

POURQUOI LES SOLUTIONS ANTIVIRUS NE PROTÈGENT PAS CONTRE LES LOGICIELS ESPIONS



NETWALKER
www.netwalkerstore.com



Sommaire

Introduction	1
Pourquoi il faut se préoccuper des logiciels espions	1
Prévalence et aggravation du risque des logiciels espions	2
Facteurs de menaces	3
Codes malveillants : virus, vers et logiciels espions	3
Pourquoi les logiciels espions sont plus dangereux que les virus	3
Exploitation de la vulnérabilité et actes intentionnels	4
Actes non intentionnels : le facteur humain	5
Comment reconnaître une infection par logiciel espion	5
Études de cas : répercussions des logiciels espions sur l'activité	6
Pourquoi les logiciels gratuits ne sont pas vraiment gratuits	6
Pourquoi le « tout-en-un » n'est pas suffisant	7
Sélection d'un fournisseur de solution contre les logiciels espions	8
Webroot, fournisseur de la meilleure protection contre les logiciels espions	9
Conclusion et recommandations	10
À propos de Webroot	10

Introduction

L'environnement actuel de l'information n'est plus ce qu'il était. Les entreprises de toutes tailles utilisent énormément Internet et les systèmes technologiques comme principaux outils de communication. Tandis que la dépendance à Internet augmente pour la reconnaissance de la marque, l'avantage sur la concurrence et le commerce électronique, elle s'accompagne d'avantages et de risques. Parmi les avantages figurent la capacité de communiquer avec la clientèle, les fournisseurs et les acteurs clés de l'activité ainsi que la possibilité de se faire connaître ; les risques incluent celui d'exposer l'infrastructure informatique à une montée de menaces en constante évolution, d'où une vulnérabilité accrue. Le bon équilibre entre la technologie et les menaces peut garantir le succès de votre entreprise. Un déséquilibre peut être synonyme de catastrophe.

C'est dans cet environnement complexe que les pirates informatiques experts de la « cybercriminalité » visent et attaquent les infrastructures technologiques non protégées, dans leur propre intérêt financier illégal. Et pour ce faire, ils ont recours aux moyens les plus efficaces et lucratifs : les logiciels espions. Les organisations de 200 à 5 000 employés sont particulièrement sensibles aux logiciels espions, car elles sont suffisamment grandes pour attirer l'attention en tant que cibles, mais en raison de leur petite taille, ne déploient pas de stratégie robuste pour se garder de cette menace.

De nombreuses entreprises de cette catégorie se caractérisent par une organisation informatique mûre, et pourtant, elles n'emploient pas d'équipe de sécurité centralisée ou dédiée. En outre, ces organisations sont très susceptibles de posséder des bureaux distants et d'avoir recours au travail nomade, les employés éloignés travaillant sans l'avantage d'un support ou d'une gestion informatique sur site. Pour aggraver la situation, les sociétés de cette taille comptent bon nombre d'employés qui stockent sur leur ordinateur des données personnelles directement visées par les pirates par le spam (courrier électronique non sollicité) ou le phishing (hameçonnage ou courrier électronique hameçon) ; les pirates revendent ensuite ces données, par l'intermédiaire d'un marché noir virtuel très sophistiqué. Dans ce type d'entreprises, les solutions et procédures de sécurité centralisées, robustes et dédiées sont indispensables.

Pourquoi il faut se préoccuper des logiciels espions

En haut de la liste des priorités de tout service informatique actuel figurent les logiciels espions. Les logiciels espions portent bien leur nom. Ils sont particulièrement sournois et coûteux, car ils fonctionnent en secret et défient souvent la détection, sauf en présence de programmes spécialement développés pour les détecter. Les entreprises qui utilisent les logiciels antivirus pour se protéger des logiciels espions (ce qu'on appelle en anglais le « featureware », ou programmes « tout-en-un ») commettent une grave erreur. Les produits antivirus, en particulier les produits généralistes ou tout-en-un n'intègrent pas les renseignements détaillés qu'il leur faut et n'ont pas les capacités de recherche nécessaires pour repousser la menace. En outre, les logiciels gratuits (en anglais, « freeware »), ou « gratuits », n'ont pas les qualités ni la sophistication nécessaires aux entreprises pour protéger leurs ressources informatiques. Ce fait est une évidence, lorsque l'on compare leurs taux de détection à ceux des solutions autonomes de lutte contre les logiciels espions. Les antivirus détectent généralement 30 à 40 % moins de logiciels espions (source : rapports Veritest, 2006).

