Guide de protection contre les cryptomalwares
Kaspersky Endpoint Security for Windows

Version 2.0

Ce guide s'applique aux produits suivants :

- Kaspersky Security Center 10.2.434 + patch D (SP1)
- Kaspersky Endpoint Security 10 for Windows 10.2.4.674 (SP1 MR2)

Check List

1. Composantes d’une protection efficace contre les cryptomalwares
   - ☐ a. Protection antivirus sur le flux de messagerie
   - ☐ b. Protection Antivirus Fichiers
   - ☐ c. Protection Antivirus Courrier
   - ☐ d. Protection contre les menaces inconnues
   - ☐ e. Blocage du lancement d’applications inconnues
   - ☐ f. Protéger vos données sensibles contre les modifications
   - ☐ g. En résumé
2. Application des mesures de renforcement de la sécurité
   - ☐ a. Import de la catégorie
   - ☐ b. Import de la stratégie
   - ☐ c. Application des restrictions de lancement d’applications inconnues
   - ☐ d. En cas de blocage d’une application légitime par le Contrôle du lancement des applications
     - Option n°1 : utiliser le système de plainte des utilisateurs via la Console d’Administration
     - Option n°2 : utiliser le registre des fichiers exécutables
     - Option n°3 : créer manuellement les règles d’exclusion dans la catégorie
   - ☐ e. Application des restrictions contre les modifications de données sensibles
   - ☐ f. En cas de blocage d’une application légitime par le Contrôle de l’activité des applications

Composantes d’une protection efficace contre les cryptomalwares

Protection Antivirus sur le flux de messagerie

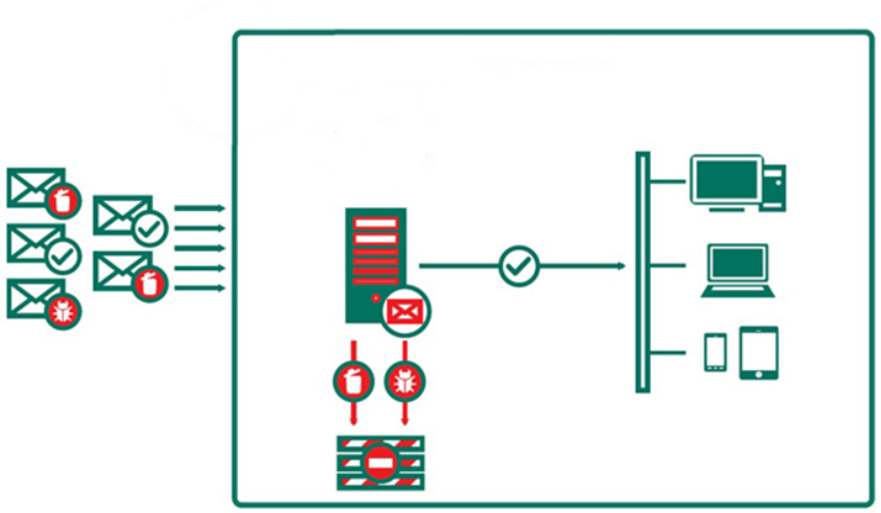
La plupart des cryptomalwares utilisent la messagerie pour se propager, c’est pourquoi il est très important d’effectuer un filtrage antivirus en amont de vos postes de travail, lorsque les messages transitent sur votre infrastructure de messagerie.

Cette analyse peut s’effectuer sur vos serveurs de messagerie au niveau des boîtes aux lettres ou encore au niveau périmétrique de votre réseau lorsque le flux est traité par vos appliances ou encore en amont chez votre fournisseur de service de messagerie : l’idéal étant d’avoir de multiples analyses à ces différents niveaux pour éviter que des emails malveillants ne parviennent jusqu’à vos utilisateurs.

Si vous le pouvez, implémenter des filtrages sur les extensions dangereuses des pièces jointes telles que EXE, BAT, CMD, etc.

S’agissant de CTB-Locker, le malware se présente sous le forme d’un fichier avec une extension SCR et est compressé dans une archive ZIP. Le format SCR étant généralement réservé aux écrans de veilles MS Windows, posez-vous la question quant à la pertinence d’autoriser l’échange de ce type de fichier par email dans votre organisation et bloquez-là si possible.

PROTECTION DES FLUX DE MESSAGERIE



Analyse des emails en amont.

- Analyse antivirus du corps des messages, des pièces jointes et des liens (phishing)
- Analyse à de multiples niveaux de l'infrastructure de messagerie : postes de travail, boîtes aux lettres, périmètre réseaux (DMZ, appliance), Fournisseur de Service Internet
- Filtrage sur les extensions des pièces jointes : SCR dans ZIP pour CTB-Locker

Protection Antivirus Fichiers

C'est l'un des modules le plus important de la solution de protection des postes de travail : **l'Antivirus Fichiers**

Dans le scénario ou l'utilisateur a réceptionné un email avec une pièce jointe infecté et celle-ci n'a pas été bloqué par les mécanismes de filtrage, lorsque le code malveillant sera enregistré sur le système il sera alors appréhendé par l'antivirus.

Kaspersky Lab ajoute régulièrement de nouvelles signatures à ces bases pour que l'Antivirus Fichiers puisse détecter les nouvelles variantes de ransomware. Ce module réalise également une analyse heuristique pour déceler les nouveaux types de virus inconnus et pour lesquels il n'y a pas de détection par signature.

Aussi la solution communique avec le réseau Kaspersky Security Network basé dans le cloud pour une protection immédiate contre les nouvelles menaces.

Ce module doit être activé en permanence pour assurer une protection efficace du système.

Protection Antivirus Courrier

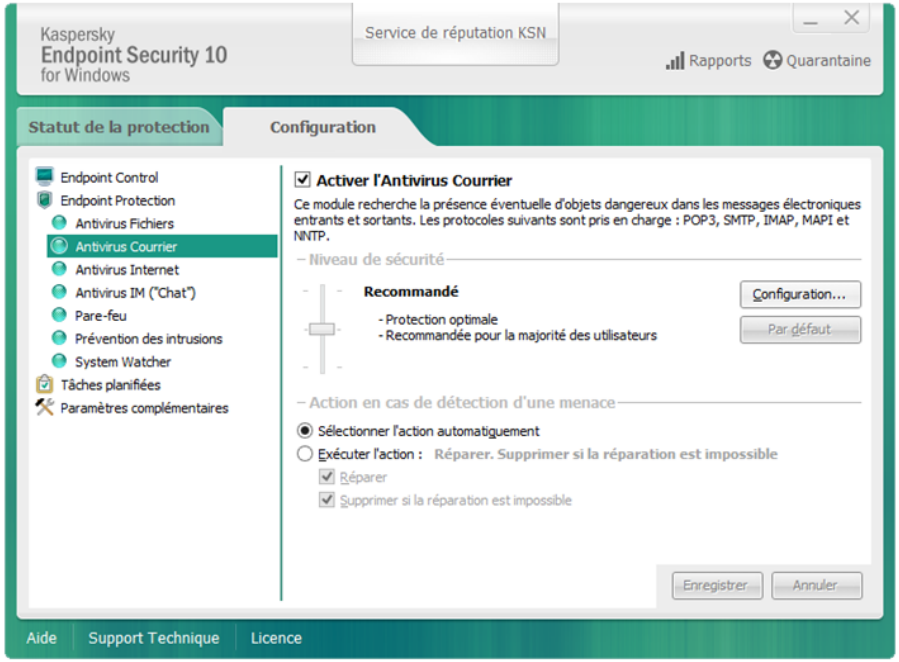
Analyse des flux

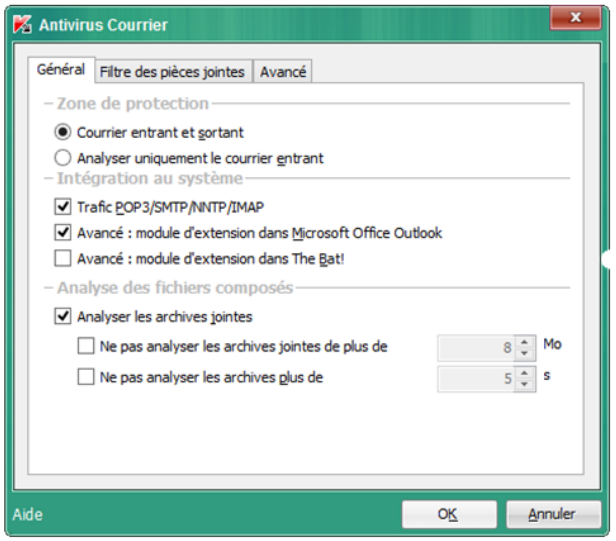
La solution Kaspersky Endpoint Security for Windows est une suite de sécurité qui protège le système à de multiples niveaux.

Contre les cryptomalwares, il est essentiel de bloquer les emails malveillants lors de la réception avant que l'utilisateur ne puisse accéder à la pièce jointe.

L'**Antivirus Courrier** analyse les messages reçus en temps réel lors de la réception du courrier. En cas de détection d'une archive jointe malveillante, ce module procède à la suppression du contenu malveillant et modifie l'objet du message pour en alerter l'utilisateur.

PROTECTION DES FLUX DE MESSAGERIE SUR LES POSTES DE TRAVAIL : ANALYSE DES FLUX





- Analyse des flux POP3/IMAP/MAPI

- Analyse des archives jointes

Filtrage des pièces jointes

Certaines extensions sont dangereuses par nature lorsqu'elles sont présentes en pièce jointe d'un email.

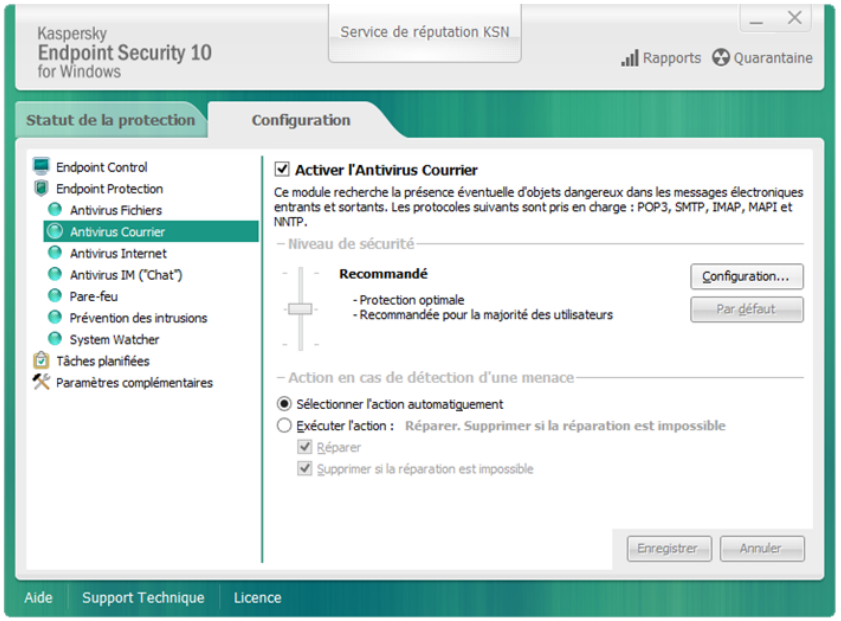
Si vous n'avez pas déjà implémenté un filtrage des extensions sur vos serveurs de messagerie, l'application Kaspersky Endpoint Security for Windows vous permet de le faire lors de la réception des messages avec la possibilité de :

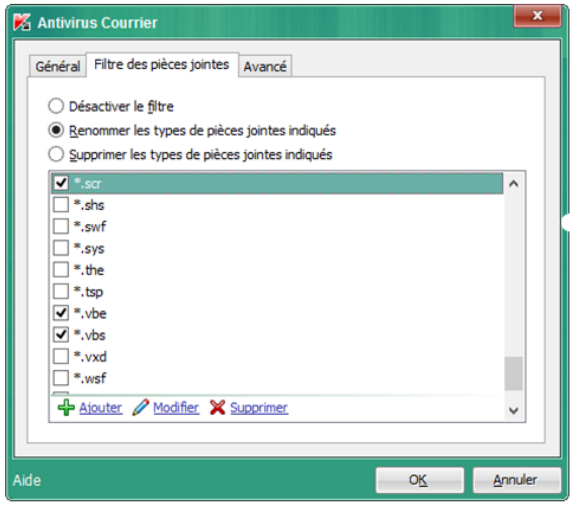
- Renommer ou supprimer directement la pièce jointe
- Ajouter/Modifier la liste des extensions filtrées

Par exemple et comme vous pouvez le voir dans la capture d'écran, les fichiers possédant l'extension SCR utilisé notamment par CTB-Locker peuvent être filtrés ainsi automatiquement.

Il est donc recommandé d'activer ce module si vous n'avez pas déjà un produit Kaspersky Lab sur votre infrastructure de messagerie qui réalise ces analyses en amont des postes de travail.

PROTECTION DES FLUX DE MESSAGERIE SUR LES POSTES DE TRAVAIL : FILTRAGE DES PIÈCES JOINTES





- Filtrage / Renommage / Suppression des pièces jointes selon une liste d'extension configurable

Protection contre les menaces inconnues

System Watcher : Analyse comportementale

Les méthodes classiques d'identification des programmes malveillants telles que l'analyse par signature réalisée par l'Antivirus Fichiers ne sont pas suffisantes pour lutter contre les 325 000 nouveaux échantillons de malware que nous identifions chaque jour. Il existe une méthode efficace pour combler ce déficit qui se repose sur l'analyse du comportement des applications dans le système et la détection d'activités suspectes.

System Watcher est le module le plus important pour bloquer les actions des cryptomalwares, voici les explications.

Tout d'abord ce composant collecte les données sur l'activité des applications et réalise une analyse comportementale. Si une application a un comportement qui s'apparente à celui d'un malware, une action de type déplacement de l'objet en quarantaine et arrêt du processus du malware est automatiquement appliquée selon les recommandations de Kaspersky Lab.

Le module récolte un grand nombre d'informations concernant la création et la modification de fichiers, le fonctionnement des services systèmes, chaque modification effectuée sur la base de registre, les appels systèmes, les données transférées sur le réseau, les liens symboliques ou encore les modifications apportées au MBR. Cette collecte de données est automatique et ne nécessite aucune interaction avec l'utilisateur.

SYSTEM WATCHER : ANALYSE COMPORTEMENTALE

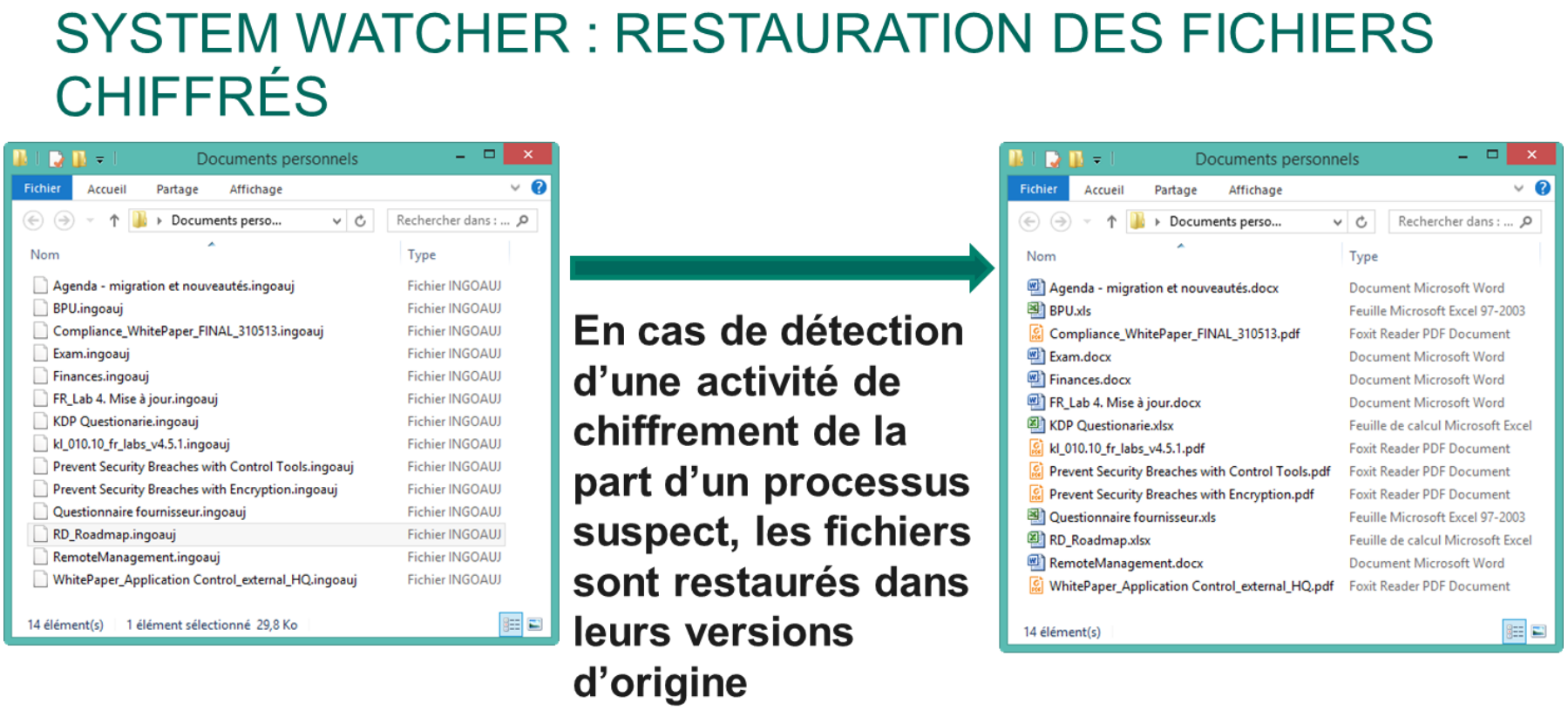
1. **Analyse comportementale via la technologie BSS (Behavior Stream Signatures)**
2. **Arrêt du processus et mise en quarantaine automatique en cas de détection**

System Watcher : restauration des fichiers chiffrés

Une autre fonction de System Watcher pertinente pour la lutte contre les cryptomalwares : la restauration des fichiers chiffrés.

