



COMMENT BLOGUER EN TOUTE SECURITE

TRUCS ET ASTUCES SUR COMMENT SECURISER
VOTRE BLOG ET VOTRE IDENTITE

BOGDAN BOTEZATU
EQUIPE DE COMMUNICATION ET D'ANALYSE DES E-MENACES

PARTICULIERS



Table des matières

Table des matières	3
<i>Déjà 147 millions de blogs.....</i>	<i>4</i>
<i>L'auto-hébergement ou le SaaS ?</i>	<i>5</i>
<i>Le blog et l'effet boomerang</i>	<i>5</i>
Spam visant les blogs.....	6
Malware visant les blogs.....	8
Hameçonnage et vishing.....	10
<i>Blog piraté. Que faire ?</i>	<i>12</i>
<i>Conseils de sécurité pour votre blog.....</i>	<i>14</i>

Déjà 147 millions de blogs

C'est en 1999 qu'on peut situer l'émergence d'un nouveau type de journalisme, appelé à gagner du terrain, notamment sous l'impulsion de deux plateformes de publications gratuites. A l'époque, personne n'avait imaginé que les blogs allaient devenir un des plus importants moyens d'expression sur Internet, ni qu'ils allaient métamorphoser le journalisme classique auquel nous étions habitués.

Il existe aujourd'hui environ 147 millions de blogs (recensés par [BlogPulse](#)), et, d'après les mêmes sources statistiques, 54.000 nouveaux blogs sont quotidiennement créés. La majorité des blogs sont des initiatives personnelles animées par une ou deux personnes, d'autres font partie de projets plus complexes liés à la communication d'entreprise, chacune dans le créneau qui lui est propre.

Ce guide présente les règles de base à respecter pour la sécurité des blogs et concerne plus particulièrement les blogs individuels, qu'ils soient hébergés directement sur le serveur des intéressés ou sur celui de fournisseurs de services spécialisés.

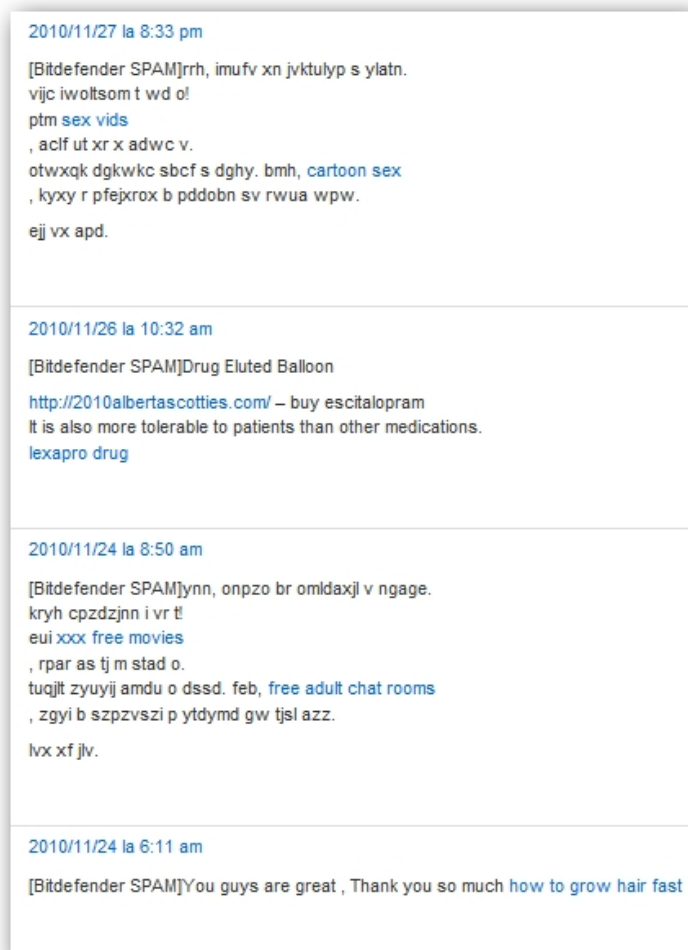
L'auto-hébergement ou le SaaS ?