Les programmes gratuits contre les logiciels espions en détectent encore moins.

À la différence des virus, les logiciels espions sont pilotés par des motivations financières qui conduisent leurs auteurs à une innovation technique rapide et une distribution très large. Les logiciels espions peuvent être difficiles à localiser et requièrent des méthodes proactives et spécialisées de détection. La suppression des logiciels espions est également complexe et problématique, puisque les nouvelles versions de programmes malveillants sont spécialement conçues pour s'incruster dans les systèmes. Les répercussions des logiciels espions sur l'activité sont très importantes : ces programmes compromettent la confidentialité, menacent les actifs et affectent la productivité au-delà des dégâts causés par les virus. Bien que dans certaines juridictions des lois soient en place, selon lesquelles les logiciels espions sont illégaux, la plupart des experts s'accordent pour dire qu'elles n'ont qu'un effet minime : elles ne découragent pas les pirates et ne remédient certainement pas au problème. La seule vraie façon de se protéger contre une menace technologique est précisément la technologie. Les logiciels spécialisés et les meilleures pratiques opérationnelles sont les outils indispensables à la protection de toute entreprise désireuse de se défendre contre cette menace grandissante.

Prévalence et aggravation du risque des logiciels espions

Depuis plusieurs années, les logiciels espions et autres programmes indésirables sont parfaitement capables de contourner les défenses traditionnelles telles que les murs pare-feu et autres solutions de périmètre, puisqu'ils se déguisent en programmes légitimes et pénètrent les ports bien établis et toujours ouverts des murs de protection. Une fois installés sur un système, ils se déguisent de nouveau en programmes légitimes et communiquent librement sur Internet par le biais des ports TCP qui sont généralement laissés sans protection.

« Les logiciels espions et les courriers hameçons sont en fait des problèmes bien plus graves que les virus pour les consommateurs », déclare John Pescatore, expert en sécurité, vice-président et chercheur chez Gartner Research, Inc. Il prédit en effet que la menace des logiciels espions ira en grandissant. D'autres rapports le suggèrent aussi, y compris un rapport de 2006 établi par ScanSafe, qui indique que le nombre de menaces par logiciels espions a augmenté de 254 % l'année dernière, tandis que les virus étaient sur le déclin.

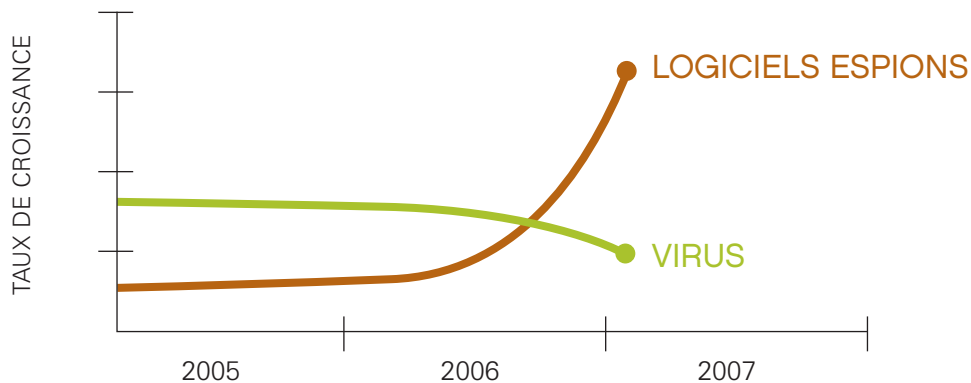


Figure 1 – Un rapport de 2006 établi par ScanSafe indique que le nombre de nouvelles menaces par logiciels espions a augmenté de 254 % l'an dernier, alors que le nombre de virus était en baisse.

Facteurs de menaces

Ces deux dernières années, les chercheurs ont remarqué un basculement considérable dans la démographie des pirates informatiques et dans leurs motivations. Il ne s'agit plus d'individus mécontents et motivés par le seul défi technologique ou le désir de faire étalage de leurs prouesses techniques. Le délit informatique d'aujourd'hui est motivé par l'appât du gain et est de plus en plus le résultat d'attaques par des groupes d'individus, avec une tendance croissante à l'engagement du crime organisé. Le paysage des menaces peut être compliqué ; les menaces se divisent toutefois en plusieurs catégories. Les programmes malveillants incluent les codes malveillants, l'exploitation de la vulnérabilité et les actes intentionnels par des tiers ; mais un autre type de vulnérabilité souvent négligé et sous-estimé est celui des actes non intentionnels causés par l'erreur humaine.