Lorsqu'un processus suspect tente de chiffrer un fichier, Kaspersky Endpoint Security crée automatiquement une copie de sauvegarde du fichier avant qu'il ne soit affecté. Ces copies de sauvegarde sont stockées dans le répertoire temporaire du système et seront utilisées pour la restauration du fichier d'origine en cas de détection d'une activité de ce cryptomalware.

Cette fonction se limite aux fichiers présents sur les disques locaux, System Watcher doit absolument être activé avant que l'activité de chiffrement n'est eue lieu pour que la restauration soit possible.



Blocage du lancement d'applications inconnues

Les cryptomalwares créent habituellement des fichiers dans certains répertoires du système pour opérer au chiffrement des données.

Par exemple dans le répertoire temporaire de l'utilisateur ou encore celui du système.

Pour aller plus loin, vous pouvez étendre le blocage aux répertoires des documents ou de téléchargement des fichiers de l'utilisateur.

A l'aide du module de **Contrôle du lancement des applications** de Kaspersky Endpoint Security et d'un ensemble de règles, vous pouvez donc interdire l'exécution de fichiers dans ces répertoires pour réduire les risques d'infection.

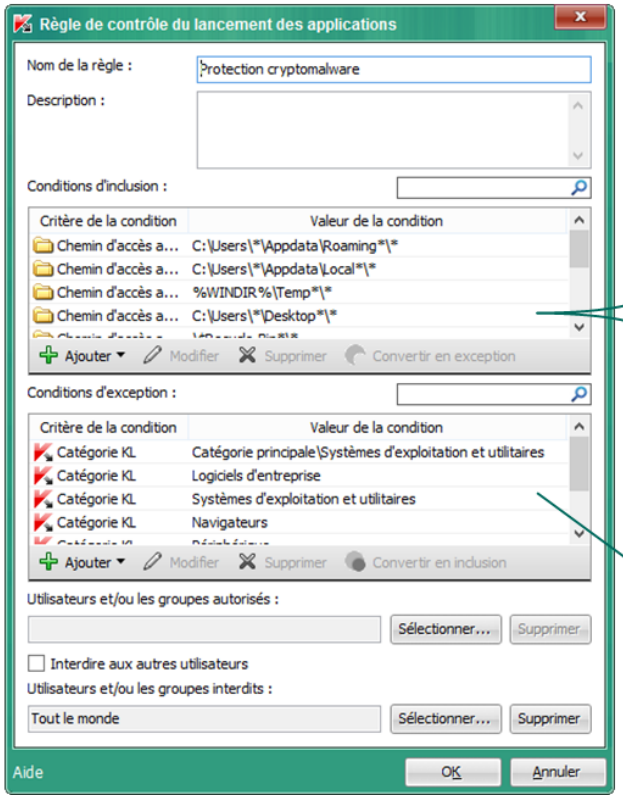
Afin d'autoriser les outils systèmes et vos applications métiers qui ont besoin d'exécuter des fichiers à ces emplacements, vous pouvez exclure les catégories d'applications référencées par Kaspersky Lab et qui couvre de nombreux fichiers grâce à notre travail de référencement. Ce lien permet de naviguer dans ces catégories et de vérifier leur contenu, vous pouvez également chercher la présence d'une application par nom, éditeur ou encore somme de contrôle de fichiers.

Bien entendu cette configuration avancée peut être implémentée de manière globale à un ensemble de machines depuis la plate-forme d'administration centralisée Kaspersky Security Center.

Notez que pour écarter tout danger lié à la mise en place d'une telle règle, vous pouvez la configurer en mode « Test » pour commencer afin de valider son bon fonctionnement. Ce mode « Test » permet de ne pas bloquer les applications mais vous êtes averti via les évènements et autres mécanismes de notifications quelles sont les applications qui auraient pu être bloquées si la règle avait été active.

En résumé et concernant cette action de renforcement de la sécurité, toute application qui n'est pas connue de Kaspersky Lab et référencée dans nos catégories et qui tente de s'exécuter depuis ces emplacements critiques sera bloquée.

RENFORCER LA SÉCURITÉ CONTRE LES CRYPTOMALWARE : BLOQUER LES APPLICATIONS



Bloquer le lancement d'applications dans certains répertoires :

- APPDATA
- TEMP
- Dossier des fichiers d'Internet Explorer
- Bureau
- Corbeille
- Répertoire système
- Dossier des documents utilisateurs
- Dossier de démarrage
- http://support.kaspersky.com/viruses/common/10952#block4

Exclure les applications de confiance référencées dans les catégories KL :

- http://whitelist.kaspersky.com/catalogue

Protéger vos données sensibles contre les modifications

Les cryptomalwares chiffrent les données personnelles issues des applications de bureautique, les images, les fichiers multimédias, bases de données, etc. Finalement tout ce qui peut paraître important pour l'utilisateur.

Avec le module de **Contrôle de l'activité des applications**, il est possible d'étendre la liste des ressources protégées à ces données sensibles.

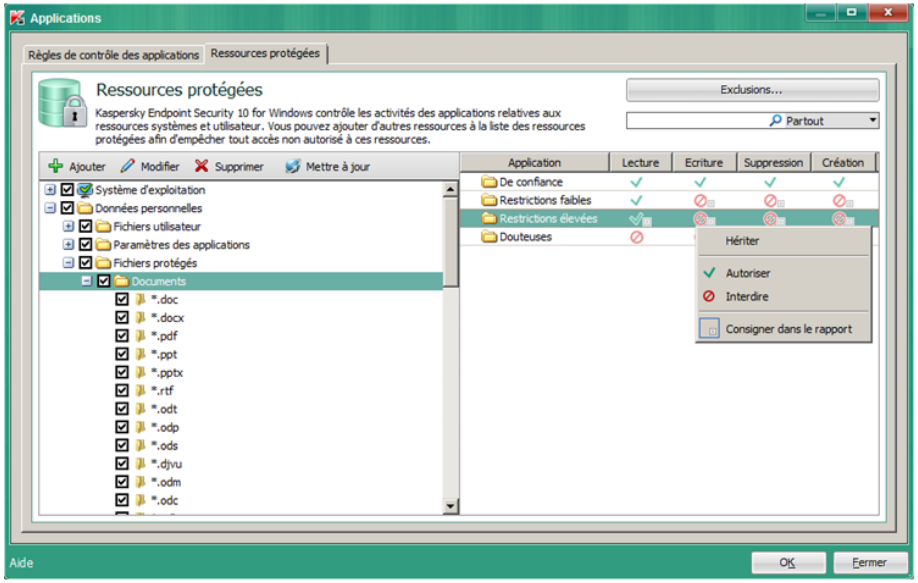
Pour cela il vous suffit de créer une nouvelle ressource protégée, et y référencer les extensions des fichiers que vous souhaitez protéger.

Par exemple, ceux qui possèdent une extension de type doc, docx, xls, pdf, zip vous pourrez même inclure les types de fichier issus de vos applications métiers dans cette liste.

L'étape suivante consiste à configurer les permissions octroyées aux applications catégorisés dans les groupes Restrictions faibles et restrictions élevées afin d'interdire à ces applications la création, la suppression et la modification de ces fichiers appartenant à la liste des extensions protégées.

Vous empêcherez ainsi le cryptomalware de chiffrer vos données sensibles en les protégeant contre toutes modifications.

RENFORCER LA SÉCURITÉ CONTRE LES CRYPTOMALWARE : PROTÉGER VOS DONNÉES



Référencer les extensions de fichiers sensibles :

- Documents (*.doc, *.docx, *.odt, *.pdf, *.pst, etc)
- Images (*.jpeg, *,.jpg, *.png, etc)
- Archives (*.zip, *.rar, *.7z, etc)
- Multimédia (*.avi, *.mp3, *.mpg, etc)
- Bases de données (*.mdb, *.sql, etc)
- Sauvegarde (*.bak, *.back, etc)
- Fichiers sources (*.php, *.js, *.c, etc)
- Fichiers issus d'applications métiers

Configurer les permissions pour les groupes d'applications avec restrictions :

- http://support.kaspersky.com/10905

En résumé

En conclusion et pour se protéger efficacement contre les cryptomalwares, veillez à réaliser une analyse du flux de messagerie sur les différents niveaux de votre infrastructure.

Equipez vos postes de travail d'une suite de sécurité qui pourra protéger vos systèmes contre les menaces en temps réel via une analyse approfondie des fichiers par signature, analyse heuristique, analyse via un système de réputation et analyse comportementale pour les menaces non référencées.

Renforcez le niveau de protection en bloquant les applications inconnues qui tentent de s'exécuter depuis des dossiers systèmes et protégez vos fichiers importants en interdisant toutes modifications par ces mêmes applications inconnues.

Régulièrement, prévenez vos utilisateurs des dangers de la messagerie et surtout des pièces jointes à vérifier avant ouverture.

Enfin et cela constitue la recommandation la plus importante contre les cryptomalwares puisqu'elle vous permettra de récupérer vos données quoi qu'il arrive : sauvegardez régulièrement vos fichiers sensibles à des emplacements inaccessible en écriture sauf pendant la période de sauvegarde, pour éviter de perdre également ces données en cas de chiffrement.

EN RÉSUMÉ

Composantes d'une protection efficace contre les cryptomalware :

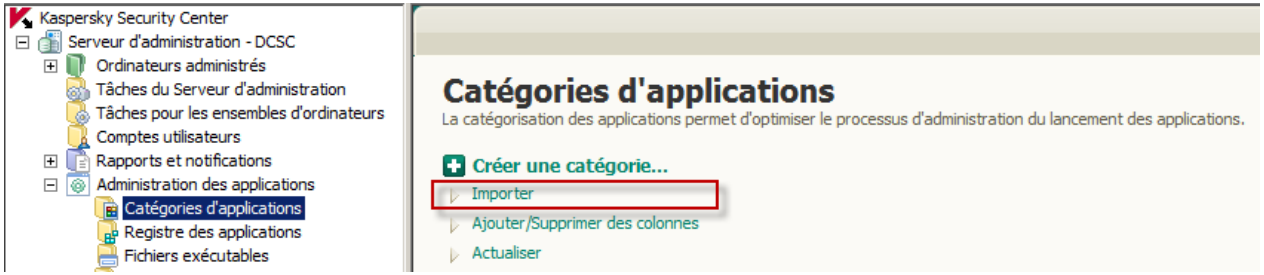
- Protection Antivirus sur le flux de messagerie à différents niveaux de l'infrastructure
- Protection des postes de travail :
  - Analyse en temps réel des fichiers (Antivirus Fichiers)
  - Analyse en temps réel du courrier (Antivirus Courrier)
  - Analyse comportementale (System Watcher)
  - Blocage du lancement d'applications pour les dossiers (Contrôle du lancement des applications)
  - Protection des extensions de fichiers sensibles (Contrôle de l'activité des applications)
- Sensibilisation des utilisateurs aux bonnes pratiques
- **Sauvegarde protégée et régulière des données**

Application des mesures de renforcement de la sécurité

Import de la catégorie

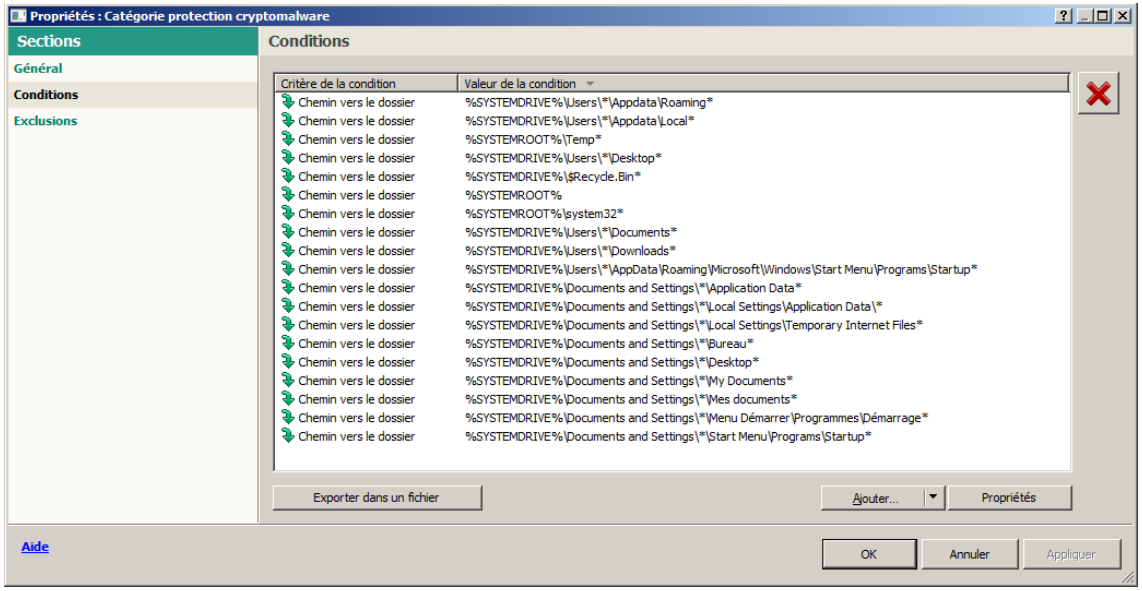
Afin de bloquer le lancement d'applications inconnues depuis certains dossiers du système d'exploitation, vous devez tout d'abord importer la catégorie correspondante depuis votre Console d'Administration Kaspersky Security Center.

Accédez au menu **Administration des applications** puis **Catégories d'applications** et cliquez sur **Importer :**



Indiquez l'emplacement du fichier **Categorie_a_importer.klc** joint à ce document et validez pour importer la catégorie.