Certains blogueurs optent pour l'ouverture d'un compte chez l'un des principaux développeurs de plateformes dédiées – notamment les blogueurs qui viennent juste d'être saisis par « la fièvre » générale – d'autres choisissent une solution personnelle, qui offre plus de liberté de gestion et de présentation, mais qui exige en même temps une extrême vigilance pour éviter les incidents.

Blogspot®, Wordpress® et LiveJournal® sont trois des fournisseurs de services les plus populaires offrant l'hébergement gratuit de blogs. Le service est ouvert à tous et sa maintenance est assurée par le fournisseur, ce qui veut dire que l'utilisateur n'a pas à se soucier des correctifs ni des questions de sécurité sur le serveur, parce qu'ils sont automatiquement pris en charge par le fournisseur. Malgré tout, bien qu'un blog hébergé par un fournisseur soit en général plus difficile à pirater, il arrive qu'il soit la proie de menaces, comme le spam et l'hameçonnage, dont les techniques sont décrites ci-dessous.

Le blog et l'effet boomerang

Quel que soit son type d'hébergement et son style de contenu, un blog est généralement créé et maintenu pour ajouter un plus à l'image d'une entreprise ou d'un particulier, et il peut même constituer une activité en soi. Les blogs publicitaires sont extrêmement répandus et sont une source de revenus pour une grande quantité de blogueurs. Il existe cependant des cas où un blog peut être détourné de son objectif initial – par exemple quand il a été compromis ou utilisé pour nuire à ses auteurs.



L'extension antispam de BitDefender identifie les commentaires de type spam et les envoie à la liste des messages nécessitant une approbation.

Spam visant les blogs

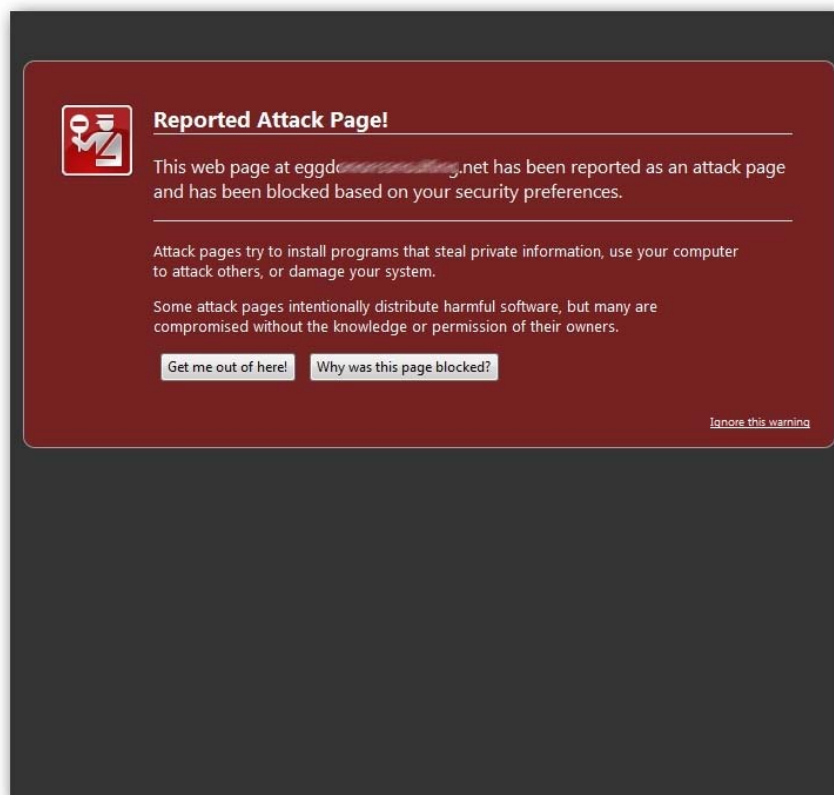
Le spam visant les blogs est le moyen le plus fréquemment utilisé pour salir la réputation de leurs auteurs. Le corps du message spam contient généralement des liens qui peuvent conduire le visiteur vers des contenus dangereux ou (pour le moins) obscènes. Un grand nombre de messages spam peut dramatiquement endommager l'usage du blog et rendre les informations correctes difficiles à trouver. Différents liens vers des sites web suspects peuvent également nuire à la réputation du blog dans les moteurs de recherche – un élément clé de la concurrence dans le commerce en ligne. Et, plus grave, les utilisateurs vont abandonner un blog imprégné de spam et il perdra ainsi sa base de lecteurs fidèles. La mauvaise nouvelle est que le spam visant les blogs est une des menaces qui affectent aussi bien les blogs hébergés par leurs auteurs que ceux qui le sont par des fournisseurs de services.