Codes malveillants : virus, vers et logiciels espions

La définition classique du code malveillant est le code inséré sans l'accord du propriétaire du système, spécifiquement afin de nuire au système. Parmi les types de code malveillant, il faut compter les virus, les vers et les logiciels espions.

L'Institut national américain de normes et de technologie, le NIST (US National Institute of Standards and Technology), a défini un virus comme un segment de code qui se reproduit en fixant des copies de lui-même à des exécutables existants. Un ver est un programme qui se reproduit et qui cause l'exécution de son nouvel exemplaire. Un ver de réseau est un ver qui se reproduit sur un autre système, en utilisant des installations communes du réseau, et qui entraîne l'exécution de son nouvel exemplaire sur ce système. Virus et vers recueillent la plus grande partie de l'attention des médias, parce qu'ils se propagent rapidement et les dégâts qu'ils causent sont visibles et manifestes. Si l'on compare le « cyber crime » à une carrière professionnelle, les créateurs de virus sont généralement des nouveaux venus de l'industrie du délit informatique. Les auteurs de virus et de vers peuvent être comparés aux tagueurs : ils veulent monopoliser l'attention et causer autant de dégâts que possible.

VIRUS / WORMS



- Se reproduit en se fixant aux fichiers
- Se propage rapidement
- Dégâts visibles
- Inconvenient

SPYWARE



- Surveillance/contrôle/enregistre les frappes au clavier
- Vole les mots de passe et les données personnelles
- Dégâts cachés
- Motivations financières

Pourquoi les logiciels espions sont plus dangereux que les virus

Autre catégorie de codes malveillants : le logiciel espion que la Commission fédérale américaine du Commerce (FTC - Federal Trade Commission) a défini comme étant un élément installé sur votre ordinateur sans votre consentement. Un logiciel espion surveille et contrôle l'usage de votre ordinateur et il est conçu pour s'introduire à votre insu au cœur de votre système. C'est pourquoi, à terme, il est souvent plus dangereux que le virus visible qui interrompt votre système. Les auteurs de logiciels espions sont très différents des auteurs de virus et de vers, puisqu'ils cherchent principalement à éviter toute détection. Plus ils fonctionnent sans être détectés, plus ils causent de dégâts.

La nature furtive du logiciel espion en fait un ennemi particulièrement dangereux : ce que vous ne voyez pas peut vous nuire. De nombreuses organisations ont un faux sentiment de sécurité, car elles ne voient pas les répercussions négatives sur leurs systèmes ou leurs réseaux.

Les enregistreurs de frappe sont particulièrement dangereux : ils enregistrent toutes les frappes au clavier et transmettent ces informations à un autre système. Armé d'informations transmises par la saisie au clavier, telles que les noms d'utilisateur et les mots de passe, un pirate informatique peut prendre le contrôle de votre système et même accéder à vos comptes en banque en ligne. Autre variante du logiciel espion : ce que l'on appelle en anglais le « ransomware », ou « logiciel de prise d'otage ». Ce type de programme crypte vos données, vous empêchant ainsi d'y accéder. Le pirate vous demande alors une rançon contre laquelle il vous donnera les informations nécessaires pour débloquer votre ordinateur.

L'autre danger du logiciel espion est sa capacité à viser des personnes spécifiques ou des informations critiques. Le vol de propriété intellectuelle, plus particulièrement celui des secrets industriels, est un problème croissant pour de nombreuses organisations. Un logiciel espion tel qu'un enregistreur de frappe peut aider très efficacement le voleur de propriété intellectuelle. La nature furtive du logiciel espion peut également contribuer à une vulnérabilité à long terme au cours de laquelle le programme réside en permanence, à l'insu de tous, sur le système visé.

Au printemps 2007, une chaîne très importante de magasins au détail a révélé que des pirates avaient pénétré dans les systèmes de son exploitation commerciale, et accédé aux informations de cartes de paiement détenues par ses magasins des États-Unis et de Porto Rico. Les experts estiment que quelque 45,7 millions de cartes de paiement ont ainsi été dérobés. À ce jour, la fraude liée à cet incident s'élève à plus de 8 millions de dollars. Lorsque l'on considère qu'il en coûte aux établissements financiers 10 dollars pour remplacer chaque carte et 180 dollars pour traiter chaque appel, on estime que cette brèche de sécurité coûtera 1,7 milliard de dollars en dommages et intérêts. Les dommages indescriptibles à la marque restent à définir.