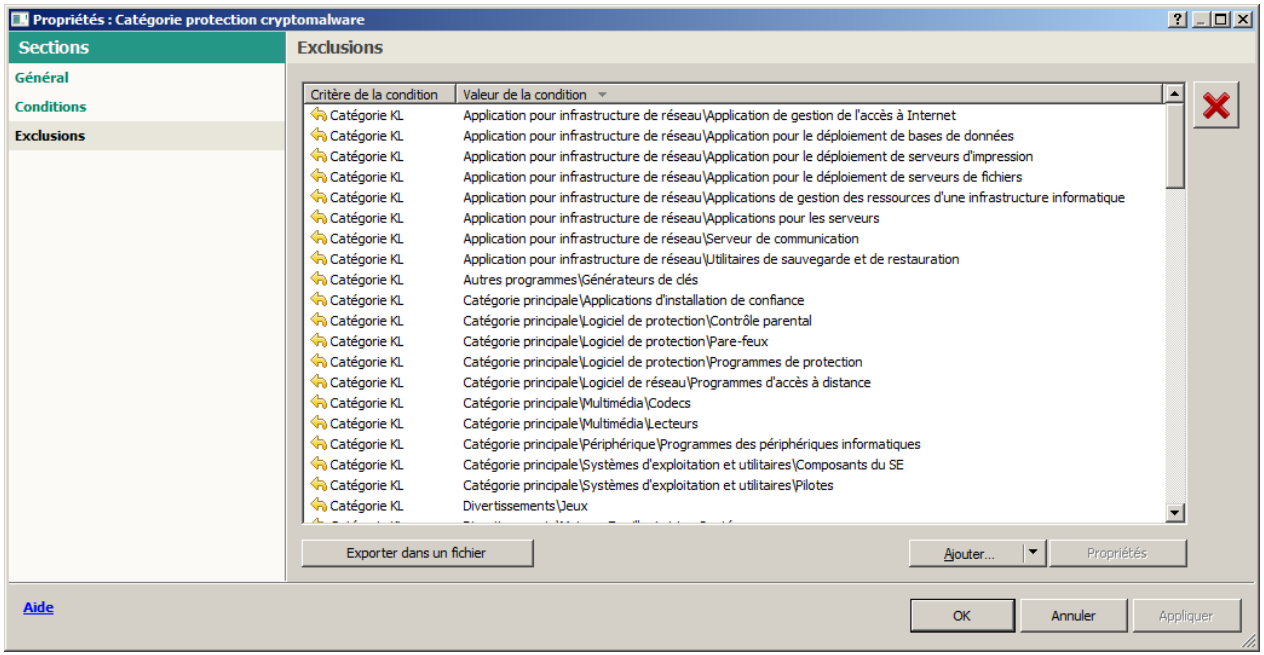
Accédez aux propriétés de la catégorie importée et ouvrez le menu **Conditions** :



Il s'agit de la liste des emplacements possibles pour les fichiers du cryptomalware, également disponible dans cet article de la base de connaissance : http://support.kaspersky.com/viruses/common/10952#block4

A l'aide du bouton **Ajouter…** vous pourrez indiquer d'autres dossiers ou d'autres critères pour renforcer l'étendue de cette protection.

Ouvrez le menu **Exclusions** :



La liste des catégories référencées par Kaspersky Lab permet d'exclure de cette règle de blocage toutes les applications connues (et saines) afin d'autoriser le bon fonctionnement du système d'exploitation et des logiciels métiers.

Vous pourrez parcourir les différentes catégories et voir la liste des applications qu'elles contiennent depuis le catalogue en ligne : http://whitelist.kaspersky.com/catalogue

En cas de blocage d'une application non référencée, reportez-vous à la section En cas de blocage d'une application légitime par le Contrôle du lancement des applications de ce guide.

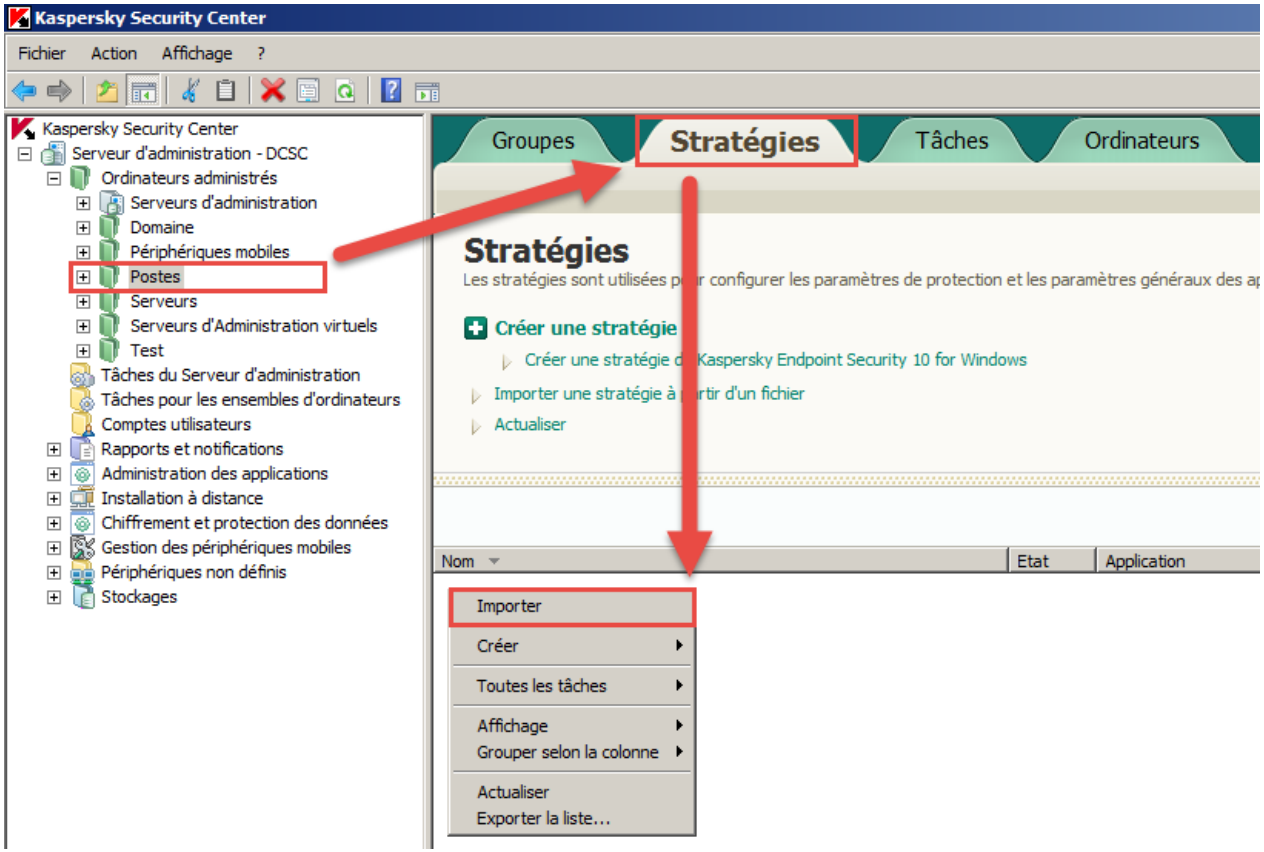
Afin d'autoriser les outils systèmes et vos applications métiers qui ont besoin d'exécuter des fichiers à ces emplacements, vous pouvez exclure les catégories d'applications référencées par Kaspersky Lab et qui couvre de nombreux fichiers grâce à notre travail de référencement.

A l'aide de bouton **Ajouter…** vous pourrez indiquer d'autres applications à exclure de l'étendue de la protection.

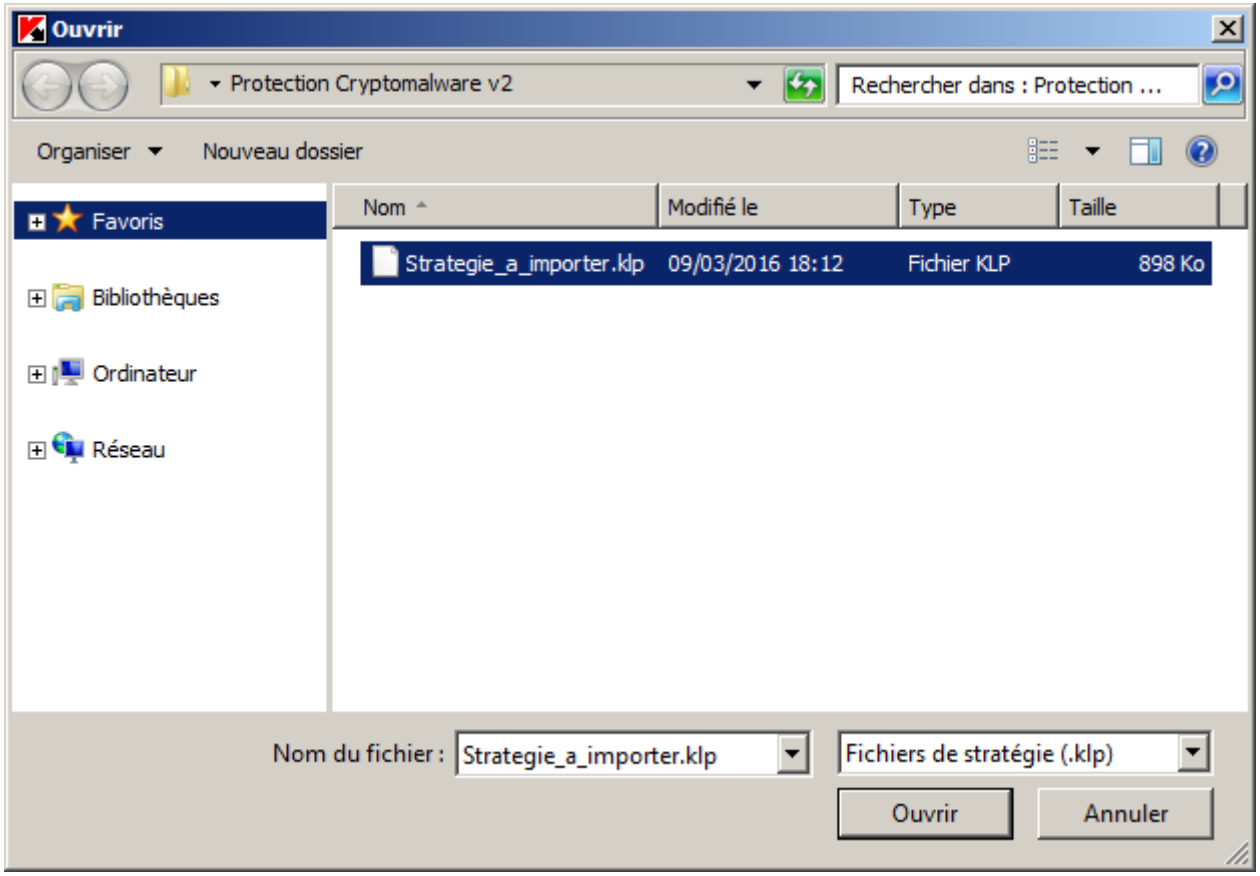
Import de la stratégie

L'étape suivante consiste à importer la stratégie qui permettra d'appliquer les restrictions correspondantes sur vos postes de travail.

Si vous avez créé un groupe dédié pour les postes de travail, vous pouvez y intégrer directement cette stratégie. Dans le cas contraire il est possible de l'insérer à la racine dans le groupe des **Ordinateurs administrés**. Sélectionnez le groupe correspondant, puis cliquez sur l'onglet **Stratégies**. Effectuez un clic droit dans la zone centrale et sélectionnez **Importer** :

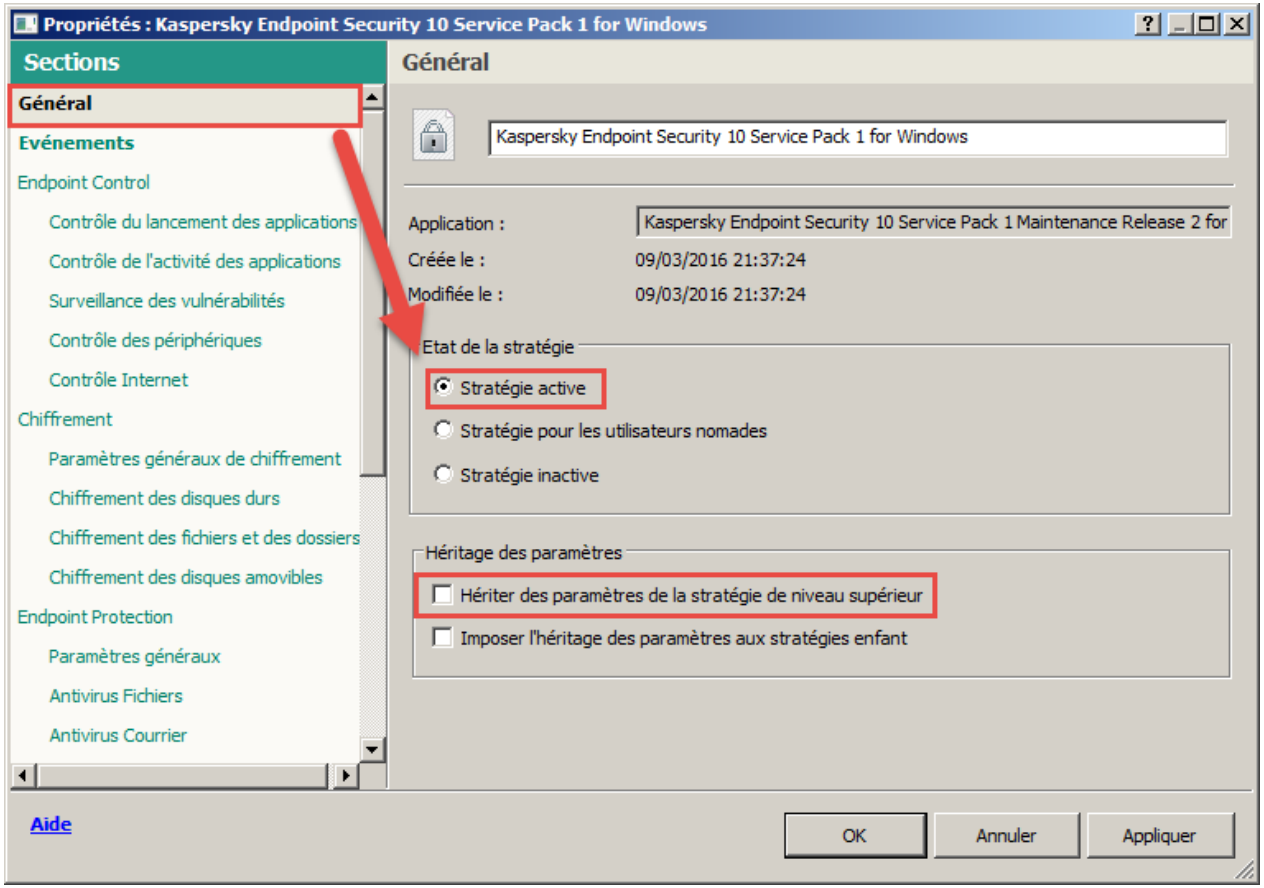


Parcourez l'arborescence et indiquez l'emplacement du fichier **Strategie_a_importer.klp** disponible dans l'archive téléchargée. Cliquez sur le bouton **Ouvrir** :



La stratégie apparaît alors dans la Console d'Administration, par défaut son état est désactivé, celle-ci ne s'applique donc à aucune machine administrée. Depuis le menu contextuel de cette stratégie, sélectionnez **Propriétés** :

Une fois la stratégie importée, il est nécessaire de l'activer. Sélectionnez **Stratégie active** dans le menu **Général** de la fenêtre des propriétés :