Remarque :

Environ 99 % de la totalité des messages spam postés sur les blogs et les forums sont envoyés par des bots – petits programmes informatiques écrits dans un langage script comme Perl ou Python. Ces bots, dont les objectifs sont particulièrement versatiles, sont aussi très faciles à contrer. Certaines des solutions les plus courantes consistent à forcer l'utilisation de JavaScript ou de cookies pour poster un commentaire. Les spam bots étant incapables de gérer le JavaScript ou les cookies, ils échoueront à transmettre le message. D'autres approches similaires consistent à ajouter un champ de texte caché via CSS, qui doit être vide. Face à ce champ vide dans le code source, le bot va essayer de le remplir avec n'importe quoi, ce qui empêchera en fait l'envoi du document.

Le bon côté des choses est qu'il est relativement facile de lutter contre le spam visant les blogs, à condition de posséder les outils adaptés et d'avoir correctement paramétré son blog. Les quelques conseils qui suivent pourront vous aider à éviter l'envoi de messages indésirables.

1. Configurez votre blog de manière à pouvoir vérifier automatiquement le premier commentaire d'un utilisateur. Les membres de la communauté se comportant correctement verront leur commentaire approuvé par un administrateur, et tous les messages qu'ils enverront par la suite seront automatiquement approuvés.
2. Configurez votre blog pour pouvoir vérifier automatiquement tous les commentaires sans exception. Ce mode est plus sûr que le précédent, mais il n'est pas tout à fait à la hauteur pour les blogs qui reçoivent quotidiennement des quantités de commentaires.
3. Installez une extension antispam dédiée. Si la plateforme Wordages a votre préférence, vous devriez adopter l'extension BitDefender Antispam. Cette solution gratuite utilise une API pour interroger le service BitDefender Antispam dans les nuages pour vérifier si un commentaire est légitime ou non.



Les alertes d'attaques sont susceptibles d'effrayer les utilisateurs qui ne reviendront peut-être plus jamais.

Malware visant les blogs

A moins que son auteur ait téléchargé des fichiers malveillants sur le compte d'hébergement de son blog, ce malware est en général le résultat d'une attaque réussie de piraterie contre le blog ou le serveur qui l'héberge.

Il existe de multiples moyens pour un attaquant de prendre le contrôle d'un blog et de son compte FTP. Ces attaques sont parfois planifiées d'excessivement près et impliquent un haut degré de connaissances technologiques. Tandis que, dans d'autres cas, les attaquants ne spéculent que sur l'association correcte d'un nom d'utilisateur et d'un mot de passe comme moyen d'accès.

1. Très souvent, les blogueurs voient leurs références de connexion compromises par des infections dues au malware sur leur ordinateur. Certains types de chevaux de Troie, comme les célèbres Facebook Hacker et le cheval de Troie iStealer, récupèrent les combinaisons nom d'utilisateur/mot de passe directement à partir des gestionnaires de mots de passe du navigateur. Enfin, et surtout, les mots de passe administratifs peuvent également être détectés par un tiers au moment où les utilisateurs non avertis accèdent à leur blog via une connexion Wiski non sécurisée dans un café Internet. Il se produit la même chose avec les références FTP – une mine d'or pour les cybercriminels qui projettent d'utiliser ces comptes pour stocker des fichiers malveillants, exploiter les paquets ou des pages de hameçonnage.

