



La technologie anti-logiciels malveillants d'Outpost Security Suite Pro

Gagnez du temps en réalisant des analyses plus rapides !

Résumé

Ce document détaille les nouvelles technologies présentes dans Outpost Security Suite Pro, permettant de combattre les programmes malveillants sans ralentir les performances du système.

Introduction

Outpost Security Suite Pro contient un module anti-logiciels malveillants qui, à la différence des anti-virus et des anti-logiciels espions traditionnels, protège de multiples menaces : les virus, les logiciels espions, les chevaux de Troie générant des botnets, les rootkits, etc. Le module est optimisé de façon à permettre une analyse plus rapide, sans interrompre l'activité normale.

Deux moteurs et un scanneur global

Le module anti-logiciels malveillants d'Outpost Security Suite Pro étend la technologie anti-logiciels espions et anti-chevaux de Troie à Outpost Firewall Pro, grâce à l'inclusion d'un moteur anti-virus dédié. Le scanneur anti-logiciels malveillants combiné propose deux mécanismes distincts pour combattre les logiciels malveillants. Ils sont mis à jour par deux équipes de recherche expertes et indépendantes, qui collaborent pour offrir une protection parfaitement intégrée contre les menaces complexes actuelles.

Breveté par Virus Buster en Hongrie, le moteur anti-virus a remporté différentes récompenses. Il est certifié par les laboratoires West Coast, ICSA et par le Virus Bulletin (pour en savoir plus, cliquez [ici](#)).

Lorsque que le scanneur anti-virus cherche des logiciels malveillants, il utilise les deux moteurs simultanément afin de localiser et de supprimer les menaces. Les mises à jour de la définition des logiciels malveillants sont consolidées et envoyées quotidiennement, afin d'assurer une protection continuellement à jour.

Les avantages des performances d'analyse

La plupart des produits dédiés à la sécurité offrent une protection contre les virus et autres programmes malveillants en analysant la présence d'un code viral. Pour l'essentiel, cela implique de se concentrer sur chaque objet du disque analysé, et de le comparer à un éventail d'empreintes malveillantes connues, extraites de menaces précédentes.

Comparer un fichier à une vaste base de données contenant les définitions de logiciels malveillants prend du temps et des ressources système. Si l'ordinateur en cours d'analyse contient également un grand nombre de fichiers, comme beaucoup de disques dur de grande capacité aujourd'hui, la tâche de vérification de l'ordinateur entier peut prendre énormément de temps.

Cependant, la majorité des utilisateurs, voient relativement peu de fichiers modifiés quotidiennement sur leur disque dur. L'analyse typique quotidienne examine donc un grand nombre de fichiers qu'il n'est pas nécessaire de vérifier. Outpost Security Suite Pro fait appel à la nouvelle technologie SmartScan, pour une approche plus intelligente, en analysant uniquement les objets ayant été modifiés depuis la dernière analyse. En résultent des analyses plus rapides, ainsi qu'une utilisation réduite des ressources système.

Comment fonctionne SmartScan

SmartScan peut réduire considérablement le temps nécessaire à l'analyse d'un système ayant été examiné au moins une fois par le module anti-logiciels malveillants d'Outpost. Cette optimisation s'obtient par l'utilisation de fichiers tampons qui stockent les informations concernant l'état de la dernière analyse réalisée sur chaque objet. Si l'objet n'a pas changé depuis la dernière analyse, il est exclu de l'analyse suivante. Le scanneur des résidents en mémoire utilise également la technologie SmartScan : si une

nouvelle application est chargée dans la mémoire, elle n'est vérifiée que si elle n'a pas été validée auparavant, ou si elle a changé depuis la dernière opération. Cela n'augmente pas seulement les vitesses d'analyse en temps réel en rendant le système plus réactif, mais accélère également les temps de démarrage du système.

Réalisation technique

Lors de l'analyse initiale, Outpost Security Suite Pro crée deux fichiers d'index auxiliaires dans chaque dossier (OP_CACHE.ATR et OP_CACHE.IDX). Ces fichiers sont masqués dans les listings du dossier, afin d'être rendus aussi résistants que possible aux ingénieries. Ces fichiers sont également protégés par la fonction auto-protection d'Outpost qui garantit que ses composants ne sont ni accessibles, ni modifiables, ni susceptibles d'être endommagés par des programmes non autorisés.

