam dédiée à l'escroquerie.

4. L'État de la Virginie a condamné le 8 avril 2005 un spammeur à une peine d'emprisonnement de neuf ans pour expédition massive au cours de l'été 2003 de courriers électroniques. Celui-ci aurait accumulé une fortune de 24 millions \$US en faisant la promotion de biens et services à l'aide de centaines de milliers de spams.

Lutte anti-spam au LAAS

Matthieu Herrb

ingénieur de recherche, CNRS/LAAS

Le LAAS (Laboratoire d'analyse et d'architecture des systèmes, unité propre du CNRS, Département sciences et technologies de l'information et de la communication) a un effectif d'environ six cents personnes et autant de comptes utilisateurs. Sur ses serveurs de messagerie électronique le laboratoire reçoit plusieurs milliers de messages par jour. Les premiers messages commerciaux non sollicités sont apparus vers la fin 1997, et depuis le phénomène n'a cessé de prendre de l'ampleur. Pour pouvoir continuer à utiliser le courrier électronique dans de bonnes conditions, il est apparu nécessaire assez rapidement de lutter contre ce fléau, appelé entre-temps spam en référence à un sketch des Monthly Python. Cet article présente l'état actuel des outils utilisés au LAAS pour faire barrage au spam, sans bloquer les messages normaux.

Les techniques anti-spam

Pour être efficace, il est indispensable de connaître le point de vue des diffuseurs de spams (les spammeurs). Leur principale raison d'être est le profit, en attirant des clients potentiels vers une activité commerciale (qui peut être une escroquerie ou une activité parfaitement légale). Le coût de diffusion de cette publicité est quasiment nul, et même un taux de retour très faible suffit à générer un bénéfice important.

En face, on trouve trois types d'outils (BARE05) : les listes noires, les filtres sur le contenu et les outils qui vérifient le respect du protocole de transport des messages électroniques (SMTP) pour éliminer les messages qui ne sont pas transportés par un vrai agent SMTP.

■ Les listes noires sont des listes d'adresses IP de machines utilisées par des spammeurs pour diffuser leurs messages. Elles sont constituées à partir de signalement de spams reçus et gérées par quelques organisations indépen-

dantes. Il est également possible de construire de telles listes automatiquement à l'aide de «pots de miel» qui attirent le spam à partir d'adresses de messagerie fabriquées à dessein et rendues visibles des seuls robots de collecte d'adresses sur une page Web très visitée.

Le principal problème des listes noires est que, en général, leur contenu échappe complètement aux utilisateurs. Il est beaucoup plus facile d'y entrer que d'en sortir. Les gestionnaires de listes noires sérieuses finissent par être découragés par les attaques dont ils sont victimes de la part des spammeurs, tandis que fleurissent les listes commerciales plus dédiées au profit qu'à la lutte anti-spam.

C'est pourquoi les listes noires ne doivent pas être utilisées seules pour rejeter un message, mais elles peuvent contribuer à définir un critère heuristique.

■ Les outils de filtrage sur le contenu cherchent à déterminer si un message est du spam ou non en fonction du contenu. Ils peuvent soit être basés sur des règles heuristiques sur la mise en forme du message (formatage HTML, présence de gros titres de couleurs vives, liens vers des sites externes, notice de désabonnement, etc.), soit sur des mots clés contenus.

Pour mieux résister aux astuces utilisées par les spammeurs pour échapper à la détection par mots clés, les systèmes de filtrage peuvent se baser sur un mécanisme de classification bayésienne avec apprentissage (GRAH02) : chaque utilisateur définit ainsi ce qu'il considère comme du spam et ce qui n'en est pas, et ajuste en permanence les scores de détection associés aux mots les plus significatifs d'un message.

■ Pour abaisser leurs coûts de diffusion, les spammeurs utilisent des outils de diffusion en masse, installés souvent sur des machines piratées plutôt que des relais de messagerie traditionnels. Ces

logiciels prennent des libertés avec le protocole SMTP, en particulier en ne traitant pas les erreurs.