2. Le piratage d'un blog peut avoir lieu dans différentes circonstances, certaines d'entre elles échappant complètement à l'utilisateur. Par exemple, une mauvaise configuration du serveur ou un logiciel vulnérable peuvent entraîner l'exploitation effective du compte d'hébergement. D'autres attaques sont directement dues à une mauvaise installation du blog ou à une extension vulnérable. Des défauts *zero-day* dans le logiciel du blog peuvent également provoquer l'ouverture de brèches dans la sécurité, ce qui expose les références de connexion, ou mener le visiteur sans méfiance vers du malware.

Quelle que soit la façon dont le malware atteint un blog, il aura forcément un impact sur le classement du blog et son fonctionnement. La plupart des moteurs de recherche font constamment tourner des vérificateurs de pages indexées pour vérifier qu'elles ne présentent pas un danger quelconque pour ceux qui les consultent. Si elles sont détectées malveillantes, elles seront aussitôt étiquetées comme dangereuses dans les résultats des recherches, ce qui signifie que les utilisateurs suivant ces liens seront avertis que le contenu demandé peut mettre en danger le visiteur ou son ordinateur.

Le malware pour blogs ne se limite pas aux menaces électroniques présentes sur le compte correspondant, mais fait également référence à des scripts variés qui, une fois injectés dans le blog, peuvent rediriger l'utilisateur vers des sites tiers distribuant un contenu dangereux, ainsi qu'à des scripts utilisés par de faux logiciels antivirus pour simuler des analyses de système. Tout bien considéré, un blog infecté sera probablement radié par les moteurs de recherche et les clients fidèles n'y retourneront probablement jamais, de peur que la visite de ce blog n'endommage leur ordinateur.

```
Registration Service Provided By: GLOBEHOSTING EUROPE
Contact: +040.312249495

Domain Name: DOWN ██████████

Registrant:
██████████
Botezatu Bogdan (bcgdan.botezatu@██████████)
5B Basarabi St.
Iasi
██████████
RO
Tel. +040.██████1233424

Creation Date: 20-Sep-2010
Expiration Date: 20-Sep-2011

Domain servers in listed order:
ns24.roserve.net
ns23.roserve.net

Administrative Contact:
██████████
Botezatu Bogdan (bcgdan.botezatu@██████████)
5B Basarabi St.
Iasi
██████████
RO
Tel. +040.██████1233424
```

Les bases de données WHOIS fournissent des informations sur le propriétaire d'un nom de domaine.

Hameçonnage et vishing

Les blogueurs qui écrivent beaucoup sur eux-mêmes doivent prendre la mesure des risques de sécurité qu'ils encourent, non seulement pour leur intimité, mais par rapport au vol d'identité ou de coordonnées bancaires.

De nombreux blogueurs ont abondamment écrit sur des sujets concernant leur musique favorite, leurs acteurs préférés, l'amour, leurs passe-temps et marottes, et sur d'autres sujets divers apparemment anodins. Il est extrêmement facile d'écrire sur ces différents sujets, ou de partager des récits d'expériences avec les lecteurs mais, parallèlement, les blogueurs peuvent rendre publiques suffisamment d'informations pour permettre à des personnes malveillantes de se livrer à une attaque réussie d'hameçonnage ou de vishing (hameçonnage par téléphone).

Pour une meilleure compréhension de ces risques, imaginons le scénario suivant : un blogueur/une blogueuse s'achète un nouveau téléphone mobile, plus efficace et intelligent. Il peut ouvrir des documents PDF, il possède une connexion Wi-Fi (ou peut au moins se connecter via le GPRS à un blog, pour l'alimenter de nouvelles informations pendant qu'il voyage). Il est très courant parmi les blogueurs de parler de leurs nouvelles acquisitions d'une manière très personnelle et précise. Le scénario qui suit provient d'un message réellement posté sur un blog et légèrement modifié pour préserver l'identité de son auteur.