Exploitation de la vulnérabilité et actes intentionnels

L'exploitation de la vulnérabilité concerne la grande taille et la complexité des logiciels et progiciels actuels. En effet, ils présentent souvent des faiblesses connues au niveau de leur conception, qui permettent aux pirates de profiter de la vulnérabilité à leur avantage. Ces failles exploitables dans le code des logiciels permettent aux pirates de charger ou d'installer des programmes malveillants, tels que les logiciels espions et les virus. Les utilisateurs d'ordinateurs et les services informatiques doivent appliquer avec diligence les correctifs de sécurité.

Les actes intentionnels par des tiers sont, par exemple, le piratage pur et simple, mais aussi les attaques indirectes telles que les attaques par saturation, ou DDOS (Distributed Denial of Service Attack – Attaque par saturation du service). Dans ce cas de figure, les réseaux d'ordinateurs contrôlés par les pirates et leurs robots tentent de saturer les réseaux ciblés par des messages ou des requêtes et de ce fait, le système visé devient incapable de fonctionner. Souvent, ces attaques sont dirigées contre les serveurs Web de haut profil. Elles peuvent entraîner le blocage complet d'une entreprise, voire d'un pays tout entier, et des pertes financières aux conséquences dramatiques pour les sites de commerce électronique.

En février 2007, une attaque par saturation très importante a été lancée contre plusieurs serveurs racines de systèmes de noms de domaines (DNS), véritables épines dorsales d'Internet. L'enquête a pu remonter jusqu'à ce que l'on appelle un réseau de zombies (en anglais, « botnet », ou réseau de robots) d'origine sud-coréenne. L'un des serveurs racines DNS était sous le contrôle du département américain de la Défense. Le monde entier a eu peur d'une attaque informatique en guise de représailles, voire d'une attaque militaire. La meilleure manière pour une entreprise de se garder d'une attaque par saturation et d'y survivre consiste à déployer une stratégie de sécurité robuste qui inclut les adresses IP supplémentaires, les murs pare-feu, les systèmes de prévention des intrusions et la protection contre les programmes malveillants en couches.

¹ Source : Département américain de l'Intérieur, Bureau de l'Inspecteur Général - Complaisance excessive, usage personnel d'Internet au Département de l'Intérieur (Sept. 06)

La nature furtive du logiciel espion en fait un ennemi particulièrement dangereux : ce que vous ne voyez pas peut vous nuire. De nombreuses organisations ont un faux sentiment de sécurité, car elles ne voient pas les répercussions négatives sur leurs systèmes ou leurs réseaux.

Actes non intentionnels : le facteur humain

Aucune technologie, aussi bonne soit-elle, ni aucun code légal ne pourraient prévenir l'élément humain de l'introduction de programmes malveillants sur les ordinateurs. Les entreprises sont des groupes de personnes. Ces personnes sont des utilisateurs d'ordinateurs et passent beaucoup de temps au bureau à composer des messages personnels, à payer leurs factures en ligne et à surfer sur Internet. Une agence fédérale américaine a signalé qu'en l'espace d'un an, l'équivalent de 50 employés à plein temps passait tout son temps à surfer sur des sites Web prohibés, véritables foyers d'infection par logiciels espions¹. Le même rapport indiquait que cet abus des ressources Internet coûtait potentiellement au département plus de 2 millions de dollars par an, en perte de productivité.

Récemment, des pirates ont réussi à transférer près d'un demi-million de dollars des fonds généraux d'une ville de Californie, vers diverses banques dans tout le pays. Le trésorier de la ville a accidentellement téléchargé un programme enregistreur de frappe qui a permis aux pirates d'obtenir les coordonnées de connexion au compte en banque et le mot de passe. Bien qu'une partie de l'argent ait été récupérée, cet exemple illustre parfaitement l'élément humain de la vulnérabilité au piratage informatique.