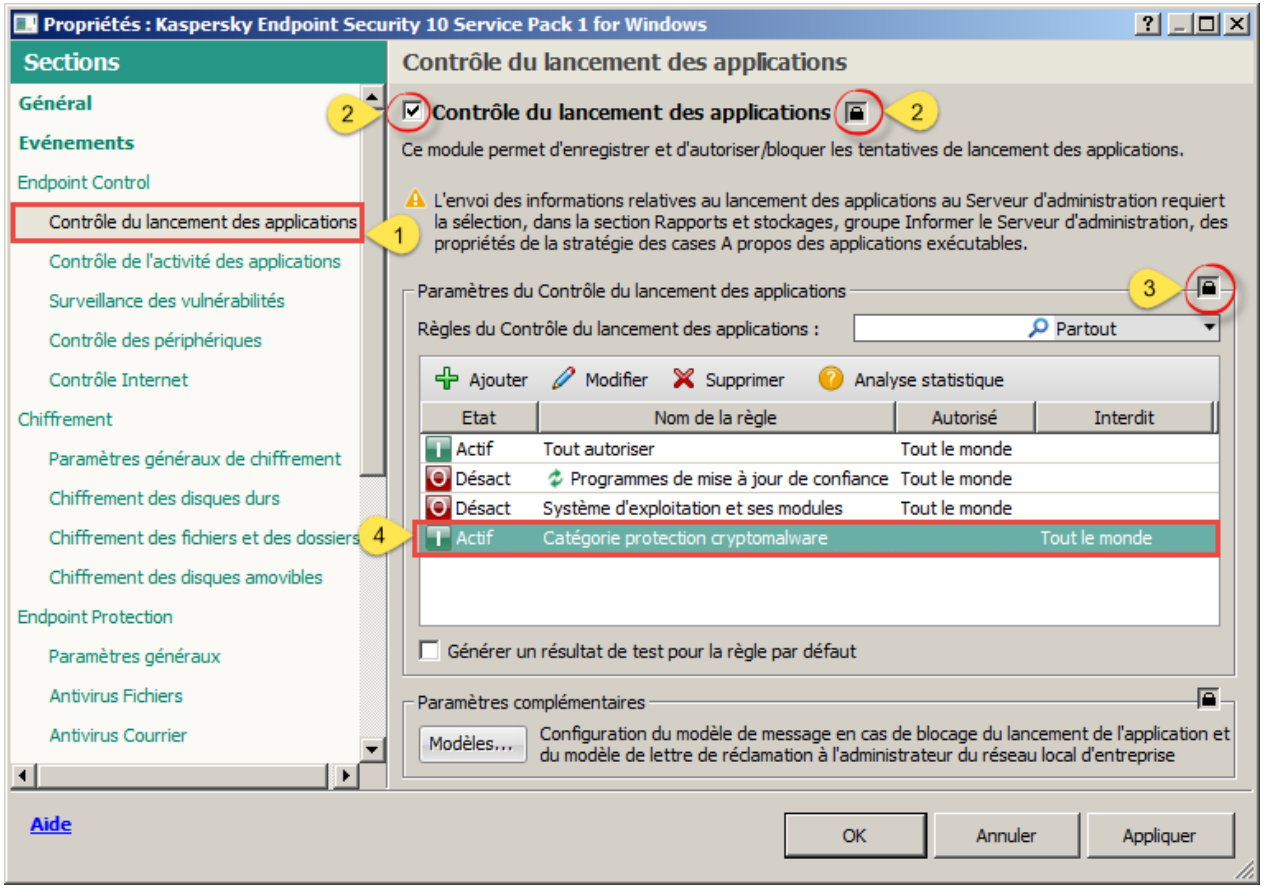


Si vous avez importé la stratégie dans un sous-groupe, veillez à ce que l'option **Hériter des paramètres de la stratégie de niveau supérieur** soit bien désactivée. Cela désactive le système d'héritage et évite que les paramètres de cette stratégie soient écrasés par ceux de la stratégie située à un niveau plus élevée dans l'arborescence des ordinateurs administrés.

Application des restrictions de lancement d'applications inconnues

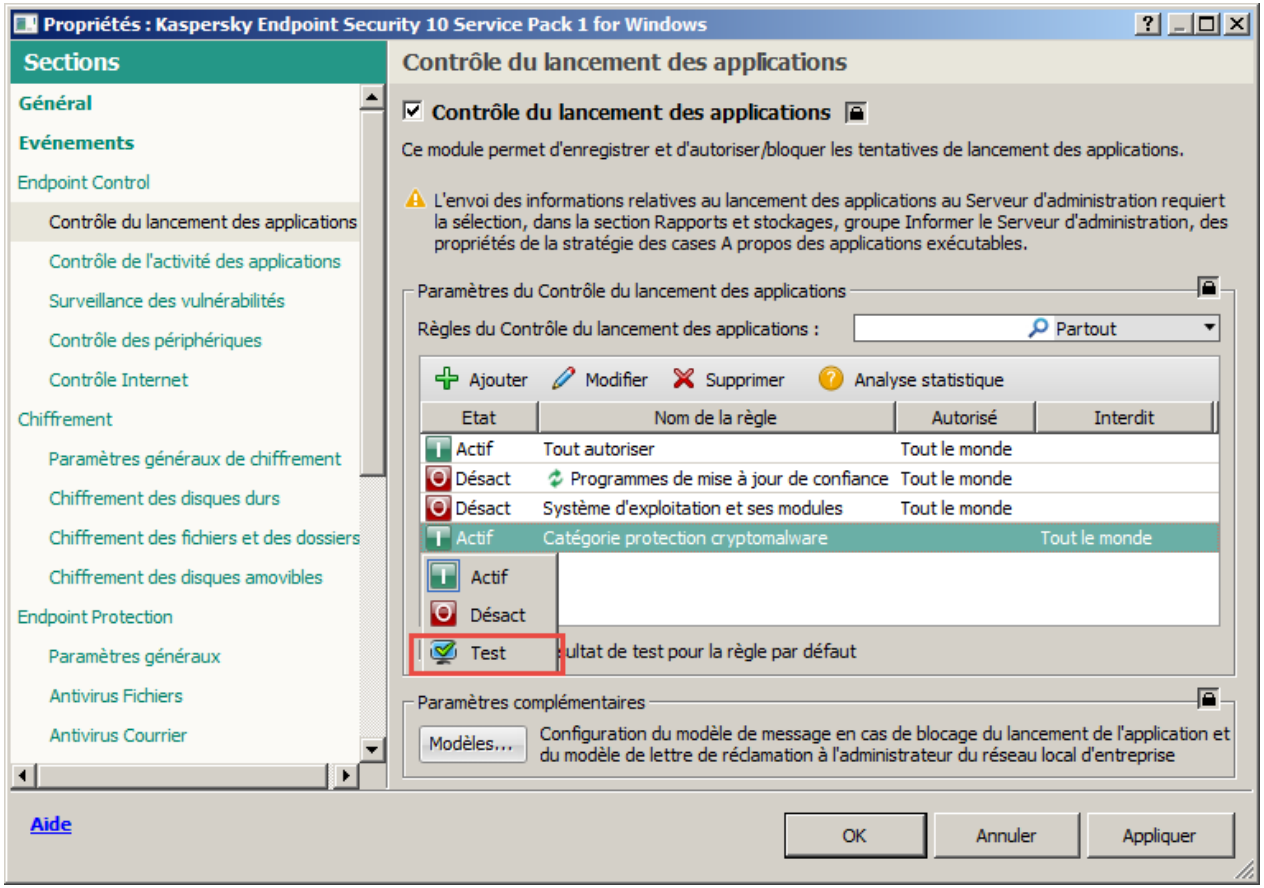
Une fois la stratégie active, vérifiez la configuration du module de **Contrôle du lancement des applications** afin de restreindre le lancement d'applications inconnues depuis les dossiers de la catégorie importée précédemment.

1. Sélectionnez le module **Contrôle du lancement des applications**.
2. Assurez-vous que le module **Contrôle du lancement des applications** est bien activé et le cadenas correspondant correctement verrouillé
3. Assurez-vous que le cadenas de la zone **Paramètres du Contrôle du lancement des applications** est bien verrouillé
4. Assurez-vous de la présence de la règle **Catégorie protection cryptomalware** et veillez à ce que celle-ci s'applique à tous les utilisateurs : groupe **Tout le monde** spécifié dans la colonne **Interdit**.

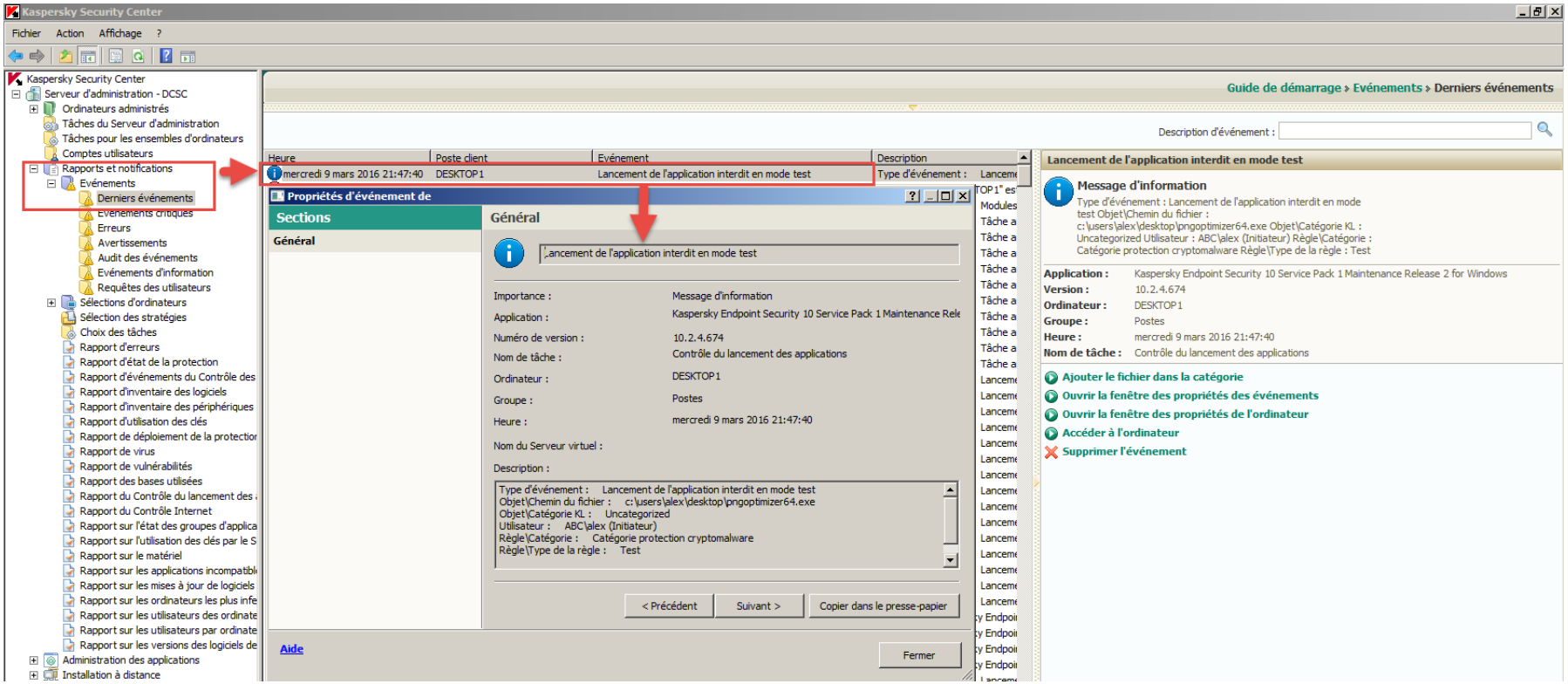


Si vous souhaitez tester cette règle avant de la généraliser, vous pouvez modifier son état sur le mode **Test**. Celui-ci ne bloque pas l'exécution de fichiers sur les postes de travail mais génère un évènement si un blocage avait eu lieu en mode **Actif**, cela permet de

valider le bon fonctionnement de ce paramétrage avec votre environnement (applications métiers, configuration système, etc.) avant un passage en production :



Dans ce mode **Test**, vous trouverez les évènements dans la Console d'Administration Kaspersky Security Center, dans le menu **Rapports et notifications**, **Evénements** :



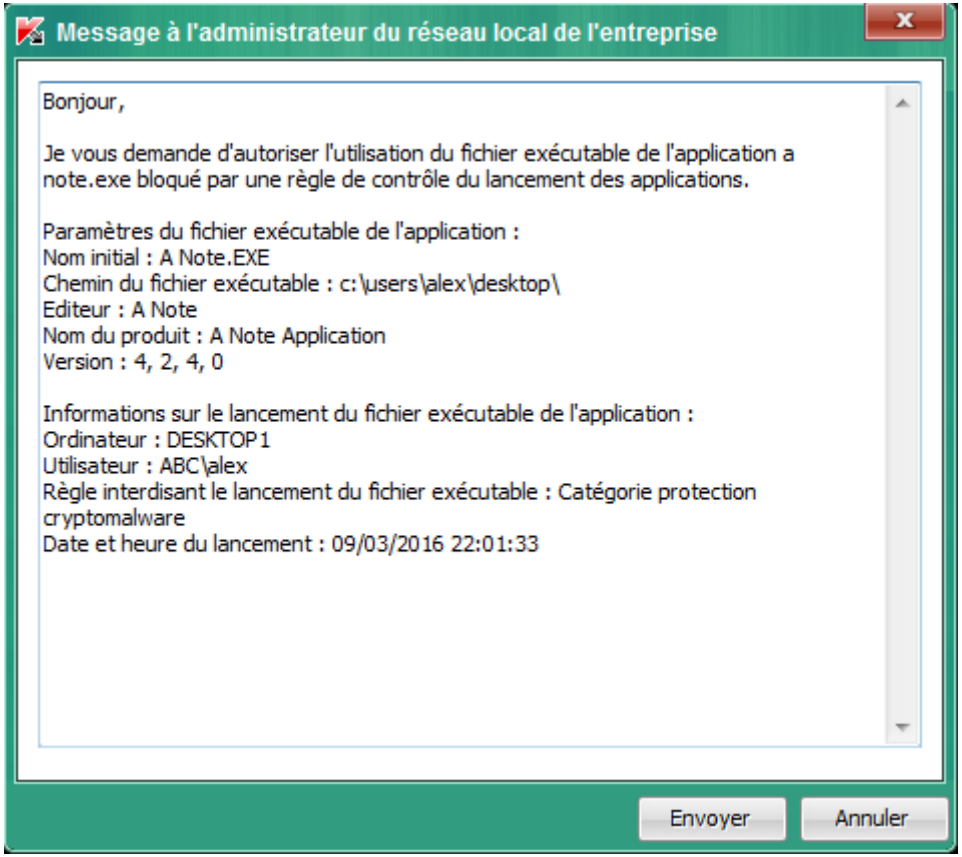
En cas de blocage d'une application légitime par le Contrôle du lancement des applications

Lorsqu'une application légitime est bloquée lors de son lancement, il est nécessaire de créer une exclusion pour celle-ci. Il existe différente façons de procéder à la création de cette exclusion, elles sont décrites ci-dessous.

Option n°1 : utiliser le système de plainte des utilisateurs via la Console d'Administration

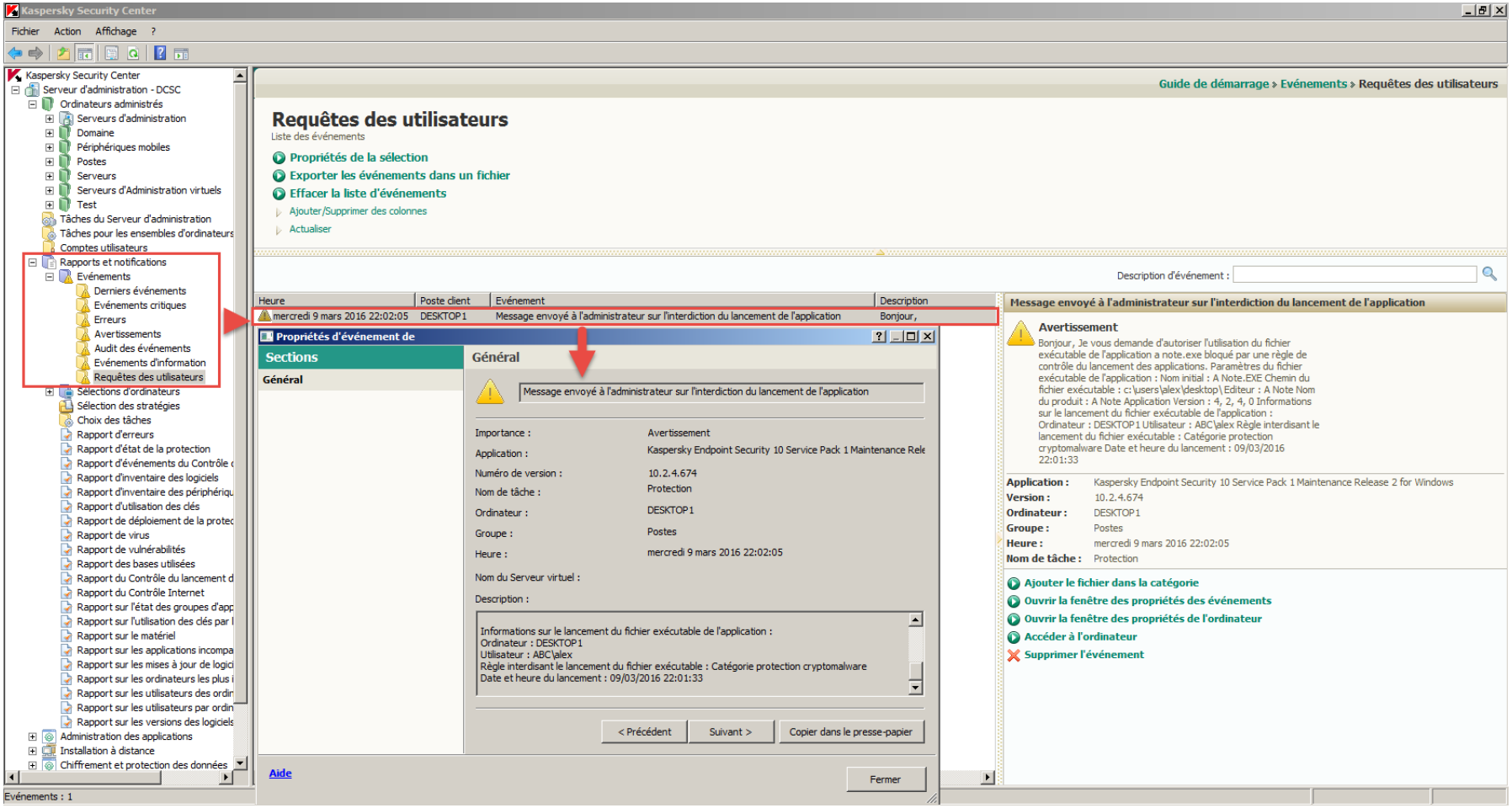
Lorsque l'exécution d'une application est bloquée l'utilisateur est notifié sur son écran par un message d'erreur MS Windows ainsi qu'une info-bulle de Kaspersky Endpoint Security for Windows. Cette dernière alerte comporte un lien **Se plaindre…** que l'utilisateur peut activer pour contester le blocage :

La nouvelle fenêtre qui s'ouvre contient un texte pré-rempli avec les informations issues du fichier bloqué telles que le nom du fichier, son emplacement, l'éditeur, le nom de la machine ou encore le nom de la session ouverte :



Lorsque l'utilisateur clique sur le bouton **Envoyer**, la plainte est envoyée au Serveur d'Administration Kaspersky Security Center.

