Les défis du courrier indésirable

Fiche de l'Internet Society sur les politiques publiques

La prolifération des courriers indésirables présente une menace nuisible, coûteuse et en constante évolution pour les internautes. Les gouvernements peuvent aider à réduire l'impact du courrier indésirable en dissuadant les contrevenants par des lois efficaces et des mesures d'application des peines, des efforts anti courrier indésirable multipartites, l'adoption des meilleures pratiques, et l'éducation citoyenne sur les dangers du courrier indésirable.

Introduction

Le courrier indésirable, c'est-à-dire ces e-mails non sollicités qui encombrent nos boîtes aux lettres électroniques, sont un défi pour les internautes, les entreprises et les responsables politiques. Les estimations varient, mais certains suggèrent que plus de 100 milliards de messages de courrier indésirable sont envoyés chaque jour, ce qui représente jusqu'à 85 pour cent du trafic e-mail quotidien mondial.[1]

L'expression *courrier indésirable* se rapporte généralement à des communications non sollicitées électroniques (généralement e-mail) ou, dans certains cas, à des communications commerciales non sollicitées en envois groupés.[2] Certains font référence à ce genre d'e-mail simplement sous la dénomination de *spam.* Alors que l'activité du courrier indésirable est largement concentrée sous forme d'e-mails, le courrier indésirable est une menace en constante évolution qui s'est propagée dans presque tous les types de messageries électroniques, y compris les services mobiles de messages courts (SMS), les messages texte, les messages des médias sociaux, les systèmes de messagerie instantanée et les forums en ligne

Au-delà de la gêne et de la perte de temps résultant du tri, le courrier indésirable peut causer des dommages importants en infectant les ordinateurs des utilisateurs avec des logiciels malveillants capables d'endommager les systèmes et de voler des informations personnelles. Il peut également consommer les ressources du réseau.

Aujourd'hui, les types de courriers indésirables nuisibles les plus courants sont les messages d'escroquerie financières, les e-mails avec un logiciel embarqué de phishing[3], maliciels botnet[4] et/ou les maliciels de

[1] Cisco Systems, système de surveillance des menaces en temps réel SenderBase, http://www.senderbase.org.

[2] Sommet mondial de l'Union internationale des télécommunications sur les régulations de l'Union internationale des télécommunications, Article 7, Communications électroniques non sollicitées en envois groupés, http://www.itu.int/pub/S-CONF-WCIT-2012/en.

[3]Le phishing est généralement une tentative faite pour acquérir des informations sensibles, telles que des noms d'utilisateur, des mots de passe et des numéros de cartes de crédit, en prétendant être une entreprise digne de confiance au cours d'une communication électronique.

racket.[5] Les spammeurs sont très inventifs et ils ne dorment jamais ! Ils créent constamment des appâts toujours plus attrayants pour inciter les utilisateurs à ouvrir les messages contenant des logiciels malveillants. Et ils continuent à chercher de nouvelles listes d'adresses e-mail et des nouveaux médias de communication à cibler.

Considérations clés

Les gouvernements à travers le monde prennent des mesures juridiques pour lutter contre le courrier indésirable, même si jusqu'à présent ces efforts sont plus répandus dans les pays occidentaux et développés. Ce pourrait être parce que ces pays étaient confrontés à la menace de courrier indésirable plus tôt. Les pays qui ont adopté des lois en ce qui concerne le courrier indésirable ont aussi défini ce qu'ils considèrent comme du courrier indésirable. Ces pays ont rendu illégal le courrier indésirable, formé les consommateurs sur la meilleure façon de gérer le courrier indésirable, et dans certains cas, ont adopté et utilisé des mesures coercitives pour dissuader les spammeurs. Le résultat a été une baisse notable de leur courrier indésirable national, comme l'ont confirmé les Pays-Bas en 2010. Après que le gouvernement néerlandais ait adopté une loi anti-courrier indésirable, les utilisateurs dans le pays ont connu une baisse de 85 pour cent en courrier indésirable national. [6]Cependant, les spammeurs se sont sans doute déplacés vers les pays sans lois anti-courrier indésirable. En plus de la législation nationale individuelle, il existe une communauté internationale de lutte contre le courrier indésirable connu sous la dénomination LAP (London Action Plan), qui collabore sur l'application des lois anti-courrier indésirable transfrontalières et aux questions connexes.[7]