Afin de garder une trace des résultats de la dernière analyse, Outpost met à jour le registre interne de ces fichiers d'index, à l'aide de données telles que la liste des fichiers d'un dossier ayant été vérifiés avant et pendant, la date de la dernière modification des fichiers, et d'autres informations à propos de la maintenance. Le scanneur récupère à partir de ces fichiers les informations sur l'état des précédentes analyses anti-logiciels malveillants de tous les éléments appartenant à chaque dossier donné.

Chaque objet vérifié au préalable reste exclu des analyses ultérieures tant que son contenu ne change pas, ou que vos signatures de logiciels malveillants n'ont pas été mises à jour. Sinon, les fichiers tampons sont vidés, et l'objet perd son statut "sain" privilégié, ce qui déclenchera une vérification obligatoire lors de la prochaine analyse.

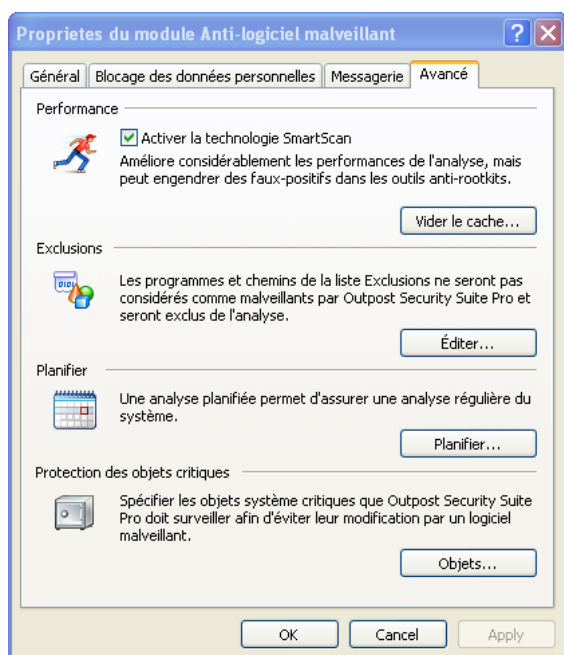
À la différence d'autres produits anti-logiciels malveillants populaires, utilisant des technologies de cache à première vue similaires, SmartScan prend en charge tous les types de systèmes de fichiers PC, et pas seulement NTFS.

Les avantages du point de vue des performances de la technologie SmartScan sont résumés dans le graphique disponible à la fin de ce document dans l'Annexe 1.

Utiliser SmartScan

Vous pouvez activer l'utilisation de SmartScan dans l'assistant Configuration, après l'installation d'Outpost Security Suite Pro. Vous pouvez accéder également aux propriétés de SmartScan à n'importe quel moment, en suivant ces étapes : 1) Cliquez sur Options dans l'interface d'Outpost puis sur Installation des plug-ins 2) Sélectionnez le plug-in Anti-logiciel malveillant 3) Cliquez sur l'onglet Avancé 4) Cochez la case Activer la technologie SmartScan, voir ci-dessous

Vous pouvez purger les fichiers tampons à n'importe quel moment, en cliquant sur le bouton Vider le cache. Ces fichiers sont automatiquement supprimés une fois Outpost désinstallé.



Remarque au sujet des outils anti-rootkits: les fichiers tampons sont en "lecture seule" et ne peuvent être visibles si vous utilisez des gestionnaires de fichiers conventionnels tels que l'Explorateur de fichiers. Certains logiciels anti-rootkits peuvent considérer les fichiers tampons comme suspects car les méthodes de dissimulation du contenu, afin d'éviter les abus malveillants, peuvent être considérées comme caractéristiques des rootkits. Malheureusement, puisque les anti-rootkits fonctionnent différemment, il nous est impossible d'affaiblir les fichiers tampons d'Outpost afin qu'ils ne soient pas vus comme étant suspects, en revanche vous pouvez être certain qu'ils sont vraiment sûrs.

Optimisation du scanneur résident

Si un fichier infecté par un logiciel malveillant est ouvert, le risque d'activation et de prolifération de l'infection est énorme. Par chance, ce risque n'apparaît pas si le fichier est simplement copié, renommé, ou si ses propriétés sont affichées, la charge finale ne sera activée que si le fichier est exécuté.

Outpost Security Suite Pro propose à ses utilisateurs de choisir la manière dont le composant anti-logiciels malveillants vérifie l'activité des programmes en temps réel : au moment de l'accès, ou au moment de l'exécution. La seconde option offre sans nul doute les meilleures performances.