« Je viens juste d'acheter un nouveau téléphone portable pour pouvoir immédiatement raconter ce qui se passe dans ma vie. Je me suis acheté hier le nouveau PDA [nom de la marque] dans une boutique [nom de l'opérateur]. C'est tellement cool que c'est incroyable. »

```
Registrant:
Contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA

Domain name: ██████████.COM

Administrative Contact:
contactprivacy.com, ██████████.com@contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA
+1.4165385457

Technical Contact:
contactprivacy.com, ██████████.com@contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA
+1.4165385457
```

Des mécanismes de protection de la vie privée permettent de cacher les informations d'enregistrement sans empêcher de contacter le propriétaire.

Ensuite, imaginons que le message ci-dessus soit lu par une personne qui appelle le blogueur en se faisant passer pour un des employés de [nom de l'opérateur]. Le numéro de téléphone des blogueurs qui ont enregistré leur propre nom de domaine figure habituellement dans la base de données du registre, avec d'autres informations comprenant adresse postale de facturation, nom et prénom et adresse électronique personnelle.

« Allo, bonjour Monsieur ! Je suis [nom] de la société [opérateur], et j'ai deux ou trois questions à vous poser sur le téléphone [nom de la marque] que vous avez acheté hier chez [boutique]. Mais je dois d'abord vous demander de confirmer votre identité. Merci de me donner votre numéro de sécurité sociale, votre date de naissance et votre adresse pour vérification. »

Il ne s'agit que d'un scénario parmi d'autres pouvant conduire à un vol d'identité massif. En règle générale, plus vous en dites sur vous-même, plus il est facile pour les attaquants d'obtenir d'autres renseignements. Parler de vos plats favoris, d'acteurs ou d'activités au jour le jour peut leur servir de base pour deviner un mot de passe électronique, ou pour remplir les informations nécessaires à la récupération d'un mot de passe, soi-disant oublié, à partir d'un compte électronique.

Limiter les risques

Si vous possédez un nom de domaine enregistré à votre nom, assurez-vous que chaque interaction éventuelle avec une personne inconnue est gérée correctement. Si vous avez le moindre doute sur la légitimité de la personne sollicitant des informations personnelles de la part d'un organisme, vous avez intérêt à refuser de répondre et de rappeler en utilisant les coordonnées indiquées sur le site web de l'organisme en question.

Une autre possibilité est de demander à votre gestionnaire de noms de domaines d'activer sur votre compte l'option de protection WHOIS, qui remplacera vos coordonnées par celles appartenant à votre organisme de protection. Vos coordonnées resteront inaccessibles à des tiers, sauf s'il s'agit d'organismes légaux.

Blog piraté. Que faire ?

Se rétablir d'un acte de piraterie peut se révéler une expérience fastidieuse, et les conséquences d'une invasion réussie peuvent se manifester longtemps, mais le plus vite vous identifiez et résolvez les problèmes, moins votre blog sera endommagé. Voici une liste des premières mesures à prendre après la découverte d'une attaque.

1. Vous devez d'abord rendre votre domaine inaccessible aux utilisateurs humains comme aux moteurs de recherche. Comme tous les fichiers du site seront nécessaires pour des analyses et (sans doute) pour la restauration, il est recommandé de n'en supprimer aucun. Vous pouvez au contraire bloquer tout le trafic en renommant le fichier index.php et en créant à sa place un fichier vierge. Soyez prudent : n'oubliez pas de créer la page factice, sinon vous risquez d'exposer d'autres fichiers de votre compte FTP. Bloquer les moteurs de recherche les empêchera de détecter que votre blog est infecté et de l'étiqueter comme malveillant.
2. Faites une sauvegarde complète de votre dossier personnel en utilisant un client FTP et exportez ensuite manuellement la base de données en tant que fichier SQL.