Les utilisateurs d'ordinateurs doivent être éduqués sur les activités en ligne qui entraînent une infection des ordinateurs par logiciel espion. L'ouverture d'applications de partage de fichiers, de programmes résidant en mode fenêtre ou de pièces jointes inconnues aux messages électroniques, est fortement susceptible d'entraîner une infection. Il n'est pas rare que les téléchargements de programmes gratuits, de musique, d'économiseurs d'écran, de papiers-peints et autres, s'accompagne de programmes indésirables dont certains sont des logiciels espions. Non seulement, il est indispensable d'éduquer les utilisateurs sur le besoin de se protéger contre les programmes malveillants, mais les personnes individuelles autant que les entreprises doivent assumer leurs responsabilités de « cyber citoyens » et apprendre à assurer leur sécurité en ligne.

Comment reconnaître une infection par logiciel espion

Une bonne pratique important consiste à reconnaître qu'un logiciel espion a infecté un ordinateur particulier. Parmi les symptômes visibles de l'infection figurent ceux-ci :

- Barrage de fenêtres-pubs non sollicitées
- Prise en orage du navigateur Internet : le site Web qui s'affiche n'est pas celui dont l'adresse figure dans la barre d'adresse
- Changement soudain ou répété de la page d'accueil Internet de l'ordinateur
- Nouvelles barres d'outils inattendues et non sollicitées
- Nouvelles icônes inattendues et inconnues dans la barre système en bas de l'écran
- Problèmes de défaillance de touches ou non-fonctionnement de certaines touches
- Messages d'erreur aléatoires
- Dégradation des performances avec longs retards à l'ouverture des programmes ou à la sauvegarde de fichiers.

Toutefois, les logiciels espions les plus dangereux restent ceux qui ne peuvent pas être visiblement détectés

Études de cas : répercussions des logiciels espions sur l'activité

La nature furtive du logiciel espion en fait un ennemi particulièrement dangereux : ce que vous ne voyez pas peut vous nuire. De nombreuses organisations ont un faux sentiment de sécurité, car elles ne voient pas les répercussions négatives sur leurs systèmes ou leurs réseaux.

Les organisations prennent pour argent comptant la devise « pas de nouvelles, bonnes nouvelles ». En matière de logiciels espions, rien n'est pourtant moins vrai ! De nombreuses entreprises utilisent des antivirus populaires et en tête du marché pour se défendre contre les logiciels espions, une erreur très coûteuse. Une grande chaîne de magasins de décoration intérieure, par exemple, a observé une hausse dramatique du nombre d'appels à son équipe de support technique : les systèmes des employés avaient ralenti pour atteindre des niveaux de lenteur totalement inacceptables. Le support technique a réagi en passant des centaines d'heures à reproduire les ordinateurs infectés. Après un nombre d'appels similaires, l'équipe du service informatique s'est doutée que la source était très probablement une infection par logiciel espion.

À l'instar de nombreuses organisations, la chaîne de magasins n'avait ni protocole ni processus spécifiques pour l'identification et le traitement des dommages potentiels causés par les logiciels espions. Elle pensait que son antivirus suffirait, puisque le développeur du produit déclarait que son programme était capable d'assurer une telle protection. Après enquête, la société a découvert que de nombreux employés dispersés au sein de l'entreprise avaient également ajouté aux systèmes des couches de différentes solutions gratuites. Aucune des solutions en place, payantes ou non, n'a réussi à identifier l'épidémie de logiciels espions. Depuis l'installation d'une solution spécifique de lutte contre les logiciels espions, l'entreprise a supprimé avec succès 6 900 instances de programmes publicitaires nuisibles, 586 chevaux de Troie et 21 programmes de surveillance malveillants.

Un cas similaire s'est produit à l'Université polytechnique de l'État de Californie (CalPoly). CalPoly compte 18 000 étudiants et son enseignement académique rigoureux jouit d'un grand renom. Naturellement, la gestion de la sécurité sur un site académique d'une taille pareille n'est pas sans difficultés. L'université était obligée de reconstruire entre 40 et 50 ordinateurs par mois, à raison de 4 à 5 heures par ordinateur, du fait des problèmes causés par les logiciels espions. À l'instar de la chaîne de magasins de décoration, l'université utilisait un antivirus développé par une grande société, et se croyait protégée des logiciels espions. Elle n'avait aucune solution spécifique de lutte contre les logiciels espions, ni de procédure nécessaire pour minimiser les dépenses, les répercussions et les conséquences des infections. CalPoly a installé une solution dédiée et depuis ce déploiement, elle a identifié plus de 100 000 infections potentielles par logiciels espions. Non seulement, les logiciels espions ont été identifiés, mais l'équipe informatique de l'université économise maintenant près de 250 heures par mois en support technique, d'où une économie de 50 000 dollars en main-d'œuvre.