Les opérateurs de réseaux et la communauté technique ont développé des bonnes pratiques pour la gestion des menaces de sécurité réseau, y compris contre le courrier indésirable. Par exemple, le Groupe de travail Messaging, Malware and Mobile Anti-Abuse (M^{3}AAWG)[8]produit des documents sur les approches et les outils disponibles pour résoudre les problèmes de sécurité, tels que la description des mesures pour mieux gérer l'impact du courrier indésirable sur un réseau. [9] Le Spamhaus Project [10]surveille les sources et les occurrences de courrier indésirable pour fournir une protection du réseau en temps réel et travaille avec les forces de l'ordre pour lutter contre le courrier indésirable. Il existe aussi des organisations nationales et internationales qui travaillent sur les moyens de mieux gérer le spam, y compris GSM Association (GSMA), les registres Internet régionaux (RIR), l'Union internationale des télécommunications (UIT) et l'Internet Society.

Il existe de nombreux outils de blocage des courriers indésirables qui peuvent améliorer la façon dont les utilisateurs traitent le courrier indésirable. Mais peu importe l'efficacité des technologies de blocage des courriers indésirables, les utilisateurs finaux devront toujours être vigilants quant à la réception de courrier

---

[4] *Un maliciel* est un terme utilisé pour définir toute une gamme de logiciels hostiles ou intrusifs, y compris les virus informatiques, les vers informatiques, les chevaux de Troie (piratage) et autres programmes malveillants qui infectent les ordinateurs des utilisateurs avec des formes de codes et des scripts exécutables, des contenus actifs et autres logiciels intrusifs.

[5] Un Ransomware est un type de programme malveillant qui demande le paiement d'une rançon pour disparaître de l'ordinateur infecté.

[6] Réussite de la loi néerlandaise contre le courrier indésirable, https://www.spamexperts.com/about/news/dutch-anti-spam-law-has-success.

[7] London Action Plan, http://londonactionplan.org.

[8] Informations sur le Messaging, Malware, and Mobile Anti-Abuse Working Group (M^{3}AAWG), https://www.maawg.org/published-documents.

[9] En juin 2015, les groupes M^{3}AAWG et LAP ont publié« Opération Safety-Net : Pratiques modèles pour répondre aux menaces sur l'internet, par téléphone et sur mobile », https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf.

[10] Informations sur le Spamhaus Project : https://www.spamhaus.org/.

indésirable nocif, car aucun outil n'est parfait et les spammeurs inventent toujours de nouvelles façons d'envoyer des courriers indésirables. En outre, il peut être difficile pour les utilisateurs de reconnaître si un message est malveillant. Un rapport de Verizon en 2015 *DataBreach Investigations* indique que 23 pour cent des destinataires de courrier électronique ouvrent des messages de phishing et que 11 pour cent cliquent sur les pièces jointes, compromettant ainsi leurs ordinateurs et leurs systèmes en réseau.[11]

Défis

D'un point de vue général, le courrier indésirable est un défi en constante évolution technique, économique et un problème de sécurité pour de nombreux pays. En tant que tel, une approche multidimensionnelle est nécessaire pour répondre à ces défis. Plus précisément, le problème du courrier indésirable offre les défis suivants à considérer :