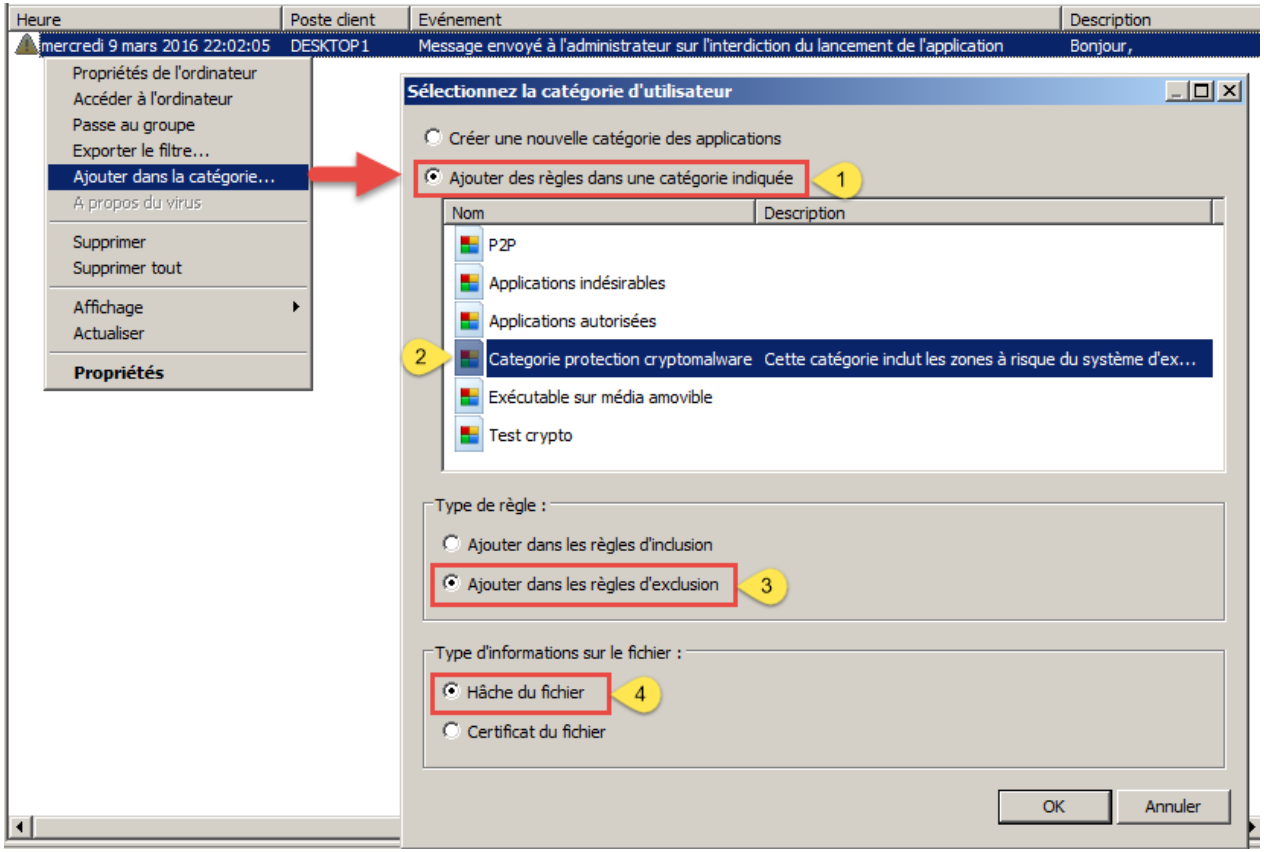
L’administrateur pourra visualiser le contenu de la plainte depuis la Console d’Administration, menu **Rapports et notifications** > **Evénements** > **Requêtes des utilisateurs** :



Veillez à bien lire le contenu de la plainte et à vérifier si le blocage concerne un fichier important pour le bon fonctionnement d’une application métier.

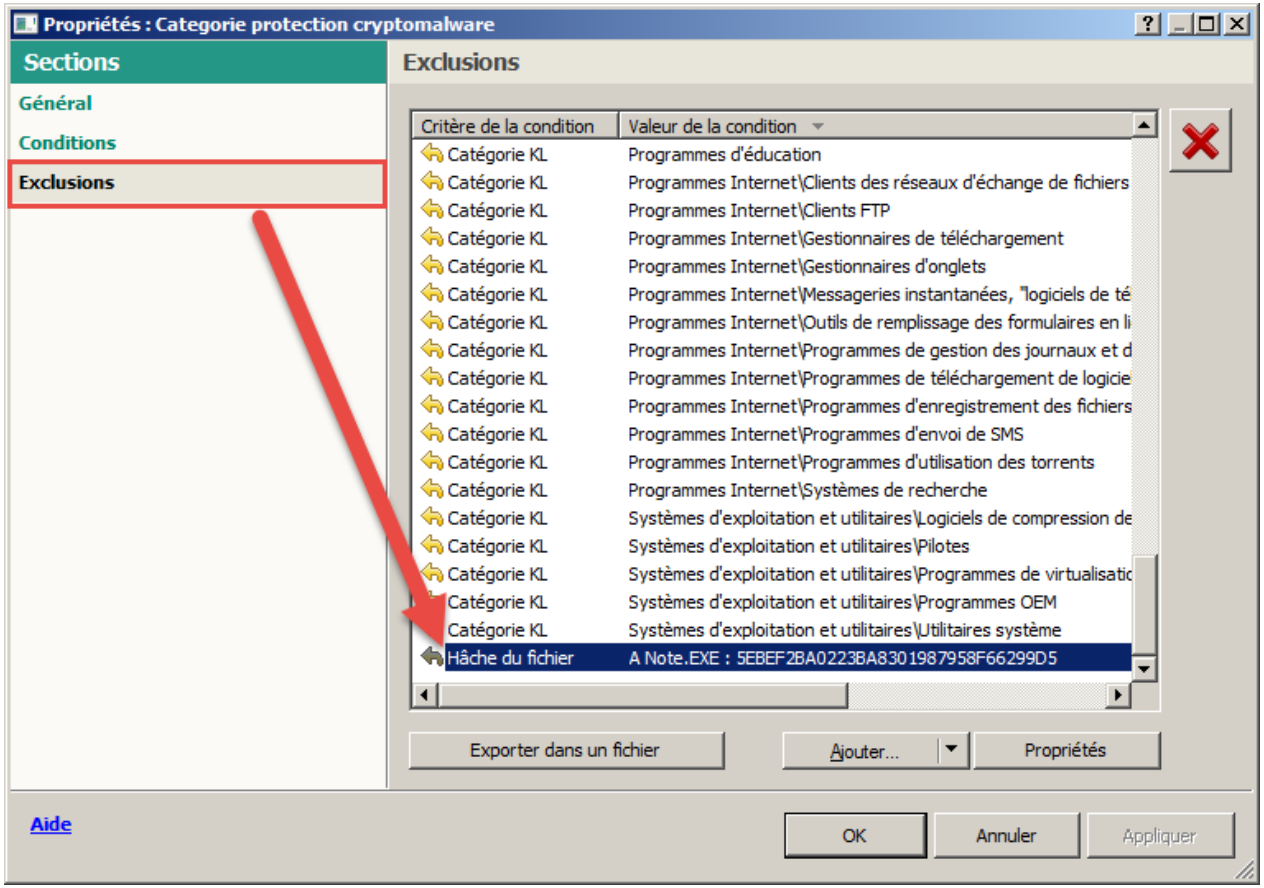
Pour exclure rapidement le fichier de l’étendue du blocage, effectuez un clic droit sur l’évènement et sélectionnez **Ajouter dans la catégorie…**

Dans la nouvelle fenêtre apparue, sélectionnez **Ajouter des règles dans une catégorie indiquée**, puis la catégorie **Categorie protection cryptomalware**, ensuite **Ajouter dans les règles d'exclusion** et enfin **Hâche du fichier**.



Cliquez sur **OK** pour valider les modifications apportées à la catégorie.

Vous pourrez vérifier l'ajout de ce fichier dans les exclusions en accédant aux propriétés de la catégorie correspondante, dans le menu **Exclusion** :



La catégorie ainsi modifiée se synchronise ensuite automatiquement sur les machines administrées, l'application des modifications peut être immédiate si les flux réseaux correspondants sont ouverts (port UDP 15000 accessible sur les machines administrées pour le Serveur d'Administration), dans le cas contraire il faudra patienter le délai de synchronisation (15 minutes, par défaut).

Exécutez le fichier qui était bloqué sur le poste de travail et assurez-vous que le blocage a été correctement levé.

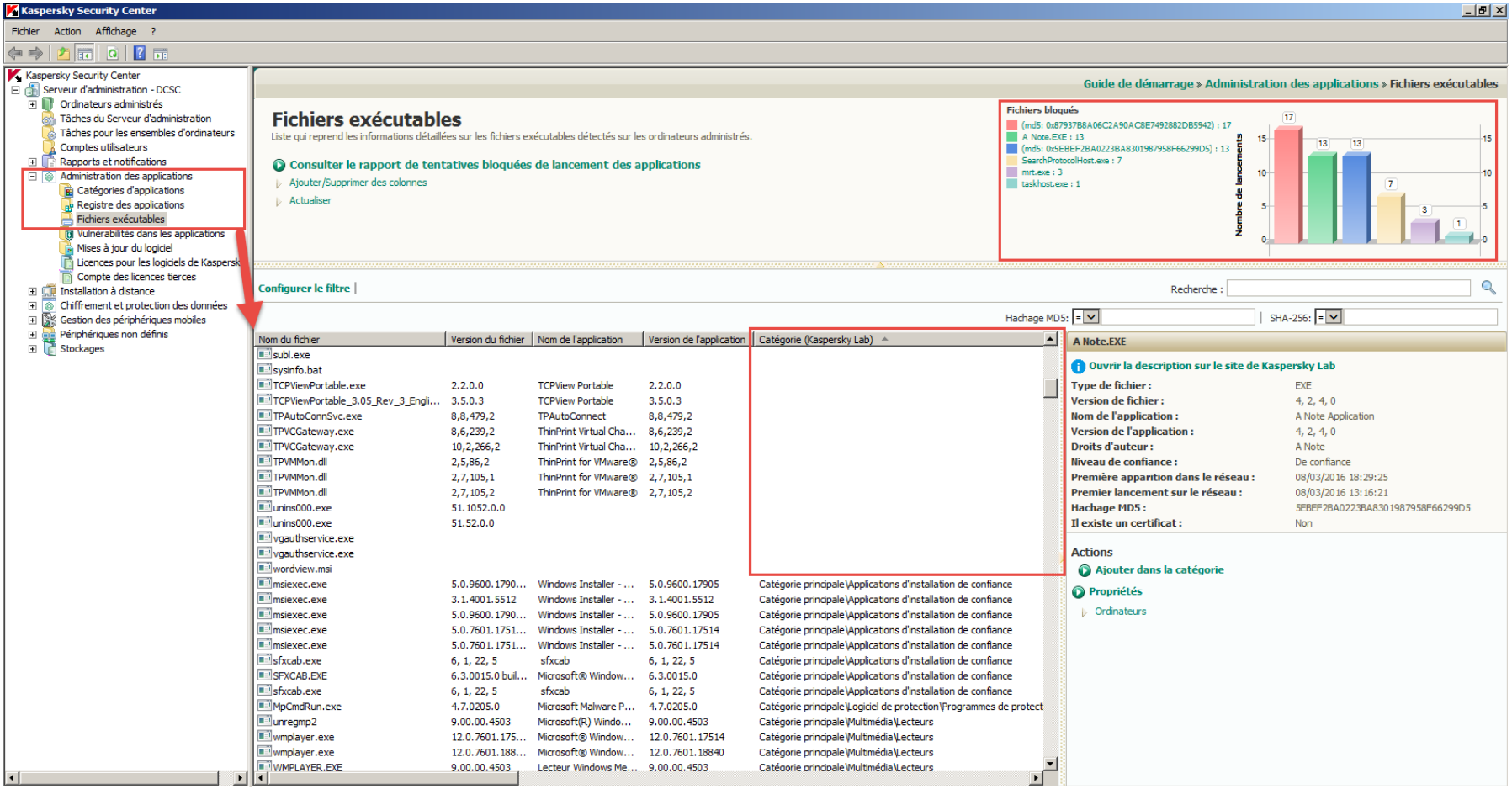
Vous pourrez également supprimer la plainte traitée de la liste depuis le menu **Requête des utilisateurs**.

Option n°2 : utiliser le registre des fichiers exécutables

Ce menu affiche la liste des fichiers exécutables détectés sur les postes clients. Après application de la stratégie importée, les informations peuvent mettre du temps à remonter, si la liste est vide patientez au moins 1 cycle de synchronisation (15 minutes par défaut).