3. Récupérez les journaux d'accès sur votre serveur web et stockez-les dans un emplacement sécurisé. Vous aurez besoin de ces journaux pour enquêter sur ce que les attaquants ont exactement fait sur votre site. L'analyse révélera comment ils s'y sont pris pour compromettre votre blog.
4. Faites une copie de tous les fichiers personnalisés que vous possédez, quels qu'ils soient. Il peut s'agir de thèmes, d'extensions et de fichiers téléchargés en tant que contenu, pratiquement de tout ce qui ne pourra plus être téléchargé de nouveau à partir du web. Ne gardez que ce qui vous semble nécessaire pour un redémarrage sans aucune perte de contenu.
5. Commencez par regarder dans les fichiers extensions et thèmes pour repérer des fragments de textes d'aspect bizarre. Portez une attention particulière aux lignes de texte du type « `eval(base64_decode(` » , suivies d'une série illisible de chiffres et de lettres, comme à l'insertion dans les scripts de noms de domaines que vous ne connaissez pas, (`<script src="http://[nomdedomaineinconnu]/nomdescript.php">` par exemple).
6. Consultez la base de données table par table et repérez toute trace éventuelle de lien suspect. Portez une attention particulière aux tableaux concernant les administrateurs, les paramètres de configuration et les articles postés sur le blog. Si vous trouvez un administrateur inconnu, supprimez-le immédiatement.
7. Une fois terminées les opérations d'inspection et de nettoyage, vous pouvez supprimer tous les fichiers de votre serveur web. Si les bases de données sont également atteintes, vous pouvez les supprimer et restaurer la copie que vous avez vérifiée manuellement.

8. Lancez le téléchargement du script de votre blog sur le serveur. Vérifiez que vous l'aviez bien obtenu du bon dépositaire. Il est obligatoire que vous téléchargiez la plus récente version du script du blog. Modifiez le fichier de configuration pour remplir les conditions de votre serveur web (utilisateur SQL, base de données, mot de passe, chemin du fichier et vos autres paramètres).
9. Vérifiez que vous n'avez pas paramétré les autorisations fichiers et dossiers à un niveau supérieur à celui strictement nécessaire à l'exécution du script. Configurer fichiers et dossiers en CHMOD 777 peut permettre à un attaquant d'écrire dans les dossiers et de réinjecter du code malveillant. Changez les mots de passe des administrateurs du blog et de l'accès FTP.
10. Renvoyez vos fichiers modifiés à leur emplacement correct via FTP. Videz le cache du navigateur et accédez à votre site web. Ensuite, recherchez votre blog avec un moteur de recherche en utilisant votre nom ou l'intitulé du blog comme mots-clés et suivez les résultats de la recherche fournis par le moteur. La plupart du temps, le malware vérifie le référent pour voir si le visiteur a eu directement accès au site ou s'est servi d'un moteur de recherche et ne se manifeste qu'aux visiteurs ayant suivi un lien.

Conseils de sécurité pour votre blog

Pour diminuer la probabilité d'être piraté il vous est conseillé de respecter quelques règles extrêmement simples :

- N'utilisez jamais de scripts provenant de téléchargements douteux et non officiels. Et surtout n'utilisez jamais de scripts déprotégés car non seulement c'est illégal, mais dangereux pour votre blog et votre serveur.