Pourquoi les logiciels gratuits ne sont pas vraiment gratuits

Les logiciels gratuits ou « partagiciels » sont une autre alternative à la solution dédiée. Les logiciels gratuits sont, comme leur nom l'indique, des logiciels gratuits qui se téléchargent sans frais. Bien que cette approche soit apparemment plus économique que l'emploi d'une solution commerciale, il est régulièrement démontré qu'elle peut vous coûter très cher. Les organisations qui fournissent les logiciels gratuits dépendent de la contribution de bénévoles pour leur financement et faute de fonds, elles ne parviennent pas toujours à suivre l'avance rapide des développements pirates. Les logiciels gratuits étant entretenus par une équipe de bénévoles au penchant technique, leur qualité n'est pas toujours à la hauteur des normes rigoureuses et de la complexité des solutions commerciales ; ils reflètent simplement le nombre de développeurs présents au moment de la création du code pour arrêter les logiciels espions.

Les logiciels gratuits sont un poids supplémentaire pour les services informatiques déjà surchargés. Ils ne sont pas gérés de manière centralisée, et les utilisateurs doivent mettre les définitions à jour manuellement, faire eux-mêmes l'analyse de leurs systèmes et déterminer eux-mêmes la légitimité des programmes installés sur leur ordinateur. Le fait de compter sur les employés pour gérer les problèmes liés aux logiciels espions crée un risque énorme en environnement d'entreprise.

Les gratuiciels sont réputés pour leurs capacités d'analyse système limitées, et il est prouvé qu'ils n'éliminent qu'une fraction des logiciels espions sur un ordinateur infecté. (Selon une critique récente dans le magazine PC Pro, le gratuiciel populaire Spybot Search & Destroy ne détecte et ne supprime qu'un peu plus de 50 % des logiciels espions et programmes publicitaires malveillants. Testé sur sa capacité à bloquer l'installation de nouveaux logiciels espions, Spybot n'arrête que 36 % des installations malveillantes.) En outre, ces programmes gratuits sont rarement mis à jour, lorsqu'ils le sont. Les auteurs de logiciels espions, par ailleurs, affinent leurs techniques très fréquemment. Ce manque d'actualisation de la protection permet aux pirates de garder une longueur d'avance et de rendre votre système vulnérable aux infections répétées. En outre, du fait de leurs pratiques de développement inappropriées, les gratuiciels peuvent déstabiliser un ordinateur et aucun support technique n'est offert si quelque chose se passe mal.

Les entreprises qui adoptent une philosophie d'utilisation des logiciels gratuits s'exposent en outre à des conséquences judiciaires. En effet, la plupart des solutions gratuites sont destinées à des ordinateurs individuels grand public, et non au déploiement à grande échelle dans un environnement d'entreprise. Les « petits caractères » du contrat de licence spécifient généralement que le déploiement du gratuiciel en entreprise requiert le paiement d'une licence d'utilisation. Face à cela, les services juridiques et informatiques choisissent de ne pas payer pour ces solutions loin d'être optimales.

Pourquoi le « tout-en-un » n'est pas suffisant

L'approche « tout-en-un », par laquelle les fonctions d'un produit sont exagérées et promues dans le cadre du fonctionnement global du produit (« featureware »), présente un caractère inapproprié qui a trait à la dynamique des grandes entreprises qui développent ce produit. Dans ces grandes entreprises, chaque unité commerciale manœuvre pour se placer avantageusement et obtenir le plus de ressources possible ; ces unités ne s'engagent pas à effectuer un développement qui profiterait au client. Cela est particulièrement vrai dans les environnements de sécurité où les grands fournisseurs ont augmenté leur capacité en acquérant de petites entreprises indépendantes, et non en développant les capacités spécifiques nécessaires pour traiter des menaces actuelles ou prévisibles. L'approche de type « boulonnage » tend à consommer des ressources de traitement et à compliquer les choses lorsqu'un client a besoin d'un support technique.

Autre manque à gagner de l'approche généraliste et non spécialisée : le manque de recherche focalisée sur l'ambition de devenir le meilleur de sa catégorie. Les développeurs généralistes cherchent simplement à compléter leur ligne de produits. Les fournisseurs spécialisés dans les solutions de sécurité, en particulier les solutions de lutte contre les logiciels espions, comprennent désormais parfaitement la menace unique que représentent les logiciels espions et autres programmes malveillants de cette catégorie. En outre, comme il s'agit de chercheurs très engagés dans le travail portant exclusivement sur cette catégorie de programmes, ils sont généralement bien mieux placés pour percevoir les tendances des attaques à plus long terme.