- Le courrier indésirable est un problème coûteux pour l'infrastructure de l'Internet et ses utilisateurs. Les gros volumes de courriers indésirables consomment les précieuses ressources du réseau, et sont un fardeau, en particulier dans les pays ayant un accès limité à l'Internet et une bande passante réduite. Les fournisseurs d'accès Internet (FAI) dépensent beaucoup d'efforts pour gérer ce trafic, et les utilisateurs finaux doivent être vigilants lors de l'ouverture de courriers indésirables qui contiennent des logiciels malveillants ou des escroqueries. Pour les abonnés aux données mobiles et ceux qui souscrivent à des services métrés, le coût de recevoir ou inconsciemment d'envoyer un grand nombre de messages de courrier indésirable peut être important. En outre, il y a des coûts de remise en état pour réparer les systèmes infectés et/ou attaqués par des logiciels malveillants permis par le courrier indésirable, ainsi que des coûts associés au vol des données aux utilisateurs.
- En général, les ressorts économiques liés au courrier indésirable penchent fortement en faveur des spammeurs. Les messages de courrier indésirable coûtent très peu à envoyer. En effet, la plupart des coûts sont couverts par les destinataires du message, les FAI, les utilisateurs infectés, ou les opérateurs de réseaux.
- La nature des courriers indésirables change avec l'introduction de nouvelles applications et nouveaux moyens d'échanger des données sur Internet. Les spammeurs évoluent dans leur capacité à utiliser ces plates-formes pour fournir des moyens plus intrusifs et dommageables pour voler des données personnelles, endommager les réseaux et infecter les systèmes.
- Le courrier indésirable affecte un large éventail d'internautes ; aucune organisation ne peut résoudre les menaces posées par le courrier indésirable par elle-même. Il faut une communauté mondiale, multipartite qui travaille ensemble pour résoudre le problème.
- Au-delà du préjudice direct aux utilisateurs et la charge supportée par les ressources du réseau, le courrier indésirable crée aussi insidieusement un manque de confiance de l'utilisateur et est considéré par certains comme un obstacle à l'utilisation de l'Internet et de l'e-commerce. Il a aussi un impact potentiellement négatif sur la réputation d'un utilisateur si son identité est volée par les spammeurs et utilisée pour envoyer des courriers indésirables.
- Les communautés impliquées dans le déploiement de mesures anti-courrier indésirable peuvent subir des représailles (par ex. les victimes d'attaques (DDoS) Distributed Denial of Service, de piratage), il est donc important que les membres des communautés globales qui combattent le courrier indésirable fournissent non seulement une assistance sur la façon de lutter contre le courrier indésirable, mais aussi un appui technique et d'autres supports contre les représailles.

[11] *Rapport d'enquête de 2015 sur la violation des données* par Verizon Corporation http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015-insider_en_xg.pdf.

Principes directeurs

L'Internet Society estime qu'une approche collaborative entre tous les acteurs concernés peut fournir les meilleures solutions d'atténuation du courrier indésirable et de protection de la sécurité. Cette approche générale est soulignée dans les principes de Sécurité collaborative de l'Internet Society, qui mettent l'accent sur une responsabilité partagée et collective entre les parties prenantes en ligne pour atteindre les résultats souhaités.[12]

Les gouvernements peuvent aider à combattre les courriers indésirables en :