Les listes grises, proposés par E. Harris (HARR03), exploitent cette caractéristique : chaque message peut être décrit par un triplet composé de l'adresse de l'expéditeur, de l'adresse IP du relais SMTP qui transmet le message et de l'adresse du destinataire. Lorsque le triplet en question n'est pas encore présent dans la base de données du destinataire, le message est rejeté avec un code d'erreur indiquant un problème temporaire et demandant au relais expéditeur de re-soumettre son message plus tard. Le triplet est enregistré, avec l'heure de sa soumission dans la liste grise. Après un délai initial (vingt-cinq minutes), le triplet passe en liste blanche et, lors de la nouvelle tentative d'envoi par le serveur, le message sera accepté. Le triplet reste alors en liste blanche pour une durée assez longue (cinq semaines), permettant aux autres messages ayant le même triplet de passer sans blocage.

Ainsi les messages qui sont envoyés par une implémentation partielle du protocole SMTP ne sont jamais reçus.

D'autres vérifications de l'implémentation du protocole SMTP sont également possibles (cohérence de la date transmise, existence du domaine de l'expéditeur, vérifications syntaxiques sur le format des différents champs...). Ces vérifications peuvent être utilisées directement pour rejeter les messages ou pour ajouter un score à un outil d'analyse du contenu.

En pratique

Le service de messagerie du LAAS est organisé selon une architecture assez proche de celle décrite dans (DELA05) : deux relais gèrent le courrier arrivant. Ils assurent les fonctions de protection antivirus et anti-spam et transmettent les messages acceptés... [suite page 5](#) ➤

vers un serveur interne qui les dépose dans la boîte à lettres du destinataire.

Les relais utilisent le logiciel Sendmail, avec la technologie Milter, qui permet d'insérer des filtres lors de chaque étape du traitement d'un message (connexion initiale, définition de l'expéditeur, des destinataires, et enfin transmission du corps du message). Les filtres utilisés, basés sur plusieurs logiciels libres, réalisent quatre fonctions :

1) Une vérification au plus tôt de la validité des adresses de destination du message, afin de retourner une erreur définitive au serveur de l'expéditeur, en évitant d'avoir à gérer l'envoi de messages d'erreur vers des adresses d'expédition inexistantes (message envoyé par un virus ou un spammeur).

2) Le mécanisme de listes grises. Le logiciel utilisé, Milter-greylis, gère également une liste blanche permanente des sites connus, qui permet de ne pas saturer la liste grise avec les adresses des correspondants les plus fréquents et de traiter les quelques cas de sites qui n'arrivent pas à traiter l'erreur temporaire retournée initialement.

3) Une fonction d'anti-virus, utilisant les logiciels Clamav et Mimedefang, qui place en quarantaine toute pièce jointe susceptible d'être exécutée directement sur la machine du

destinataire, en fonction d'une liste de types de fichiers établis par Microsoft. Ce traitement permet d'éliminer tous les virus non encore présents dans la base de données de l'anti-virus.

4) Un filtrage anti-spam sur le contenu des messages acceptés. SpamAssassin permet, à l'aide d'une base de règles heuristiques, de marquer les messages avec score indiquant s'ils ont les caractéristiques d'un spam. Ce score est ajouté sous forme d'un en-tête spécifique, X-Spam-Score, qui permet au logiciel de messagerie de l'utilisateur final de décider comment traiter le message.

Au niveau des logiciels de messagerie des utilisateurs

Cette machinerie au niveau des relais de messagerie élimine ou marque comme tel une proportion importante des spams et des virus. Néanmoins, certains messages indésirables peuvent passer à travers, notamment lorsqu'ils sont émis ou relayés par des serveurs qui implémentent entièrement le protocole SMTP.

L'équipe d'administration système du LAAS recommande à ses utilisateurs des outils de messagerie adaptés à l'environnement du laboratoire : soit Mozilla Messenger ou Thunderbird, qui sont tous deux multi-plateformes (Mail, sous Mac OS X, répond également à toutes les spécifications).

Ces outils intègrent tous un outil de filtrage bayésien qui permet, après apprentissage, de reconnaître les spams avec une fiabilité d'autant plus grande que l'apprentissage adapte la classification aux critères de jugement de chaque utilisateur.

Les utilisateurs qui ne souhaitent pas utiliser l'un des logiciels préconisés et ne disposent pas d'un mécanisme de filtrage intégré peuvent, avec l'aide de l'équipe d'administration système, positionner une règle de classification avec l'outil Procmail pour acheminer les messages marqués comme spam par SpamAssassin vers une boîte à

lettres particulière (ou les détruire directement).