D'autres utilisateurs d'ordinateurs comptent sur les suites logicielles de sécurité « tout-en-un » pour se protéger des logiciels espions. La plupart de ces solutions ont commencé en tant qu'antivirus et se sont vu ajouter une technologie limitée contre les logiciels espions après coup. Les logiciels espions évoluent particulièrement vite. La protection requiert donc une expertise tout à fait spéciale. Comparées aux solutions dédiées, les solutions gratuites ou tout-en-un détectent et éliminent moins de logiciels espions. Les clients croient être protégés, parce que la case « logiciels espions » est cochée sur l'emballage de leur produit, mais la technologie que renferme ce produit ne suffit pas à assurer la protection nécessaire.

	WEBROOT® ANTISPYWARE	SOLUTION TOUT-EN-UN	SOLUTION GRATUITE
Blocage et protection en temps réel	OUI	OUI	NON
Capacités de détection à la racine	OUI	OUI	NON
Mises à jour fréquentes de définitions	OUI	OUI	NON
Mises à jour automatiques de définitions	OUI	OUI	NON
Mises à jour automatiques du programme	OUI	OUI	NON
Capacités de reporting	OUI	OUI	NON
Gestion centralisée	OUI	OUI	NON
Protection officiellement en tête du marché	OUI	NON	NON
Équipe de recherche dédiée	OUI	NON	NON
Support clientèle gratuit	OUI	NON	NON
Système automatisé de recherche de logiciels espions	OUI	NON	NON
Défense proactive contre les logiciels espions émergents	OUI	NON	NON
Certifications indépendantes d'organismes tiers	OUI	NON	NON

Sélection d'un fournisseur de solution contre les logiciels espions

La meilleure pratique de protection des ordinateurs personnels et des réseaux d'entreprises contre les logiciels espions consiste à utiliser un logiciel spécialisé dans la lutte contre cette menace précise. En bref, un logiciel spécialisé dans la lutte contre une menace précise s'acquitte bien mieux de sa tâche qu'un logiciel générique ou qu'un groupe de produits logiciels assemblés après coup.

Devant la croissance dynamique des logiciels espions et les inconvénients des solutions gratuites, tout-en-un ou non dédiées, que peut-on faire, pour protéger son ordinateur ? La protection contre les logiciels espions requiert une solution capable d'analyser le système en profondeur, pour révéler toutes les traces de programmes malveillants et menaces afférentes. Cette protection doit non seulement, supprimer entièrement les logiciels espions du système, mais aussi bloquer les nouvelles menaces, avant qu'elles ne puissent infecter le système. Toutefois, en plus d'être puissante, elle doit être facile à installer, à déployer et à gérer.

Une protection trop complexe risque d'être mal configurée ou, pire, elle risque de ne pas être utilisée du tout. Non content d'offrir une technologie robuste et un support clientèle complet, le fournisseur d'une telle solution doit disposer d'un groupe de recherche dédié qui se concentre sur la nature informelle et évolutive des logiciels espions.

Un bon exemple de recherche spécialisée est celui du système Phileas® de Webroot Software. Phileas est un système révolutionnaire de recherche en ligne qui trouve les logiciels espions indésirables sur Internet, avant qu'ils n'infectent les ordinateurs des utilisateurs. Phileas met en place des définitions avant que les nouveaux logiciels espions ou leurs variantes ne puissent être déployés en masse sur Internet. Ces nouvelles définitions sont automatiquement téléchargées sans intervention de la part de l'utilisateur du système. Dans son rapport de Mars 2007 sur la sécurité d'Internet, Webroot indiquait qu'en utilisant son système de recherche automatisée de logiciels espions, Phileas, elle est parvenue à découvrir que 17 pour cent (soit 42 millions) des 250 millions d'adresses Internet du monde abritent des programmes malveillants. Près de 3 millions de ces sites malveillants ont été découverts dans la seule année 2006.