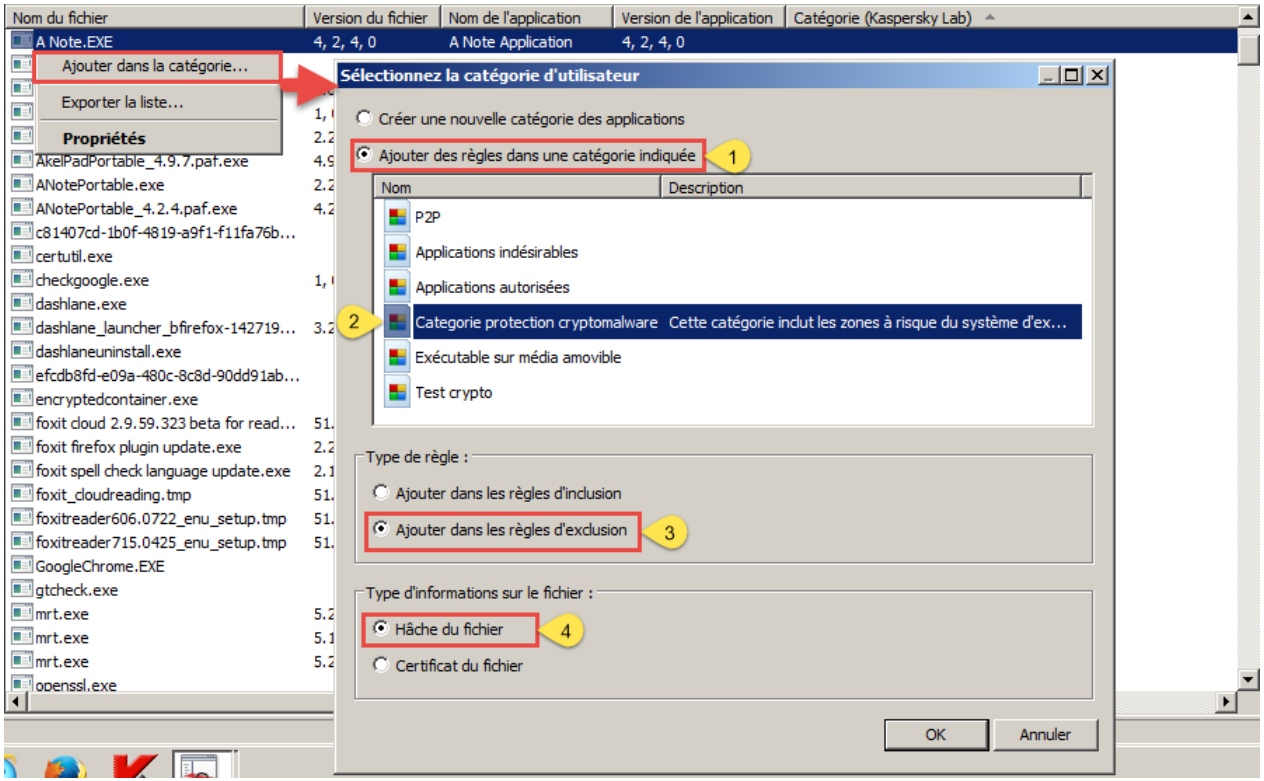
Depuis cette fenêtre, il est rapidement possible d'obtenir les informations suivantes :

- TOP des exécutables bloqués dans le graphique situé en haut à droite
- Liste des exécutables non catégorisé par Kaspersky Lab et potentiellement bloqué. Vous pouvez effectuer un classement selon la colonne **Catégorie (Kaspersky Lab)** pour voir rapidement les fichiers exécutables concernés.



Pour exclure rapidement le fichier de l'étendue du blocage, effectuez un clic droit sur l'évènement et sélectionnez **Ajouter dans la catégorie…**

Dans la nouvelle fenêtre apparue, sélectionnez **Ajouter des règles dans une catégorie indiquée**, puis la catégorie **Categorie protection cryptomalware**, ensuite **Ajouter dans les règles d'exclusion** et enfin **Hâche du fichier**.

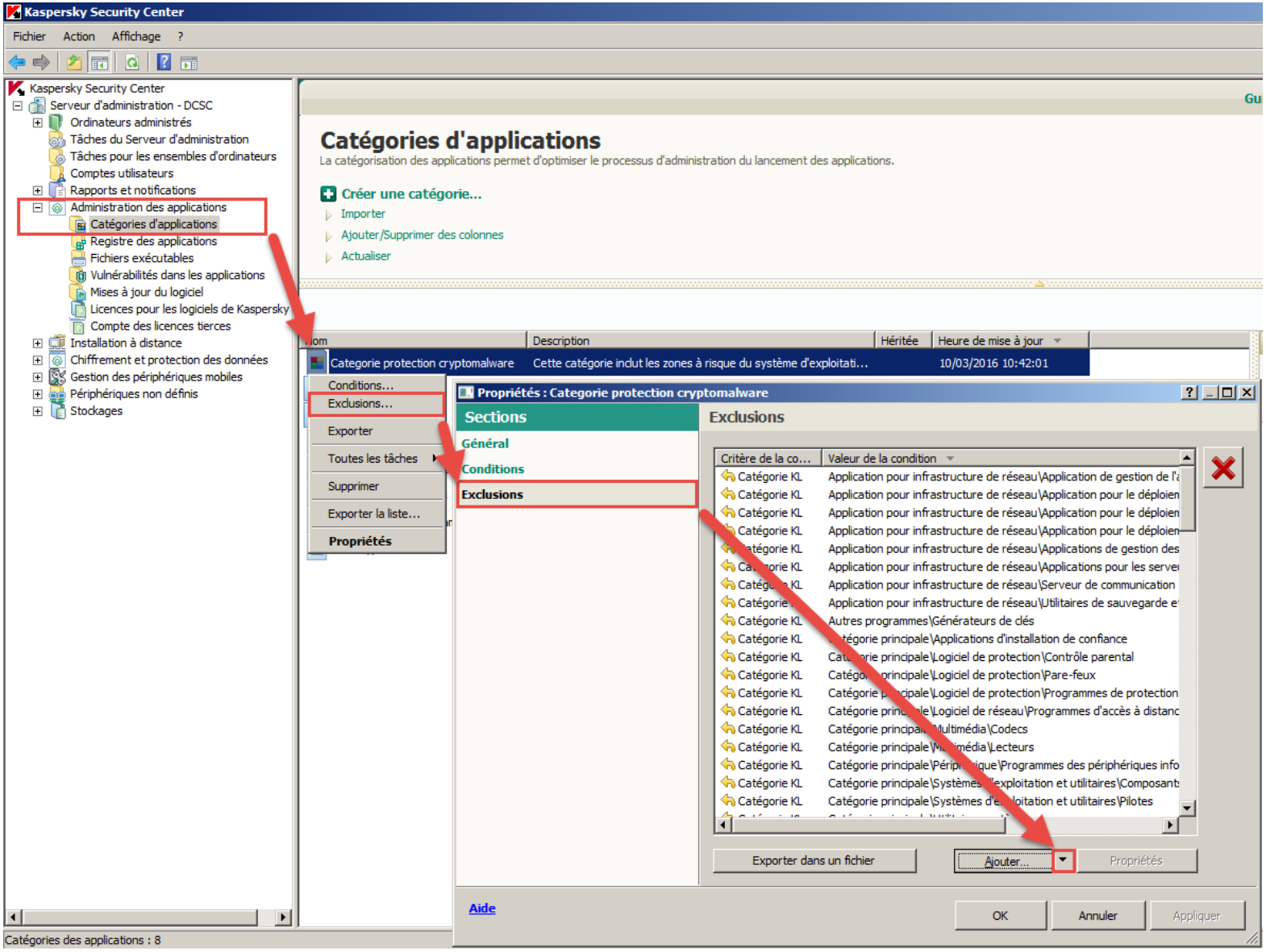


Note : il est possible de sélectionner plusieurs exécutables à l'aide des boutons **SHIFT** et **CTRL** afin d'ajouter plusieurs éléments dans les règles d'exclusion de la catégorie.

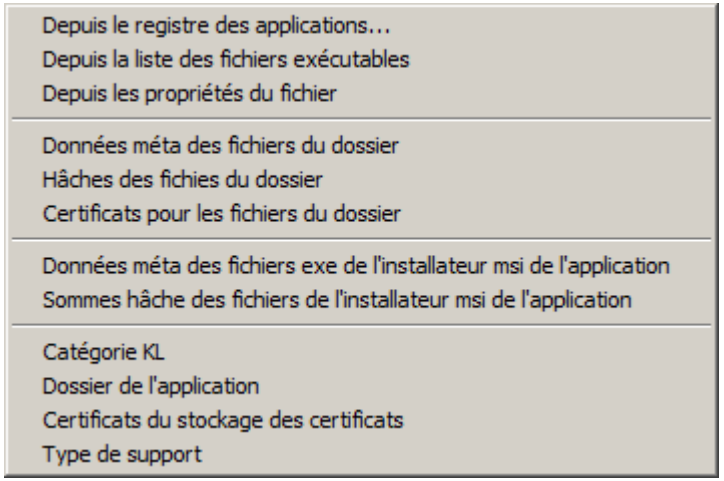
Cliquez sur **OK** pour valider les modifications apportées à la catégorie.

Option n°3 : créer manuellement les règles d'exclusion dans la catégorie

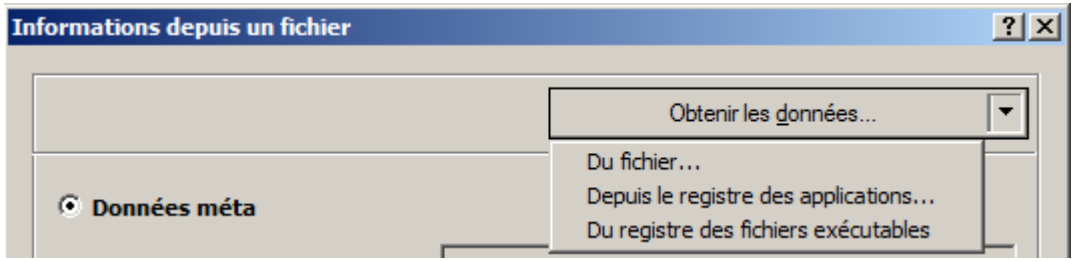
Les règles d'exclusion basées sur le hash d'un fichier deviennent obsolètes lorsque l'application est mise à jour, car le hash est modifié. Pour un choix plus large d'options concernant les règles d'exclusion, vous pouvez modifier directement la liste depuis les propriétés de la catégorie. Accédez au menu **Administration des applications**, puis **Catégories d'applications** de la Console d'Administration et sélectionnez l'option **Exclusions** dans les propriétés de la catégorie **Categorie protection cryptomalware** :



Cliquez sur la flèche à droite du bouton **Ajouter…** plusieurs possibilités d'ajout d'éléments sont alors disponibles :



Par exemple, vous pourrez utiliser les métadonnées d'un fichier afin de créer une règle plus souple que celle qui se repose uniquement sur le hash. Sélectionnez l'option **Depuis les propriétés du fichier** et dans la nouvelle fenêtre apparue, utilisez l'une des 3 méthodes proposées pour récupérer les informations du fichier :

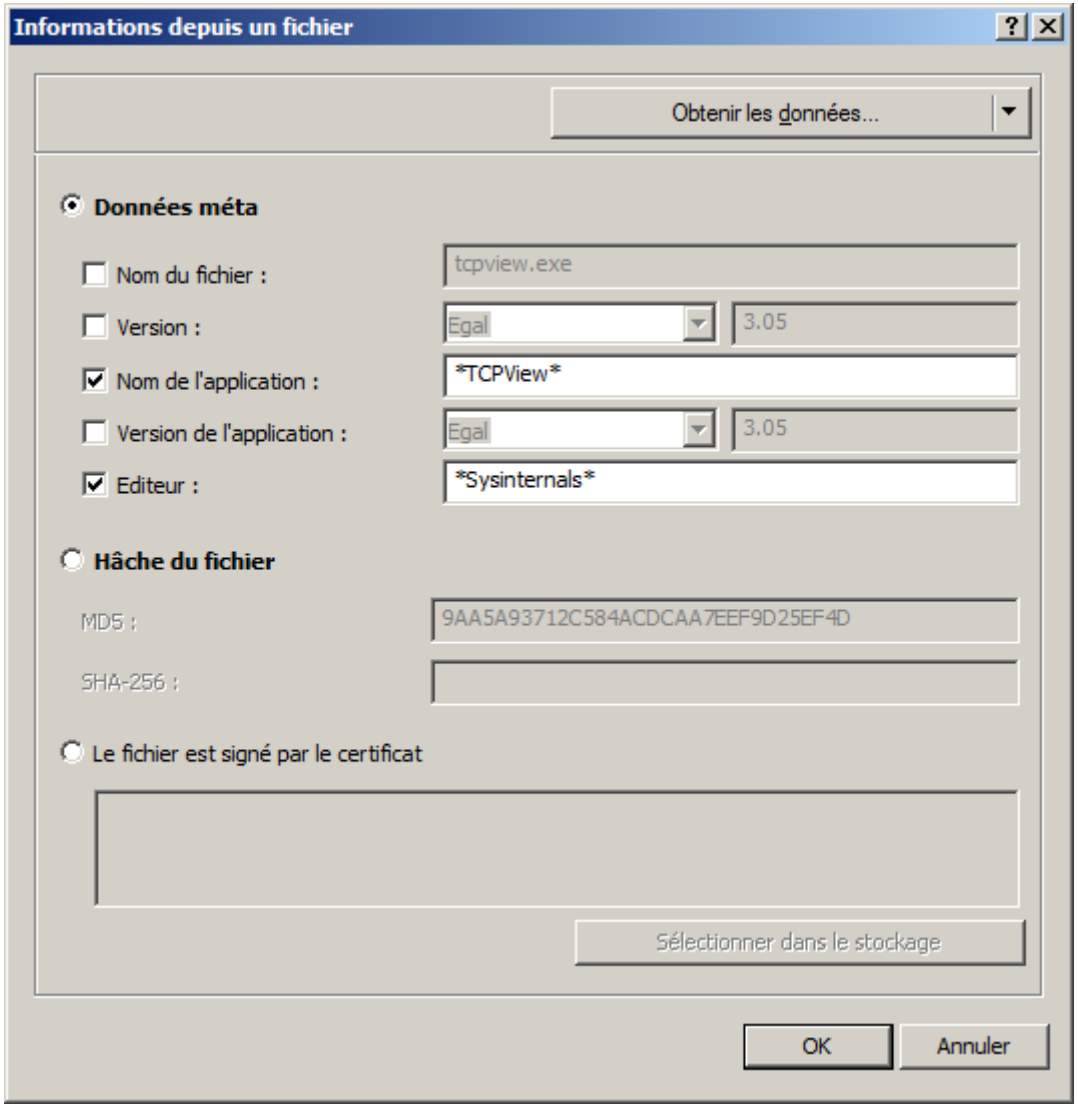


En utilisant le contenu des champs **Nom du fichier**, **Version**, **Nom de l'application**, **Version de l'application** et **Editeur**, vous pourrez créer des règles d'exclusion basées sur l'un ou plusieurs de ces critères.

Les champs **Version** et **Version de l'application** permettent de préciser un numéro de version à l'aide de plusieurs expressions.

Un masque contenant le caractère * permet de remplacer n'importe quelle chaîne de caractères. Ainsi, il est possible de créer une règle et d'y inclure toutes les applications ou une application spécifique développée par un éditeur en particulier.

Exemple : autoriser toutes les versions de l'application TCPView développée par Sysinternals :

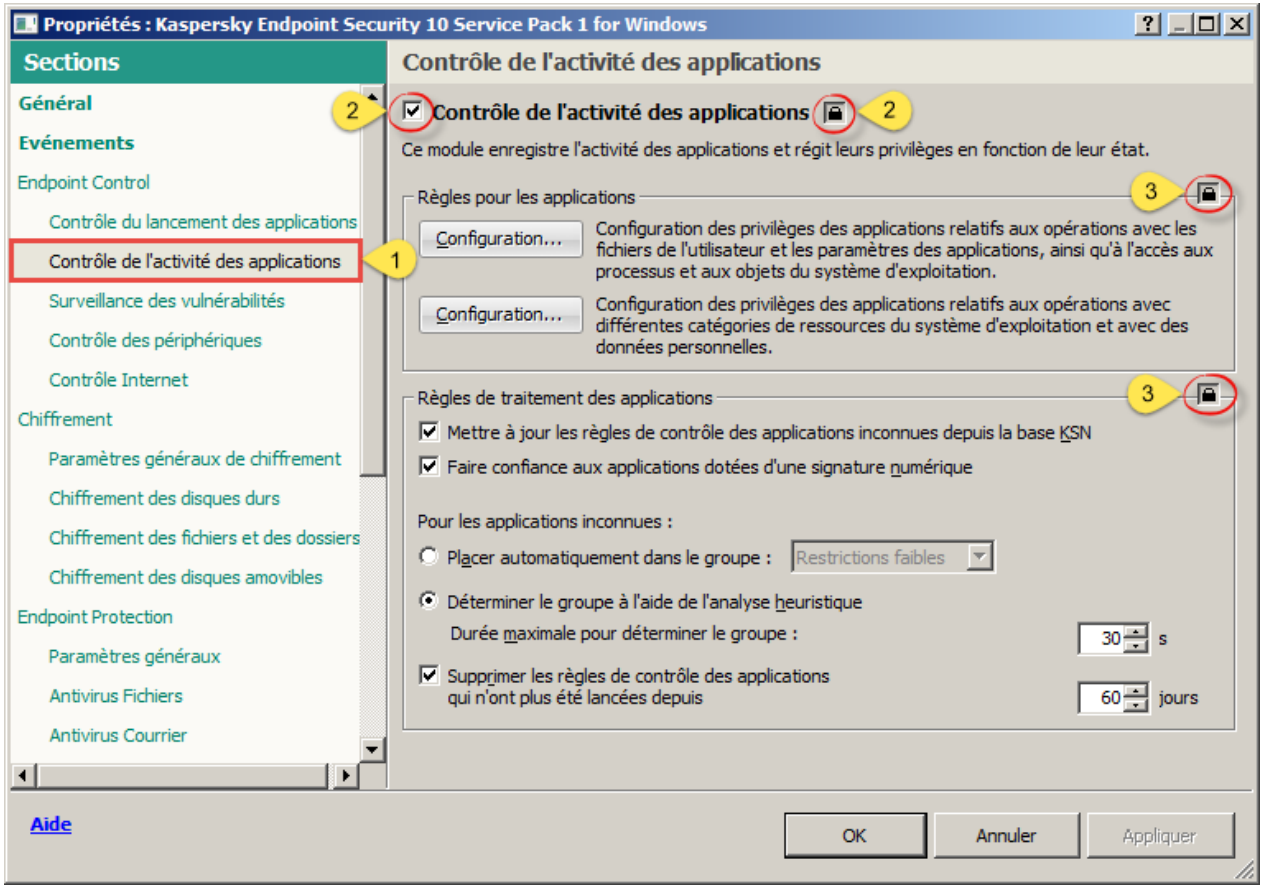


Attention, les règles d'exclusion définies à partir de critères peu précis (par exemple, sur le critère **Nom du fichier** uniquement) peuvent constituer un risque car il n'est pas rare qu'un code malveillant usurpe le nom d'un programme légitime et connu pour passer inaperçu.