- **Comprenant le paysage en constant évolution du courrier indésirable.** Les spammeurs font constamment évoluer leurs méthodes pour la diffusion de courrier malveillant. Les gouvernements devraient s'appliquer à être à jour sur les techniques d'envoi de courrier indésirable, les tendances et l'évolution des menaces. Ils peuvent également jouer un rôle clé en soutenant la recherche sur l'identification, le suivi, et l'atténuation des courriers indésirables et autres menaces en ligne, ainsi que l'élaboration de mesures connexes pour soutenir l'élaboration de politiques publiques. Ils peuvent d'autre part encourager les méthodes de respect de la confidentialité de l'information en partageant les informations en temps réel et les menaces avec les parties prenantes.
- **S'associer avec les parties prenantes pour réussir**. Le courrier indésirable est un problème à multiples facettes. Un éventail de parties prenantes jouent un rôle et doivent être impliquées dans l'élaboration de stratégies, de bonnes pratiques et des approches de mise en œuvre de mesures anti-courrier indésirable, y compris le développement d'outils d'atténuation du courrier indésirable et des logiciels malveillants. La coordination et les partenariats entre les parties prenantes du secteur public et privé devraient être développés afin de produire des solutions robustes contre le courrier indésirable. Des entités utiles à engager comprennent les coalitions anti-courrier indésirable et les groupes de travail (tels que M^{3}AAWG), les équipes d'intervention de la sécurité informatique, les opérateurs de réseaux, les fournisseurs d'accès Internet et les fournisseurs de services en ligne, la communauté technique de l'Internet, les groupes d'affaires et de défense des consommateurs, la société civile et d'autres ayant un intérêt dans la lutte contre le spam, les logiciels malveillants et d'autres activités malveillantes en ligne.
- **L'adoption d'une législation anti-courrier indésirable et l'application des mesures appropriées.** Comme indiqué précédemment, la législation anti-courrier indésirable, des lois fortes de protection des consommateurs et de vigoureuses mesures d'application des lois peuvent aider à dissuader les acteurs incriminés et à réduire la quantité de courrier indésirable envoyé et reçu dans un pays. [13]Les organismes gouvernementaux chargés d'appliquer les lois et règlements contre le courrier indésirable doivent être bien financés, publier les résultats des mesures d'exécution des lois, et faciliter le signalement du courrier indésirable et la distribution de logiciels malveillants par les internautes.
- **Collaboration avec des homologues internationaux.** Le courrier indésirable est un problème transfrontalier. La collaboration entre les gouvernements à travers le monde pour lutter contre le courrier indésirable, y compris les actions internationales d'application de la loi, est essentielle pour affronter avec succès la prolifération mondiale du courrier indésirable.
- **Éduquer et autonomiser les citoyens.** Les gouvernements devraient soutenir les secteurs public et privé lors d'initiatives d'éducation des internautes sur la façon de reconnaître et de se protéger contre le

[12] Principes de sécurité collaborative de l'Internet Society, http://www.internetsociety.org/collaborativesecurity.

[13]Une ressource complète pour connaître la législation contre le courrier indésirable est disponible à l'adressehttp://www.spamlaws.com. Des liens vers plusieurs approches législatives nationales se trouvent dans la Boîte à outils Anti-spam de l'Internet Society à l'adresse http://www.internetsociety.org/spamtoolkit.

courrier indésirable et les autres menaces en ligne. Les internautes doivent aussi être conscients de leur droit d'exercer un recours pour la perte ou les dommages causés par le courrier indésirable illégal et autres activités malveillantes en ligne.

Ressources supplémentaires

L'Internet Society a publié un certain nombre de documents et de contenus liés à cette question. Ceux-ci sont disponibles en téléchargement gratuit sur le site Web de l'Internet Society.

- Boîte à outils Anti-spam de l'Internet Society, www.internetsociety.org/spamtoolkit.
- Formation virtuelle de l' Internet Society : Spam et menaces sur la toile, http://www.internetsociety.org/what-we-do/inforum-learn-online/inforum-course-spam-and-online-threats.
- Petit guide sur les spams, http://internetsociety.org/spam/short-guide-spam.
- Historique du spam, http://www.internetsociety.org/doc/history-spam.
- *Combattre le spam : politique, approches techniques et sectorielles,*http://www.internetsociety.org/doc/combating-spam-policy-technical-and-industry-approaches.

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Genève, Suisse
Tél : +41 22 807 1444 • Fax : +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tél : +1 703 439 2120 • Fax : +1 703 326 9881
E-mail: info@isoc.org

bp-spam-20151030-fr