Webroot, fournisseur de la meilleure protection contre les logiciels espions

Webroot AntiSpyware Corporate Edition (anciennement Spy Sweeper® Enterprise) a été à plusieurs reprises reconnue, à la fois par les consommateurs et les experts, comme la meilleure solution de lutte contre les logiciels espions, disponible sur le marché actuel, sur la base de son efficacité, de sa facilité d'utilisation, de son support clientèle et de la protection globale qu'elle offre. En fait, elle a remporté le prix du Meilleur produit de lutte contre les programmes malveillants, décerné en 2007 par SC Magazine.

Test après test, Webroot AntiSpyware est capable de détecter, supprimer et bloquer plus de menaces (logiciels espions, programmes publicitaires indésirables, chevaux de Troie, enregistreurs de frappe et menaces à la racine des systèmes) que ses concurrents. Pour assurer une protection continue contre de nouvelles menaces après son installation, Webroot AntiSpyware actualise et renforce constamment ses défenses, sur la base des données reçues de Phileas. Par l'intermédiaire de Phileas, Webroot analyse le Web sans relâche, découvre sans cesse de nouvelles souches de logiciels espions et crée des défenses proactives contre les menaces émergentes, avant qu'elles ne puissent nuire aux systèmes. Le résultat ? Une meilleure protection et des utilisateurs qui gardent une longueur d'avance sur les menaces en évolution constante.

Bien que tout service informatique veuille être certain d'avoir la meilleure protection possible, Webroot comprend que la plupart des entreprises ne veulent pas se concentrer sur leur sécurité, mais plutôt sur leur travail quotidien. C'est dans cet esprit qu'a été développée la solution Webroot AntiSpyware. Le programme analyse les systèmes, bloque les menaces et incorpore automatiquement les mises à jour avec un minimum d'intervention de la part de l'administrateur. Les rapports sont simples et indiquent clairement quel programme malveillant a tenté d'attaquer vos systèmes et lequel a été bloqué, pour que vous voyiez clairement la menace et communiquiez à qui de droit l'efficacité du produit.

Les logiciels de sécurité Webroot ont été reconnus, à de nombreuses reprises, comme les meilleurs du marché, tant par les rédacteurs que par les lecteurs de SC Magazine, PC World, PC Magazine, PC Pro, InfoSecurity et bien d'autres. Ils ont été primés huit fois en tant que Choix des rédacteurs de PC Magazine. Ils sont certifiés par les laboratoires ICSA, West Coast et Veritest. Leur technologie antivirus a réussi 38 des tests de Virus Bulletin 100 ces neuf dernières années. Aucune solution majeure n'a jamais atteint pareil résultat !

Conclusion et recommandations

Le problème des logiciels espions est bien plus important que vous ne le pensez, et il grandit rapidement. Les solutions génériques de type « tout-en-un » ne possèdent pas la spécialisation nécessaire pour identifier de manière proactive les nouvelles menaces et pour protéger efficacement les systèmes informatiques. Les logiciels gratuits, quant à eux, n'ont pas la technologie robuste requise par ce type de protection. Il existe une meilleure manière de protéger votre entreprise. Dans la configuration complexe qui est celle des entreprises actuelles, la meilleure protection est la solution Webroot AntiSpyware Corporate Edition.

À propos de Webroot

Webroot Software, Inc. fournit des logiciels de sécurité à la pointe de la technologie actuelle aux consommateurs, aux petites et moyennes entreprises et aux grandes entreprises du monde entier. Reconnue mondialement pour sa ligne de produits de lutte contre les logiciels espions et les virus, récompensée par de nombreux prix, Spy Sweeper®, la société a développé son offre de sécurité, pour inclure Webroot Parental Controls, solution conçue pour les parents désireux d'assurer la sécurité de leurs enfants en ligne. Les logiciels de sécurité Webroot sont régulièrement notés en tête du marché par des médias réputés et sont adoptés par des millions d'utilisateurs partout dans le monde. Webroot® AntiSpyware Corporate Edition est une solution d'entreprise complète, à gestion centralisée, qui bloque, détecte et élimine radicalement les logiciels espions de tous les systèmes d'un réseau. Webroot® AntiSpyware Corporate Edition with Antivirus offre une protection combinée contre les logiciels espions et les virus. Disponibles en solutions de marque ou intégrés au système par les fabricants d'ordinateurs, les produits Webroot sont décrits en détail sur le site <http://www.webroot.com> et dans les boutiques informatiques des plus grands détaillants du monde.

NETWALKER

NetWalker
7 rue de Metz
94240 L'HAY LES ROSES

Tél : 0 174 875 442
Fax : 0 825 218 058
www.netwalkerstore.com