En terme de gestion quotidienne, cette solution nécessite un peu de travail :

- Assistance et information des utilisateurs (initialement *via* le conseil de laboratoire, puis régulièrement pour les nouveaux arrivants *via* l'intranet), toujours inquiets en raison du côté critique de la messagerie électronique comme moyen de communication.
- Contrôle régulier des logs qui permet de détecter les anomalies de fonctionnement éventuelles des filtres (listes grises ou antivirus).

Veille technologique indispensable pour évaluer et intégrer les nouveaux outils qui apparaissent au gré des modifications du comportement des spammeurs.

Conclusion

La solution anti-spam mise en place au LAAS élimine une grande partie des messages indésirables, rendant ainsi la messagerie utilisable malgré un environnement de plus en plus pollué. L'utilisation des listes grises supprime une grande part de ces messages et contribue à désengorger les serveurs de messagerie, qui peuvent ainsi plus efficacement réaliser les fonctions de filtrage antivirus sur les messages restants.

Cependant, il ne faut pas perdre de vue que les diffuseurs de spams ont déjà commencé à s'adapter aux mécanismes de listes grises et qu'il va donc falloir trouver de nouvelles parades.

Enfin, le contenu des messages transportés par le spam est également une source d'inquiétude : de la vente relativement inoffensive de produits pharmaceutiques ou de logiciels piratés, le contenu du spam s'oriente de plus en plus vers l'escroquerie pure et simple *via* le vol d'identifiants bancaires (phishing).

La lutte contre ces pratiques qui relèvent du grand banditisme ne peut se faire sans action sur le terrain législatif et judiciaire à l'échelle du monde entier.

matthieu.herrb@laas.fr

■ Bibliographie

- [GRAH02] *A plan for spam*, P. Graham, <http://www.paulgraham.com/spam.html>
 [HARR03] *The next step in the spam control war: greylisting*, E. Harris, <http://projects.puremagic.com/greylisting/>
 [DELA05] « Mise en place d'une passerelle SMTP sécurisée », J.-M. Delapierre, *MISC magazine*, n° 17, janvier-février 2005
 [BARE05] « La lutte contre le spam », N. Bareil, *MISC magazine*, n° 17, janvier-février 2005

■ Outils cités

- Clamav <http://www.clamav.net/>
 Milter-greylis <http://hcnnet.free.fr/milter-greylis/>
 Mimedefang <http://www.mimedefang.org/>
 Sendmail <http://www.sendmail.org/>
 SpamAssassin <http://spamassassin.apache.org/>
 Thunderbird <http://www.mozilla.org/thunderbird/>

Point de vue de...

Kostya Kortchinsky du CERT-Renater

La sécurité des systèmes d'exploitation Windows

Pour beaucoup, le système d'exploitation de Microsoft est encore synonyme d'insécurité, d'instabilité, et est à l'origine de la plupart des maux des systèmes d'information actuels. Mon opinion est tout autre. Je suis utilisateur régulier, voire acharné, de Windows et de Debian Linux depuis plusieurs années, et plutôt satisfait des deux. Ayant de plus un point de vue relativement proche du système, j'ai pu apprécier les modifications apportées par Microsoft à ses OS, notamment en ce qui concerne leur sécurité et leurs nouvelles fonctionnalités. Étant l'une des rares personnes en France à travailler (publiquement) sur la recherche de failles en environnement Windows 32 bits, mon approche des entrailles de l'OS le plus répandu est spécifique. Je suis à l'origine de la découverte de diverses vulnérabilités: MS04-042, MS04-045, MS05-010, MS05-017, et plusieurs autres qui suivront dans un avenir proche. Je travaille aussi sur les failles trouvées par d'autres, afin d'en évaluer l'impact potentiel, de développer des outils adaptés à leur détection et des parades sur le réseau. Il est possible d'avoir un système d'information sous Windows sûr, et voici quelques points qui, selon moi, vont dans ce sens.

Système d'exploitation « fermé »

Parmi les doléances exprimées au sujet de Windows, outre la non-gratuité du produit, figure l'impossibilité (ou du moins la grande difficulté) d'avoir accès à ses sources. Bien évidemment, l'obscurantisme n'a jamais garanti la sécurité d'une application, mais encore moins son insécurité! Il est toujours possible à partir d'un binaire d'obtenir du code assembleur qui pourra être analysé. Preuves en sont les vulnérabilités trouvées jusqu'à présent par ce biais, qui laissent suggérer que Windows est tout aussi « auditable » que n'importe quel autre système d'exploitation. Cela n'en fait certainement pas un logiciel « Open Source », mais au moins ne doit pas être retenu en sa défaveur. Je vous renvoie à la conférence SSTIC qui aura lieu en juin 2005 (1) si vous voulez plus de détails sur les procédés mis en œuvre.