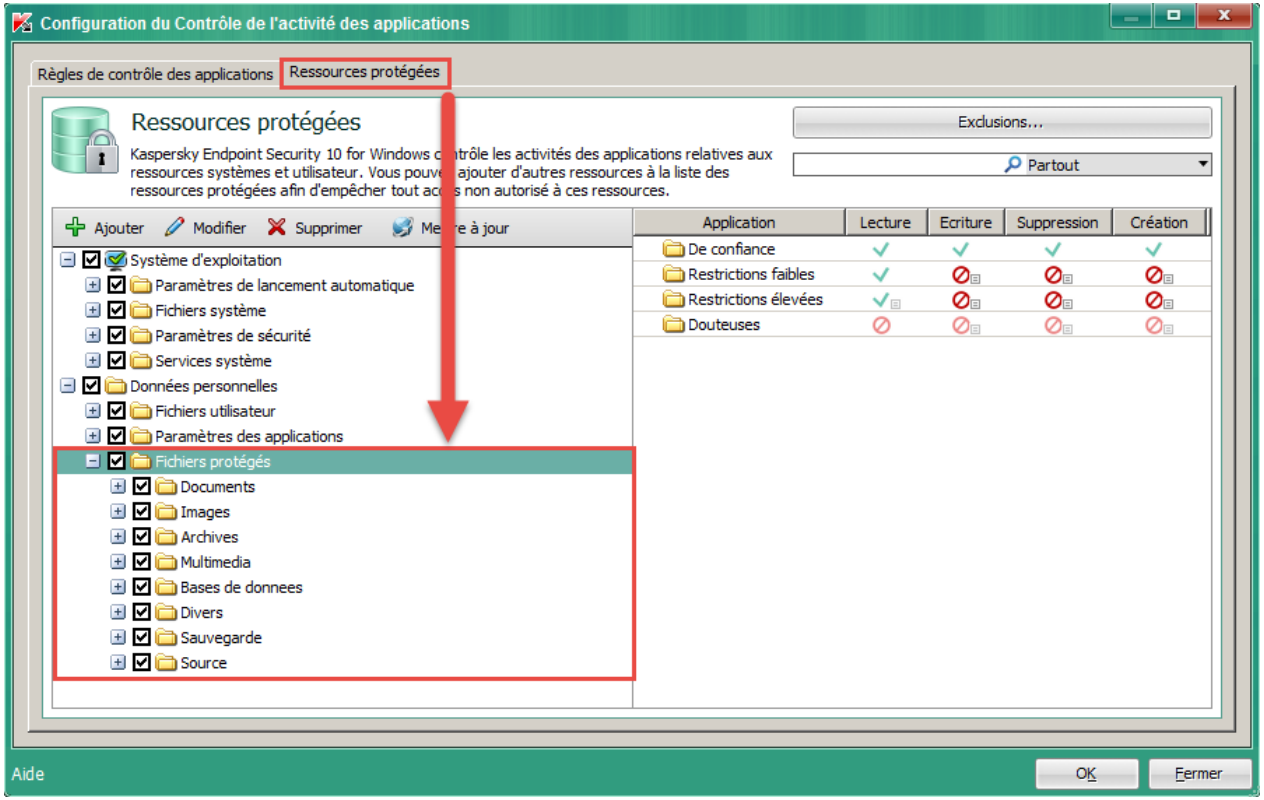
Application des restrictions contre les modifications de données sensibles

Une fois la stratégie active, vérifiez la configuration du module de **Contrôle de l'activité des applications** afin de restreindre les modifications de vos fichiers importants par les applications inconnues.

1. Sélectionnez le module **Contrôle de l'activité des applications**.
2. Assurez-vous que le module **Contrôle de l'activité des applications** est bien activé et le cadenas correspondant correctement verrouillé
3. Assurez-vous que les cadenas des zones **Règles pour les applications** et **Règles de traitement des applications** sont bien verrouillés



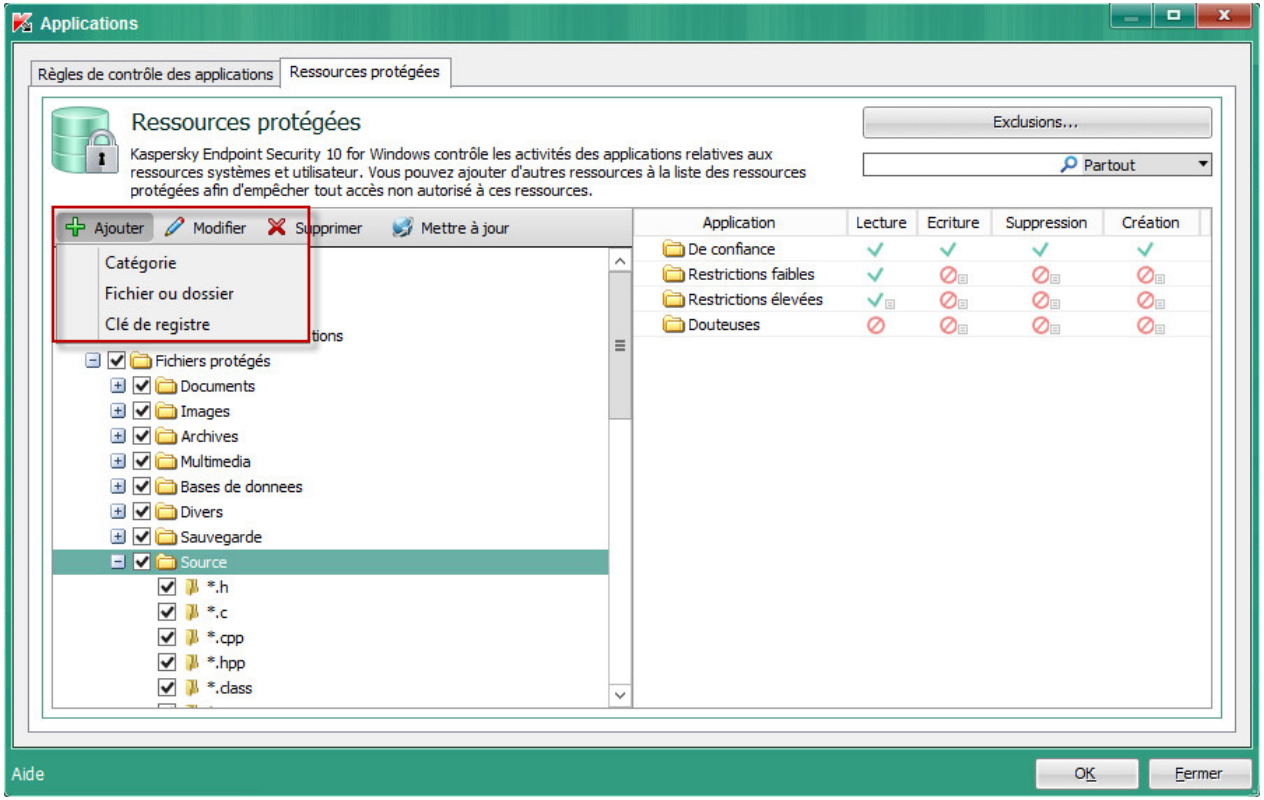
4. Cliquez sur le bouton **Configuration…** du bas et dans la nouvelle fenêtre apparue, dans l'onglet **Ressources protégées**, assurez-vous de la présence du dossier **Fichiers protégés** et de ces sous-dossiers :



En plus de la liste des ressources protégées par défaut, le dossier **Fichiers protégés** contient les extensions de fichiers usuels à protéger contre le chiffrement par les cryptomalwares :

- Documents (*.doc, *.docx, *.xls, *.pdf, etc.)
- Images (*.jpeg, *.jpg, *.png, etc.)
- Archives (*.zip, *.rar, *.7z, etc.)
- Multimédia (*.avi, *.mp3, *.mpeg, etc.)
- Bases de données (*.mdf, *.sql, *.mdb, etc.)
- Divers (*.iso, *.pst, *.crt, etc.)
- Sauvegarde (*.bak, *.old, *.dba, etc.)
- Source (*.h, *.cpp, *.cs, etc.)

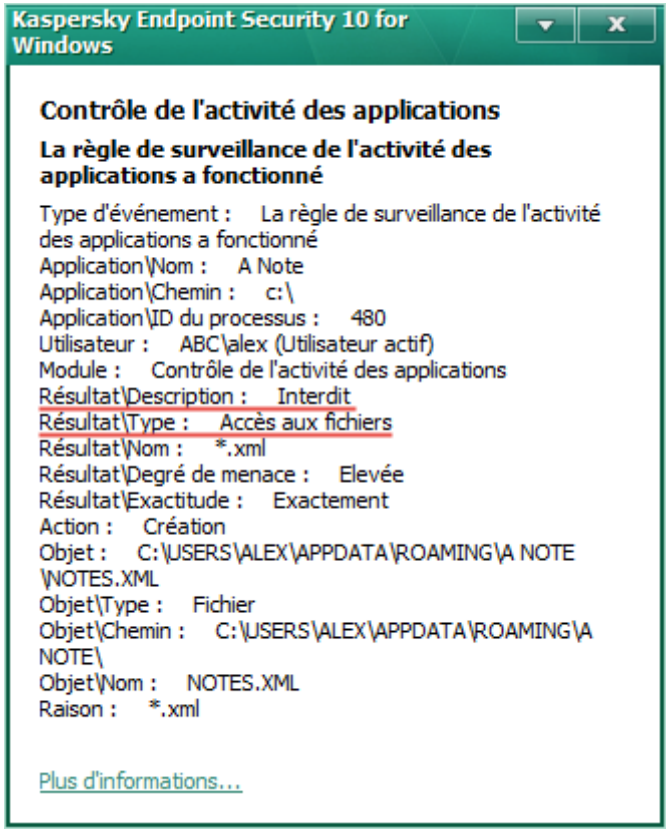
Vous pouvez ajouter les extensions des fichiers non référencées et correspondant à vos données importantes, par exemple celles qui sont générées par vos applications métiers. Utilisez le moteur de recherche pour vérifier la présence d'une extension dans la liste :



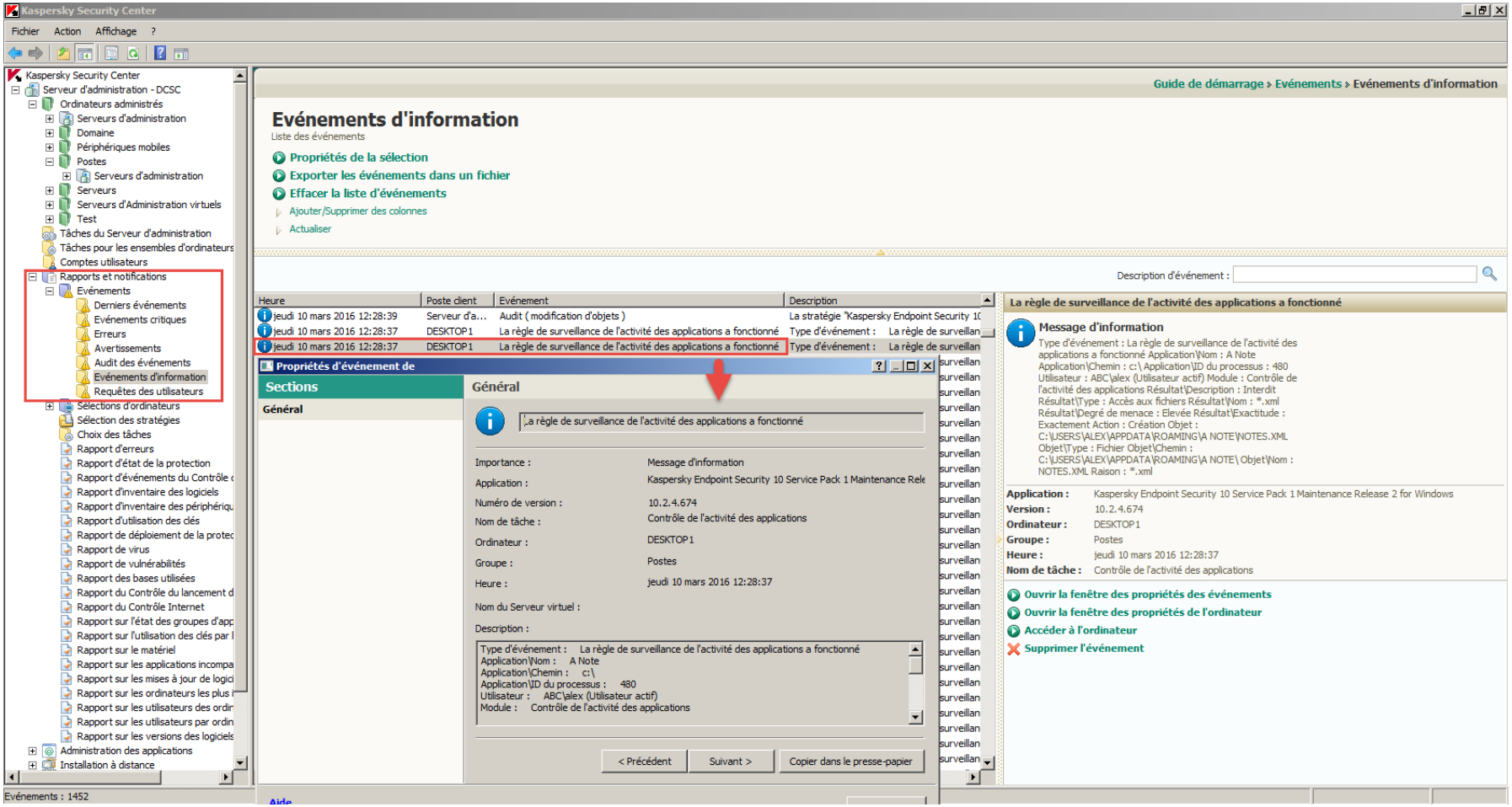
En cas de blocage d'une application légitime par le Contrôle de l'activité des applications

Lorsqu'une application légitime n'est pas autorisée à effectuer des actions (écriture, modification ou suppression) sur des fichiers protégés, il est nécessaire de créer une exclusion pour celle-ci.

