

## Protéger votre réseau : comment atténuer les effets néfastes des logiciels espions à l'intérieur des organisations

Quelques techniques qui permettront aux organisations de réduire les frais de services techniques informatiques, l'utilisation abusive des ressources du système d'exploitation, et la perte de productivité suite aux attaques de logiciels espions et malveillants.

### Éduquer votre personnel et tous les utilisateurs du réseau

- Imposer une charte d'utilisation précisant les programmes non autorisés susceptibles d'être bloqués au niveau de la passerelle et supprimés des postes de travail.
- Renseigner tout utilisateur de votre réseau sur les dangers des programmes et services « gratuits », qui cachent souvent des logiciels malveillants responsables d'importants ralentissements, de l'intrusion des fenêtre-pub d'entrée (pop-ups), et du vol informatique. (cf. *Protéger votre ordinateur: comment éviter et supprimer les logiciels espions*, pour des renseignements supplémentaires.)
- Former votre équipe d'assistance technique à reconnaître les symptômes subtils des logiciels espions (ralentissement des logiciels et lors du démarrage, performance irrégulière, plantage) pour bien identifier les causes premières et prendre les contre-mesures adaptées.

### Bloquer les logiciels espions au niveau de la passerelle

Les conseils suivants vous permettront de paramétrer les passerelles mandataires (proxy) ou pare-feu afin de filtrer les logiciels espions avant qu'ils n'atteignent votre réseau :

- Établir des règles pour empêcher les téléchargements « drive-by » qui infectent les ordinateurs dès lors d'une visite à leur site hôte (fichiers CAB et OCX non approuvés).
- Définir des règles pour empêcher le téléchargement à partir des sites connus pour diffuser des logiciels espions (repertoriés dans les listes de filtrage de contenu).
- Définir des règles pour empêcher le téléchargement des fichiers exécutables provenant de sites suspects ou à haut risque (sites appartenant à des secteurs où l'on retrouve souvent des logiciels espions).
- Vérifier les fichiers au niveau de la passerelle pour repérer d'éventuels codes-espions connus.
- Établir des règles pour bloquer la communication avec les sites hôtes des logiciels espions du type « phone home » ; signaler tous les postes de travail susceptibles d'être infectés.
- Analyser les journaux des communications pour déceler les destinations dont la fréquence des visites et (où) le trafic sont anormalement élevés.
- Mettre en place une protection anti-pourriel efficace afin de limiter les occurrences de logiciels espions cachés dans les pourriels.

### Protéger les ordinateurs d'entreprise contre les logiciels espions

Les applications anti-logiciels espions de bureau peuvent détecter et supprimer les logiciels espions qui essaient de s'exécuter. Pour une performance optimale, veillez à respecter les consignes suivantes :

- Mettre à jour les logiciels et les fichiers de signatures.
- Préférer des applications de sécurité de bureau qui permettent une gestion et un déploiement centralisés.

- Pour assurer une défense en profondeur, déployer les technologies de plusieurs chercheurs en anti-logiciels espions, aux niveaux du bureau et de la passerelle.
- Actualiser les rustines (patch) du système d'exploitation et du navigateur pour minimaliser la vulnérabilité dûe aux failles de sécurité.
- Le réglage minimum des options de sécurité et de vie privée des navigateurs ne doit jamais être en dessous de « medium ».
- Interdire la navigation sur internet pour tout utilisateur connecté avec des privilèges d'administrateur.
- Maintenir une liste des logiciels et (ou) de fichiers exécutables approuvés, et faire un contrôle hebdomadaire du réseau pour repérer d'éventuelles entrées non-conformes.
- Pour les ordinateurs atteints d'infections chroniques de logiciels espions, envisager de tout réinstaller.

Ce contenu peut être reproduit librement sous réserve du respect de son intégrité, et de la citation de sa source : l'Antispyware Coalition (ASC). Pour plus de détails consultez <http://www.cdt.org/about/copyright.php>.