Des progrès conséquents

Quant à la protection des systèmes, des efforts importants ont été apportés à différents niveaux afin de remplacer le plus grand nombre d'appels à des fonctions jugées peu sûres (copies de chaînes de caractères, formatage de chaînes de caractères), au profit d'alternatives plus fiables. Des systèmes de protection de la pile et du tas ont aussi été rajoutés, de même que quelques autres vérifications, une séparation des privilèges accrue, réduisant l'impact de vulnérabilités potentielles sur le système. Au niveau poste de travail, Windows XP SP2 propose la protection la plus aboutie; au niveau serveur, ça sera Windows 2003 (SP1 sous peu). Au final, très peu d'exploits ciblent ces derniers. Les bulletins du mois d'avril corroborent cela (2).

Capacité d'ajustement accrue

Certes, la configuration « out of the box » d'un Windows n'est pas ce qui se fait de mieux en la matière, mais les possibilités d'arrangement sont nombreuses, et réaliser un « master » d'un CD jugé sûr n'est plus un travail de spécialiste. Pour les systèmes existants, je vous invite à lire les articles de Jean-Baptiste Marchand sur la minimisation des services sur les systèmes Windows 2000 à 2003 (3) (4), ou regarder du côté d'un outil comme XPlite (payant) (5) permettant de désinstaller bon nombre de composants. Pour ce qui est de la réalisation de CD bootables, adoptez nLite (6), il vous rendra bien des services.

(1) Symposium sur la sécurité des technologies de l'information et des communications
<http://www.sstic.org/>

(2) Microsoft security bulletin summary for april 2005 -

<http://www.microsoft.com/technet/security/bulletin/ms05-apr.msp>

(3) Minimisation des services réseaux sur les systèmes Windows

http://www.hsc.fr/ressources/brevets/min_srv_s_win.html

(4) Minimizing Windows server 2003 network services -

http://www.hsc.fr/ressources/brevets/min_w2k3_net_srv.html

(5) XPlite and 2000lite Professional v1.5 -

<http://www.litepc.com/xplite.html>

(6) nLite, Windows Installation Customizer -

<http://nuhi.msfm.org/nlite.html>

Séparation des privilèges

Autre point faible depuis des années, héritage des systèmes grand public Windows 95, 98, et Millennium: la difficulté de la mise en œuvre de la séparation des privilèges. Contrairement au monde Unix où il est largement admis que les tâches quotidiennes ne nécessitent pas les droits du super-utilisateur, il n'en va pas de même sous Windows où les privilèges de l'administrateur pouvaient être requis régulièrement. Des progrès ont aussi été faits dans ce domaine, aussi bien par Microsoft qui a, par exemple, intégré la commande « Exécuter en tant que... » à ses systèmes, qu'aux développeurs d'applications tierces qui prennent davantage en compte le fait qu'un utilisateur puisse ne pas être administrateur de son poste. Du point de vue du CERT RENATER, les compromissions de systèmes d'exploitation Windows par des failles de l'OS sont en chute libre, au profit de vulnérabilités de pages web dynamiques ou des comptes utilisateurs aux mots de passe trop faibles. Bien sûr, des correctifs sont toujours régulièrement publiés, mais cela fait longtemps que nous n'avons pas rencontré un phénomène de l'ampleur de Blaster ou Sasser - peut-être l'été prochain? Ultime point faible persistant contre lequel le système ne peut pas forcément grand-chose, ses utilisateurs légitimes...

kostya.kortchinsky@renater.fr

SÉCURITÉ INFORMATIQUE

numéro 53 mai 2005
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités: tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité: 4 numéros par an.
Lectorat: toutes les formations CNRS.

Responsable de la publication:

JOSEPH ILLAND
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris XVI
Tél. 01 44 96 41 88
Courriel: Joseph. Illand@cnrs-dir.fr
<http://www.sg.cnrs.fr/fsd>

ISSN 1257-8819

Commission paritaire n° 3105 ADEP
La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine