
# Listes noires ou listes blanches : quels logiciels choisir ?

**Livre blanc**

Simplifying Computer Management eurosales@faronics.com www.faronics.com
Venture House, 2 Arlington Square, Downshire Way, Bracknell, RG12 1WA, England **Tel:** +44 (0) 1344 741057 · **Fax:** +44 (0) 1344 741067
Faronics EMEA · Registered in England and Wales No. 6923261 · Registered Office: 130 Wood Street, London EC2V 6DL

## Introduction

Les risques posés par les logiciels malveillants, prenant la forme de rootkits (outils de dissimulation d'activité), de virus et de chevaux de Troie, sont plus nombreux chaque jour. Selon un récent rapport, les menaces augmentent de manière exponentielle avec une moyenne de 73 000 logiciels malveillants uniques ayant été détectés chaque jour au cours du premier trimestre de 2011. Cela représente une hausse de 26 % des taux de création de logiciels malveillants par rapport à la même période en 2010.

En réponse à la croissance explosive des logiciels malveillants, les entreprises demandent des solutions de sécurité plus robustes incluant fréquemment deux approches opposées : les listes noires et les listes blanches. Ce livre blanc s'intéresse aux logiciels de listes noires, l'une des solutions les plus courantes qui se consacre au traitement du nombre grandissant de menaces malveillantes. Cependant, il s'intéresse également aux logiciels de listes blanches, approche relativement nouvelle et moins couramment utilisée pour combattre ce problème.

## Motifs des logiciels malveillants

Depuis que le tout premier virus informatique a été détecté en 1986, le taux d'apparition de logiciels malveillants a explosé au cours des 25 dernières années. Ce qui était au début un hobby pour les passionnés de technologie à la recherche d'un défi et de célébrité a évolué pour devenir l'outil essentiel de tout réseau de crime organisé. Les cybercriminels d'aujourd'hui sont des professionnels motivés par les avantages financiers du vol et de la vente de données propriétaires, de dossiers financiers, de fichiers du personnel, de dossiers médicaux, de listes de clients et bien plus.

Les outils sont simples à obtenir avec la prolifération de kits de logiciels malveillants mis à disposition sur Internet. Aujourd'hui, mêmes les individus ne possédant aucune compétence technique peuvent devenir des pirates en quelques minutes et créer des chevaux de Troie et commettre d'autres méfaits. Le piratage devient une profession tellement lucrative que les criminels investissent désormais dans leurs attaques au moyen de recherches, de programmeurs et de testeurs pour garder une longueur d'avance sur la sécurité informatique.

Aujourd'hui, les risques règnent sur le Web. 90 % des infractions sont le résultat d'une activité de crime organisé ciblant les informations d'une entreprise. En 2009, la quasi-totalité des infractions ont impliqué des logiciels malveillants personnalisés, parvenant à exposer 140 millions de dossiers. Et comme le nombre d'infractions augmente constamment, les entreprises resserrent leur infrastructure de sécurité informatique.

## Effets des logiciels malveillants

Les logiciels malveillants deviennent plus malicieux, nuisibles et coûteux pour leurs victimes que jamais. Les récents rapports indiquent une hausse alarmante des pertes financières engendrées par les logiciels malveillants et les violations de données.

## Coût des violations de données

D'après certaines estimations, le coût de la cybercriminalité s'élève à quelques millions de dollars pour l'économie américaine, mais d'autres l'ont estimé à des centaines de milliards. Une étude de 2010 menée par le Ponemon Institute a estimé que le coût annuel moyen de la cybercriminalité pour une seule entreprise victime allait de 1 million à 52 millions de dollars américains, avec une moyenne tournant autour de 7,2 millions de dollars américains, démontrant une hausse de 7 % par rapport à 2009.

## Coût du vol d'identité

Selon une publication de Javelin Strategy and Research datant de 2011, le coût annuel du vol d'identité s'élève à 37 milliards de dollars américains, incluant toutes les formes de vol d'identité, pas seulement celles réalisées sur Internet. Selon un article publié en janvier 2011, 11,1 millions d'adultes ont été victimes de vol d'identité aux États-Unis, représentant une hausse de 12 % par rapport à 2008. Aux États-Unis, la fraude a totalisé 31 milliards de dollars et les entreprises perdent 221 milliards de dollars chaque année, à travers le monde, pour cause de vol d'identité.

## Coût des attaques au jour zéro

Autre préoccupation : le problème posé par les attaques de virus au jour zéro, contre lesquelles il n'y a aucun moyen de défense garanti. Les vulnérabilités exploitées par les attaques au jour zéro offrent une porte dérobée vers tout système d'exploitation et représentent une sérieuse menace pour les entreprises. Selon les toutes dernières recherches, le nombre de logiciels malveillants capables de muter augmente au même rythme que les compétences techniques des attaquants s'améliorent. En moyenne, seuls 15 systèmes sont affectés par un logiciel malveillant spécifique avant qu'il ne soit changé pour éviter d'être détecté et continuer à faire des ravages.
La santé et l'éducation sont les deux secteurs présentant la majorité des violations de données, tandis que les secteurs financiers et gouvernementaux subissent le plus grand nombre de vols d'identités. Les récents gros titres ont démontré qu'aucune entreprise n'est invincible car même certains des géants et leaders de l'industrie de la sécurité ont été victimes d'attaques.

## Vue d'ensemble des solutions

L'une des plus importantes catégories de la protection traditionnelle contre les logiciels malveillants est la technologie de listes noires, qui inclut les solutions de listes noires traditionnelles telles que les antivirus et les logiciels anti-espions.

## Les solutions de listes noires traditionnelles

Une liste noire est une liste d'entités spécifiques, à savoir des noms de domaines, adresses e-mail ou virus, contenant des éléments présumés dangereux ou potentiellement dévastateurs, qui se voient refuser l'accès à l'infrastructure qu'elles essaient de pénétrer. Par exemple, un site Internet peut être placé sur une liste noire parce qu'il est réputé frauduleux ou parce qu'il exploite les vulnérabilités du navigateur pour envoyer des logiciels espions ou autres logiciels indésirables à un utilisateur.
Le concept de liste noire peut aussi être utilisé pour empêcher la réception d'e-mails indésirables. Les utilisateurs peuvent créer une règle dans un programme anti-spam bloquant la réception d'e-mails provenant d'un expéditeur spécifique (ou correspondant à d'autres critères précisés), que le programme aurait normalement autorisé.
Les solutions de listes noires traditionnelles les plus courantes sont les antivirus et les logiciels anti-espions. Un logiciel de liste noire fonctionne en bloquant les menaces connues. Les sociétés qui conçoivent des logiciels antivirus maintiennent une base de données des virus connus qu'elles fournissent à leurs abonnés. Lorsqu'un nouveau virus est identifié, les sociétés d'antivirus créent une protection spécifique contre celui-ci et fournissent cette mise à jour à leurs utilisateurs.

**Avantages d'une solution de liste noire :**

- les mises à jour des listes de virus sont automatiques et ne nécessitent donc aucun temps de maintenance
- permet l'identification, et parfois l'élimination, des logiciels malveillants
- les mises à jour peuvent être effectuées à la volée par un serveur de mises à jour
- offre une sécurité et une protection totales contre toutes les menaces actuellement connues
- polyvalente : elle combat tous les types de menaces malveillantes

**Inconvénients d'une solution de liste noire :**

- Elle ne vous protège que des menaces connues, ce qui signifie souvent qu'une personne doit être victime d'une nouvelle menace avant qu'elle ne soit identifiée
- Un logiciel malveillant infecte une moyenne de 15 systèmes avant de muter et de changer sa signature, le rendant indétectable pour les solutions de liste noire
- En moyenne, les solutions antivirus n'arrêtent qu'environ 19 % des menaces
- Cette solution nécessite l'ajout des virus ou logiciels espions à la liste noire, laissant les postes de travail et réseaux vulnérables aux attaques au jour zéro

- Les utilisateurs donnent essentiellement le contrôle de leurs réseaux à un fournisseur tiers, et doivent continuellement mettre à jour les définitions de virus et de logiciels espions, alourdissant la charge en termes de matériel et de bande passante réseau
- Par sa nature même, il s'agit d'une solution très gourmande en ressources, ralentissant tout ordinateur

## Joe le videur et la technologie de liste noire

Joe est le videur de l'Hi-Tek Bar. Chaque soir, à l'ouverture du bar, c'est lui qui a la responsabilité de laisser rentrer, ou non, les personnes. Pour aider Joe, ses supérieurs lui fournissent une liste des personnes qui ne sont pas autorisées à rentrer dans le bar. Lorsque ces individus arrivent à la porte, espérant rentrer, Joe consulte sa liste, et s'il les y voit, il leur refuse l'accès au bar.

Cependant, si un homme apparaissant sur la liste se rase la tête et se fait pousser une moustache en guidon, il se peut que Joe ne le reconnaisse pas la prochaine fois lorsqu'il se présentera au bar. Dans un tel cas, Joe le laissera probablement rentrer, lui permettant de faire ce qu'il veut. De plus, ce n'est pas parce que quelqu'un ne se trouve pas déjà sur la liste des personnes non autorisées qu'il ou elle ne représente pas une menace pour le bar. Cela signifie simplement que le bar ne l'a pas encore vu avoir un comportement indésirable, mais Joe n'a aucun moyen de savoir qui pourrait être dangereux.

## Solutions de listes noires avancées

Les solutions de listes noires ont évolué au-delà du simple blocage des menaces connues pour inclure l'heuristique. L'heuristique est l'application des connaissances basées sur l'expérience pour résoudre un problème. En collaboration avec un logiciel antivirus, elle est parfois utilisée pour décrire la capacité à analyser et filtrer les fichiers susceptibles de contenir un virus informatique ou un autre logiciel malveillant.

Un logiciel d'heuristique recherche des sources connues, des expressions textuelles couramment utilisées et des modèles de transmission ou de contenu typiquement associés à des fichiers contenant des virus, comme les expériences passées l'ont montré. L'heuristique est un terme inventé par les chercheurs d'antivirus pour décrire un programme antivirus détectant les virus en analysant la structure du programme, son comportement, et d'autres attributs, plutôt qu'en recherchant simplement des signatures.

**Avantages d'une solution heuristique :**

- elle ne nécessite aucune mise à jour des fichiers de définition
- elle peut potentiellement intercepter les attaques au jour zéro
- elle offre un niveau de protection supplémentaire car elle ne se fie pas uniquement aux fichiers de définition ; elle peut parfois trouver une menace n'apparaissant pas dans une liste noire

**Inconvénients d'une solution heuristique :**

- elle émet des hypothèses sur le problème qu'elle tente de résoudre et peut produire des résultats non optimaux
- des fichiers légitimes peuvent aussi avoir un modèle semblable à celui d'un fichier malveillant, provoquant la création de nombreux « faux positifs » et retardant la livraison d'e-mails ou de fichiers valides
- c'est une technologie relativement récente ; il lui faudra encore du temps pour se développer et s'améliorer

## Joe le videur et les solutions heuristiques

De retour à l'Hi-Tek Bar, les supérieurs de Joe ont décidé d'essayer une approche différente. Au lieu de produire une liste avec des noms ou des photos d'individus spécifiques non autorisés dans le bar, ils utilisent un ensemble de règles plus générales pour déterminer qui a le droit d'entrer et qui n'en a pas le droit. Pour créer ces règles, ils les ont basées sur les types de personnes ayant causé des problèmes par le passé. Par exemple, il a été demandé à Joe de refuser l'accès à toutes les personnes aux crânes rasés et aux moustaches en guidon parce que des personnes aux caractéristiques physiques semblables ont déjà causé des problèmes dans le bar.

Cependant, à la grande surprise du patron de l'Hi-Tek Bar, son fils vient de rentrer d'une année de randonnée en Asie avec le crâne rasé et une moustache en guidon. Joe le regarde brièvement et refuse de le laisser rentrer car il correspond en tout point au profil des fauteurs de trouble, malgré le fait qu'il soit le fils du patron et un client accommodant et digne de confiance.

## Une approche différente : la solution de liste blanche

Une technologie de liste blanche est l'opposé d'une technologie de liste noire. La liste d'entités, à savoir les noms de domaines, adresses e-mail ou fichiers exécutables, ne répertorie que celles autorisées à rentrer dans le système. Par exemple, une liste blanche de noms de domaine est une liste d'URL qu'il est autorisé d'afficher, même en cas de présence d'un programme bloquant les e-mails indésirables.
L'exemple le plus familier pour illustrer les solutions de listes blanches est la création par l'utilisateur d'une liste d'adresses e-mail autorisées desquelles il accepte de recevoir des messages, quelles que soient les règles d'un éventuel programme anti-spam.
L'un des types de listes blanches les plus importants est la liste blanche d'applications. Lorsqu'on utilise une liste blanche d'applications, seuls les programmes pré-approuvés ont l'autorisation de fonctionner sur une machine, tandis que tous les autres programmes non approuvés ne peuvent tout simplement pas se lancer.

**Avantages d'une solution de liste blanche d'applications :**

- offre une protection contre les attaques de logiciels malveillants, au jour zéro et ciblées car aucun fichier exécutable non autorisé ne peut se lancer
- améliore la productivité des employés et l'efficacité de traitement des postes de travail car aucune application indésirable telle qu'un programme de discussion, un service P2P, un logiciel-espion ou un cheval de Troie, ne s'installera ou ne se lancera
- élimine le risque d'amendes et d'audits coûteux pour licence non conforme car aucun logiciel illicite ou sans licence ne sera installé
- économise l'argent des entreprises en diminuant les temps d'arrêt, en allongeant les cycles de vie des PC, et en réduisant le volume des billets d'assistance, créant des opportunités de transfert de coûts pour aider les entreprises à faire davantage avec moins

**Inconvénients d'une solution de liste blanche :**

- la configuration de la liste blanche peut prendre un certain temps, à moins d'utiliser une solution de liste blanche d'applications avancée
- gérer les mises à jour sans commandes avancées peut poser problème car les mises à jour peuvent légèrement altérer l'identité de l'application approuvée à partir de ce qui a déjà été approuvé sur la liste blanche existante, empêchant le programme de se lancer