- **Vérifier les fichiers à l'exécution** Cela évite aux programmes malveillants de se lancer et permet l'analyse des fichiers uniquement s'ils sont ouverts. Les autres commandes d'accès aux fichiers comme copier, visualiser les propriétés des fichiers, ou afficher le contenu d'un dossier n'ont pas d'impact sur cette sélection.
- **Vérifier les fichiers à l'accès** Ce mode déclenche une analyse des logiciels malveillants dès que survient une tentative d'accès à un fichier quelconque.

Avantages

Cette approche offre une protection sur mesure à tous les utilisateurs. Certaines personnes ne se sentent en sécurité que si elles vérifient chaque fenêtre et chaque porte de leur maison tous les jours. La vérification des fichiers à l'accès procure à ces utilisateurs une véritable tranquillité d'esprit. Les autres se contentent de vérifier seulement lorsqu'un risque potentiel se présente, et pour ces utilisateurs, vérifier les fichiers à l'exécution est un choix plus judicieux.

Réalisation technique

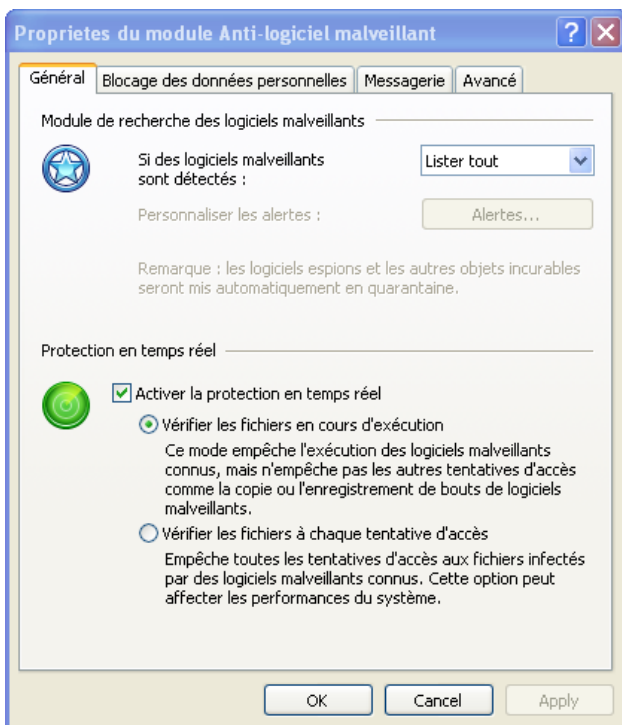
Dans le mode à l'exécution, Outpost Security Suite Pro intercepte les modules en cours de chargement, responsables de l'exécution du code. Ce code est alors vérifié par le plug-in anti-logiciels malveillants avant qu'il n'obtienne l'autorisation d'établir le contrôle. Ce mode vérifie les fichiers des programmes exécutables et les fichiers de documents (comme Word ou Excel) pouvant potentiellement contenir des commandes macro et autres codes « exécutables cachés ». Cependant, il ne recherche de virus dans les fichiers pendant les opérations de copie et d'enregistrement.

Dans le mode à l'accès, toutes les tentatives d'accès aux fichiers sont interceptées. Cela garantit que l'accès aux fichiers normalement non désignés pour contenir un code programme, mais pouvant avoir été exploités par leur vulnérabilité, est également contrôlé et sécurisé.

Choisir le mode approprié

Pour choisir le mode approprié :

- 1) Sélectionnez le plug-in Anti-logiciel malveillant dans le menu Options d'Outpost
- 2) Cliquez sur l'onglet Général
- 3) Cochez la case Activer la protection en temps réel, puis cliquez sur le bouton radio approprié pour le mode opératoire désiré, comme affiché ci-dessous



Résumé

La nouvelle combinaison du module anti-logiciels malveillants et de la technologie SmartScan d'Outpost Security Suite Pro est toujours en alerte pour prévenir tous les risques potentiels. Elle analyse rapidement et précisément, réduit la charge sur les ressources système, ne s'active que lorsque cela est nécessaire, et est vraiment facile d'utilisation. Pour plus d'informations, et pour télécharger une version d'essai, rendez-vous sur <http://www.agnitum.fr/products/security-suite/index.php>.

Annexe 1 : statistiques de performances et graphiques