- Maintenez un compte FTP propre : ne mélangez pas le compte hébergeant votre blog avec d'autres scripts que vous voulez tester. Une vulnérabilité mineure dans le script d'un tiers peut compromettre votre blog. Effectuez toujours vos tests sur un serveur web local.
- N'ajoutez pas des extensions ou des thèmes qui ne servent à rien. Limitez-vous à ce dont vous avez vraiment besoin pour éviter de vous retrouver avec une extension ou un thème exploitables. Assurez-vous aussi que les extensions que vous souhaitez télécharger proviennent de sources auxquelles vous pouvez faire confiance. En cas de doute, consultez la communauté des utilisateurs.
- Faites régulièrement des sauvegardes de la base de données SQL. Utilisez une extension pour automatiser les opérations et récupérez les sauvegardes par courrier électronique ou via un deuxième compte FTP. Utiliser le même compte pour stocker les sauvegardes n'est pas une bonne idée, car un attaquant peut tenter de les falsifier ou même les supprimer après un piratage réussi.
- Utilisez des mots de passe robustes pour les comptes FTP et les utilisateurs administratifs. Ne les communiquez à personne, en aucun cas. Vous pouvez également installer une solution antimalware complète pour vous assurer que votre système est exempt de chevaux de Troie. Certaines attaques de blogs réussies ont été conduites en utilisant des noms d'utilisateurs et des mots de passe légitimes, interceptés par des keyloggers ou autres chevaux de Troie.
- Faites particulièrement attention à la façon dont vous sélectionnez votre fournisseur d'hébergement. Les sites payants sont généralement meilleurs que les gratuits et, puisque vous allez vous dépouiller d'un peu d'argent, vérifiez que vous allez obtenir des sauvegardes automatiques quotidiennes, un code d'accès et une configuration de serveur adaptée à votre script de blog.

Les informations et données contenues dans ce document sont la représentation de l'opinion de BitDefender® sur les sujets traités le jour de la publication. Ce document et les informations qui y sont contenues ne doivent pas être interprétés comme un engagement ou un accord de la part de BitDefender.

Même si toutes les précautions ont été prises lors de la rédaction de ce document, l'éditeur, les auteurs et les contributeurs ne pourront être tenu responsables en cas d'erreurs et/ou omissions. Aucune responsabilité ne peut non plus être engagée pour des dommages résultant de l'utilisation d'informations contenues dans ce document. De plus, les informations contenues dans ce document peuvent faire l'objet de corrections, sans annonce préalable. BitDefender, l'éditeur, les auteurs, et les contributeurs ne peuvent garantir la mise à disposition de nouveaux documents ou d'informations supplémentaires en rapport avec ce document-ci.

Ce document et les données contenues dans celui-ci n'ont qu'un but informatif. Si une assistance professionnelle est nécessaire, une personne compétente dans ce domaine devra être contactée. Ni BitDefender, l'éditeur, les auteurs ou les contributeurs ne peuvent être tenus responsables de dommages en résultant.

Le fait qu'un individu ou une organisation, un travail individuel ou collectif (incluant les documents imprimés, les documents électroniques, sites web, etc.) soient cités et/ou soient source d'informations n'implique pas que BitDefender, l'éditeur, les auteurs ou les contributeurs soient responsables des informations ou recommandations que ceux-ci pourraient fournir. Les lecteurs doivent prendre en compte que BitDefender, l'éditeur du document, les auteurs ou les contributeurs ne peuvent garantir la justesse de toute information après la date de publication, comme les adresses web et liens Internet listés dans le document, et qui pourraient avoir changé ou disparu entre le moment où ce document a été rédigé et publié, et le moment où il est lu.

Les lecteurs doivent se conformer aux lois internationales régissant la propriété intellectuelle, concernant toute partie de ce document. Aucune partie de ce document ne peut être reproduite, stockée, ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement, etc.) ou pour toute autre raison, sans la permission écrite de BitDefender.

BitDefender peut avoir breveté des applications, marques, droits d'auteur, ou toute autre propriété intellectuelle couvrant des sujets traités dans ce document. Sauf stipulation expresse dans un contrat de licence écrit de la part de BitDefender, ce document ne donne aucun droit sur les brevets, marques, droits d'auteur ou autre propriété intellectuelle.

Copyright © 2010 BitDefender. Tous droits réservés.

Tous les autres produits et noms d'organisations cités dans ce document le sont à simple but d'identification et sont la propriété et/ou marques de leurs propriétaires respectifs.