## Joe le videur et la technologie de liste blanche

Joe le videur travaille toujours à l'Hi-Tek Bar. Il essaie désormais une troisième et nouvelle approche pour empêcher que les personnes non souhaitées ne rentrent dans le bar. Cette fois-ci, ses supérieurs ont donné à Joe une liste des personnes autorisées à rentrer. Ils ne se préoccupent plus de qui n'est pas autorisé à rentrer.
Joe n'essaie pas de déterminer qui ressemble à un fauteur de trouble en se basant sur un ensemble de règles générales. Il laisse simplement rentrer dans le bar les personnes se trouvant sur la liste des personnes autorisées. Il ne fait du coup plus aucune erreur et n'a plus peur de se tromper. Il est donc bien plus heureux.

**Faronics Anti-Executable**

Le logiciel Faronics Anti-Executable adopte une approche différente de la protection contre les logiciels malveillants. Le logiciel Anti-Executable permet aux administrateurs de choisir quelles applications sont autorisées à fonctionner sur un poste de travail. Tout fichier exécutable non autorisé par le logiciel Anti-Executable ne pourra jamais se lancer ou s'installer. Le logiciel Anti- Executable se base sur le concept de liste

blanche et au lieu d'être configuré pour bloquer les fichiers exécutables indésirables sur un système, il est configuré pour autoriser les fichiers exécutables voulus sur un système.
Cela fait un certain temps que la communauté informatique a reconnu l'efficacité des listes blanches d'applications. Cependant, les difficultés associées à la création d'une liste blanche initiale et le temps passé au maintien de celle-ci ont dissuadé de nombreuses entreprises d'adopter cette stratégie de sécurité. En exploitant une fonctionnalité avancée, Faronics Anti- Executable offre aux entreprises l'avantage des listes blanches d'applications sans augmenter la charge de travail de l'équipe informatique.

En termes de sécurité, le logiciel Anti-Executable remplit le vide que les solutions antivirus seules ne peuvent combler. Avec les dizaines de milliers de nouveaux logiciels malveillants qui apparaissent chaque jour, les programmes antivirus n'arrivent simplement pas à suivre. Étant donné les menaces représentées par les logiciels malveillants capables de muter, les attaques ciblées et les menaces au jour zéro, compter sur la seule capture des menaces connues ne suffit plus. Sachant qu'il faut une moyenne de 11,6 jours pour qu'un programme antivirus capture une nouvelle menace, cela expose les réseaux des entreprises à de sérieux risques pendant bien trop longtemps.
Le logiciel Anti-Executable bloque les deux principaux outils utilisés lors d'une attaque pour donner le contrôle aux pirates. Il vous protège contre l'exécution d'enregistreurs de frappes non autorisés et les programmes d'accès de contrôle à distance, qui exposent les réseaux d'entreprises aux criminels. Le logiciel Anti-Executable est la protection ultime contre les attaques au jour zéro tout simplement parce que le logiciel ne reconnaîtra pas ces programmes exécutables malveillants comme des applications autorisées. En conséquence, les temps d'arrêt dus aux logiciels malveillants sont considérablement réduits.
Faronics Anti-Executable offre une technologie de liste blanche avancée pour aider les professionnels informatiques à minimiser les défis posés par les solutions de listes blanches traditionnelles. L'inclusion d'une option permettant de configurer la liste blanche au moment du déploiement réduit la nécessité pour le personnel informatique de créer manuellement une nouvelle liste blanche pour chaque machine. De plus, la possibilité d'attribuer un statut « éditeur fiable » à un fabricant de logiciels comme Microsoft aide les professionnels informatiques à mieux gérer leurs mises à jour, garantissant une disponibilité continue des machines.
Les solutions de listes blanches sont une option simple et sûre pour un contrôle total du système. Le concept de liste blanche appliqué à la sécurité des postes de travail place le contrôle total entre les mains de l'administrateur, garantissant une plus grande tranquillité d'esprit.

## À propos de Faronics

Avec une réputation bien établie d'aide aux entreprises pour gérer, simplifier et sécuriser leurs infrastructures informatiques, Faronics permet d'en faire plus avec moins en maximisant la valeur de la technologie existante. Nos solutions offrent une fiabilité totale des postes de travail, un contrôle intégral du système et une gestion sans perturbation de l'énergie des ordinateurs.
Fondée en 1996, Faronics possède aujourd'hui des bureaux aux États-Unis, au Canada et au Royaume-Uni, ainsi qu'un réseau mondial de partenaires. Nos solutions sont développées dans plus de 150 pays dans le monde et aident plus de 30 000 entreprises.

## Droit d'auteur