L'utilisateur est notifié par un message sur son bureau contenant les détails de la restriction :



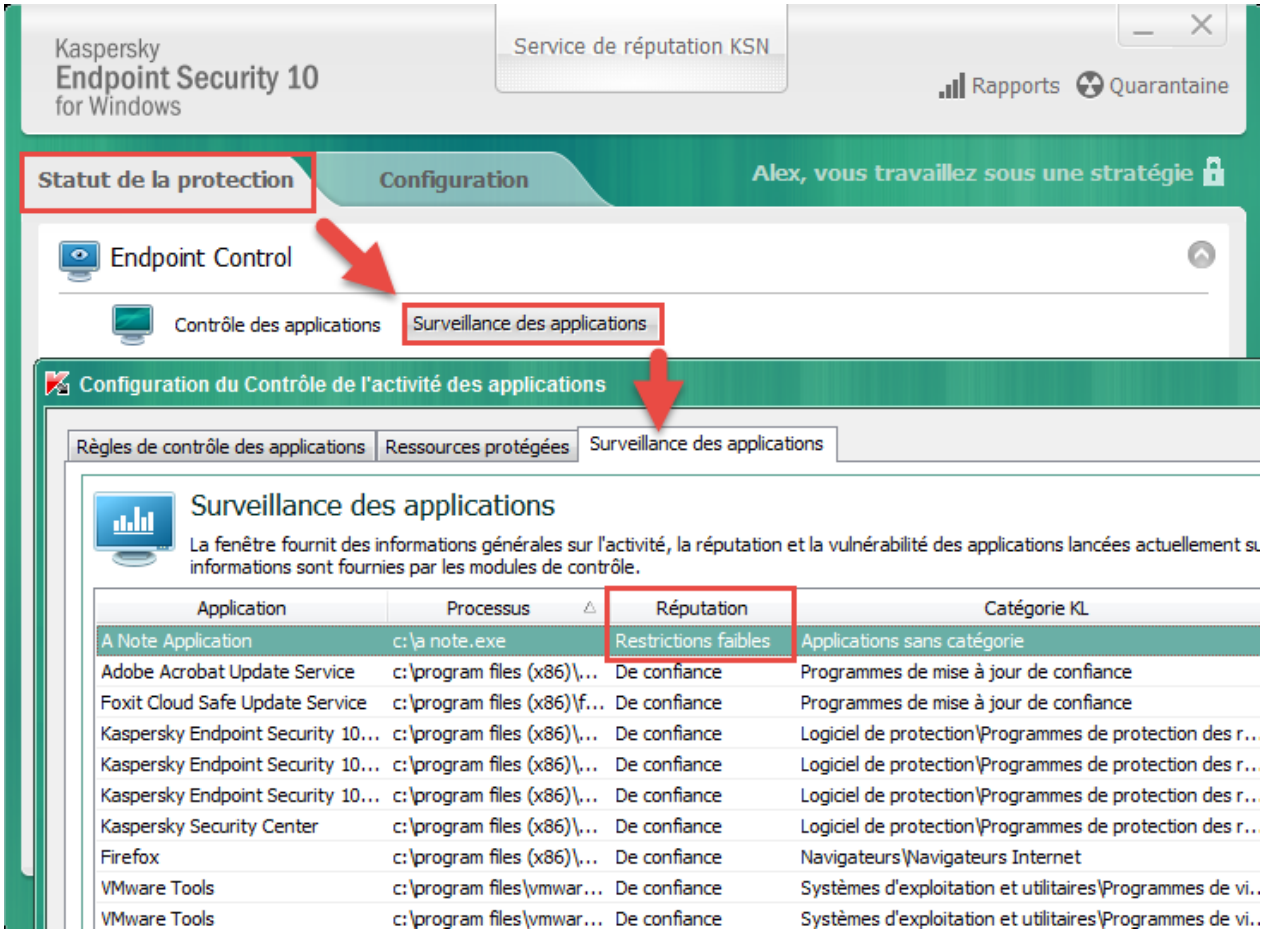
L'administrateur pourra visualiser la même information dans le menu **Rapports et notification**, **Evénements** puis **Evénements d'informations** :



Cela signifie que l'application a été placée dans l'un des groupes à restriction lors de son lancement par Kaspersky Endpoint Security for Windows:

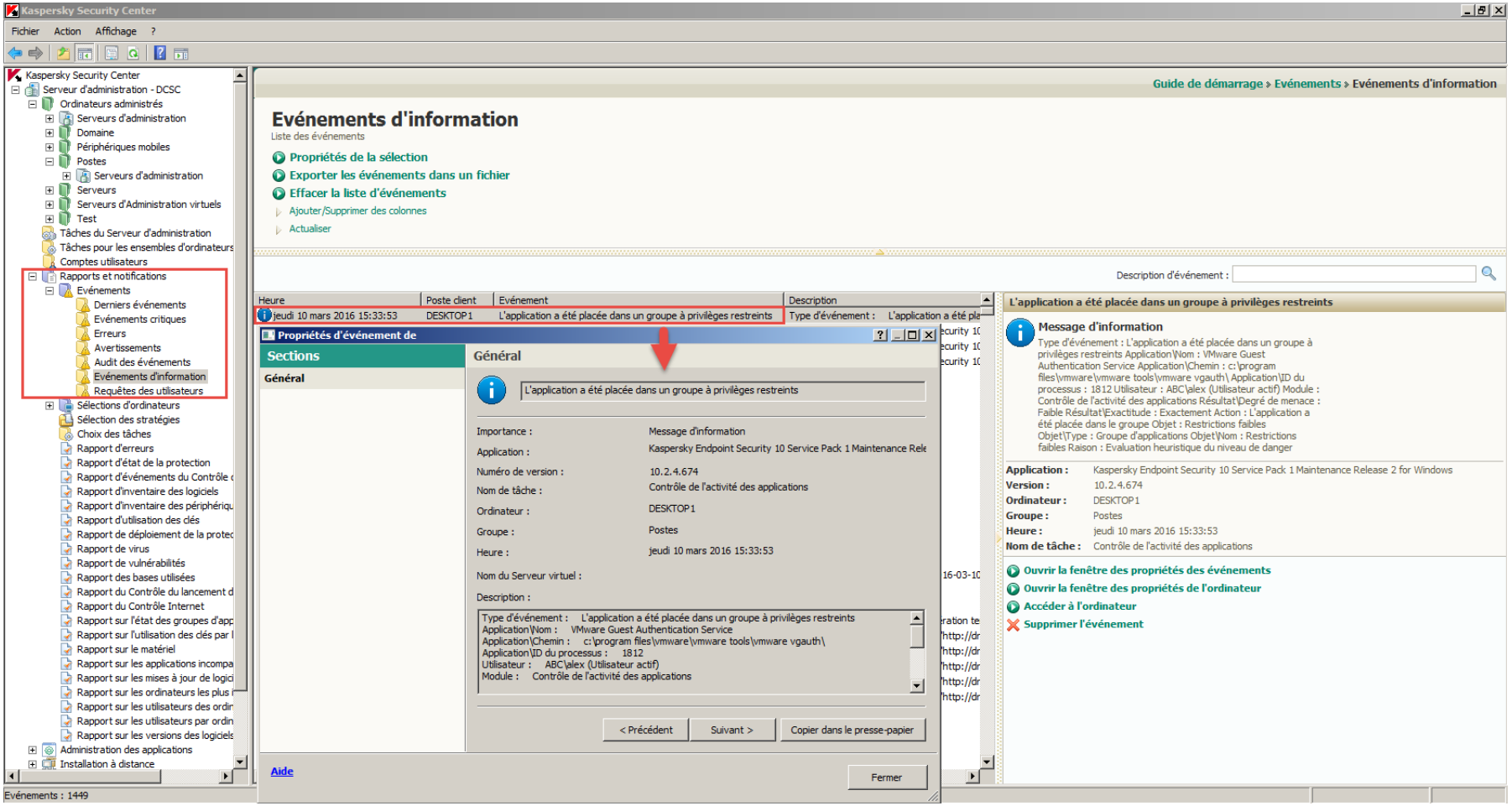
- Restriction faibles
- Restrictions élevées

Il est possible de visualiser cette information depuis l'interface locale de l'application Kaspersky Endpoint Security for Windows, dans l'onglet **Statut de la protection** cliquez sur le bouton **Surveillance des applications** et observez le contenu de la colonne **Réputation** pour l'application concernée :

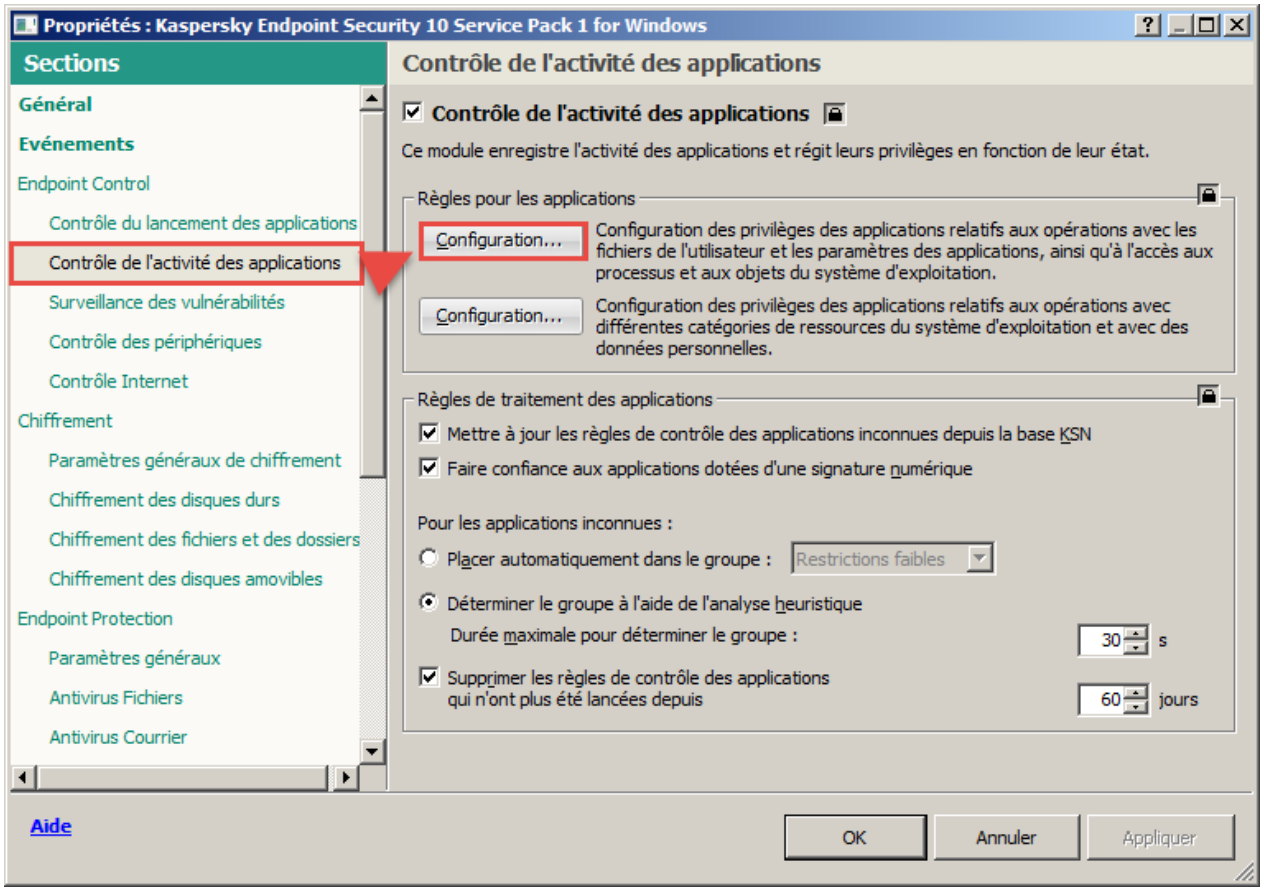


Application	Processus	Réputation	Catégorie KL
A Note Application	c:\a note.exe	Restrictions faibles	Applications sans catégorie
Adobe Acrobat Update Service	c:\program files (x86)\...	De confiance	Programmes de mise à jour de confiance
Foxit Cloud Safe Update Service	c:\program files (x86)\f...	De confiance	Programmes de mise à jour de confiance
Kaspersky Endpoint Security 10...	c:\program files (x86)\...	De confiance	Logiciel de protection\Programmes de protection des r...
Kaspersky Endpoint Security 10...	c:\program files (x86)\...	De confiance	Logiciel de protection\Programmes de protection des r...
Kaspersky Endpoint Security 10...	c:\program files (x86)\...	De confiance	Logiciel de protection\Programmes de protection des r...
Kaspersky Security Center	c:\program files (x86)\...	De confiance	Logiciel de protection\Programmes de protection des r...
Firefox	c:\program files (x86)\...	De confiance	Navigateurs\Navigateurs Internet
VMware Tools	c:\program files\vmwar...	De confiance	Systèmes d'exploitation et utilitaires\Programmes de vi...
VMware Tools	c:\program files\vmwar...	De confiance	Systèmes d'exploitation et utilitaires\Programmes de vi...

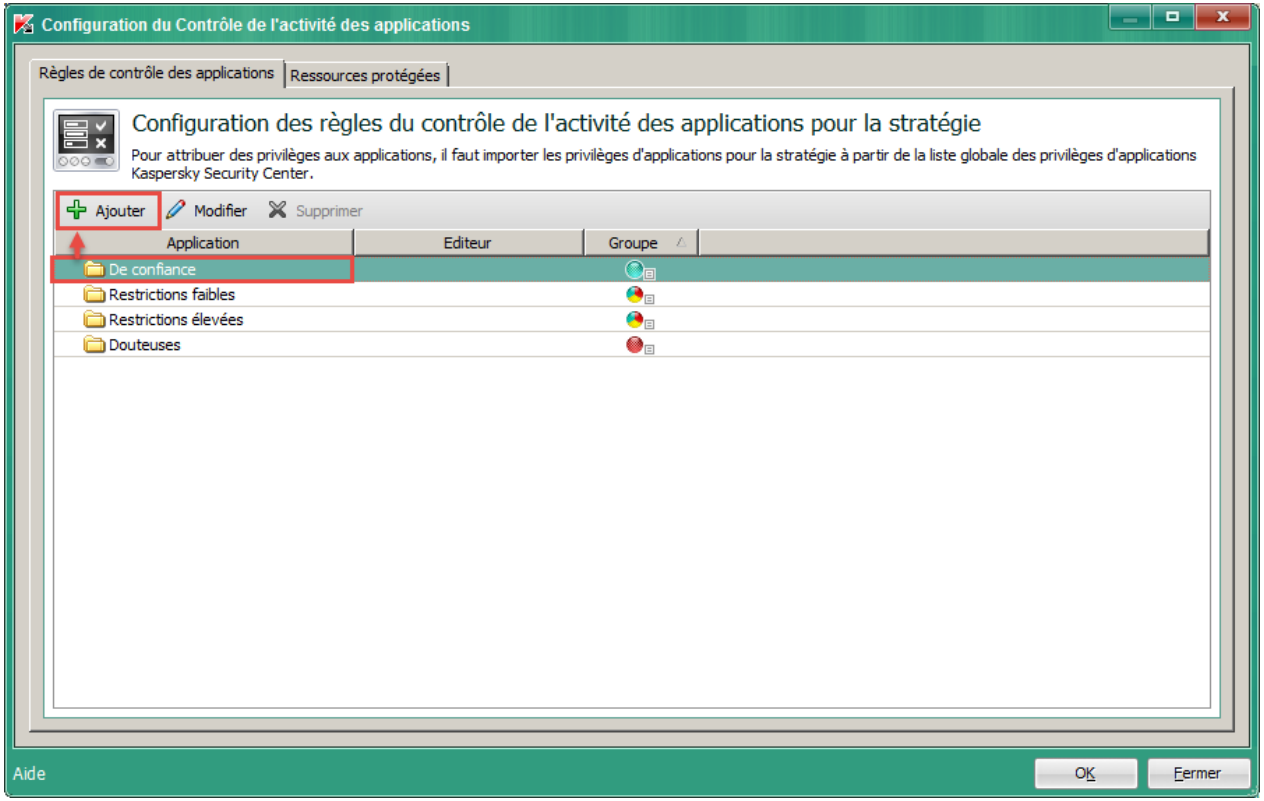
L’administrateur pourra visualiser la même information dans le menu **Rapports et notification**, **Evénements** puis **Evénements d’informations** :



Afin d'affecter le fichier au groupe **De confiance** et lui permettre d'effectuer tous type d'action sur les fichiers protégés, accédez aux propriétés de la stratégie puis rendez-vous dans le menu Contrôle de l'activité des applications et enfin cliquez sur le bouton Configuration… du haut :

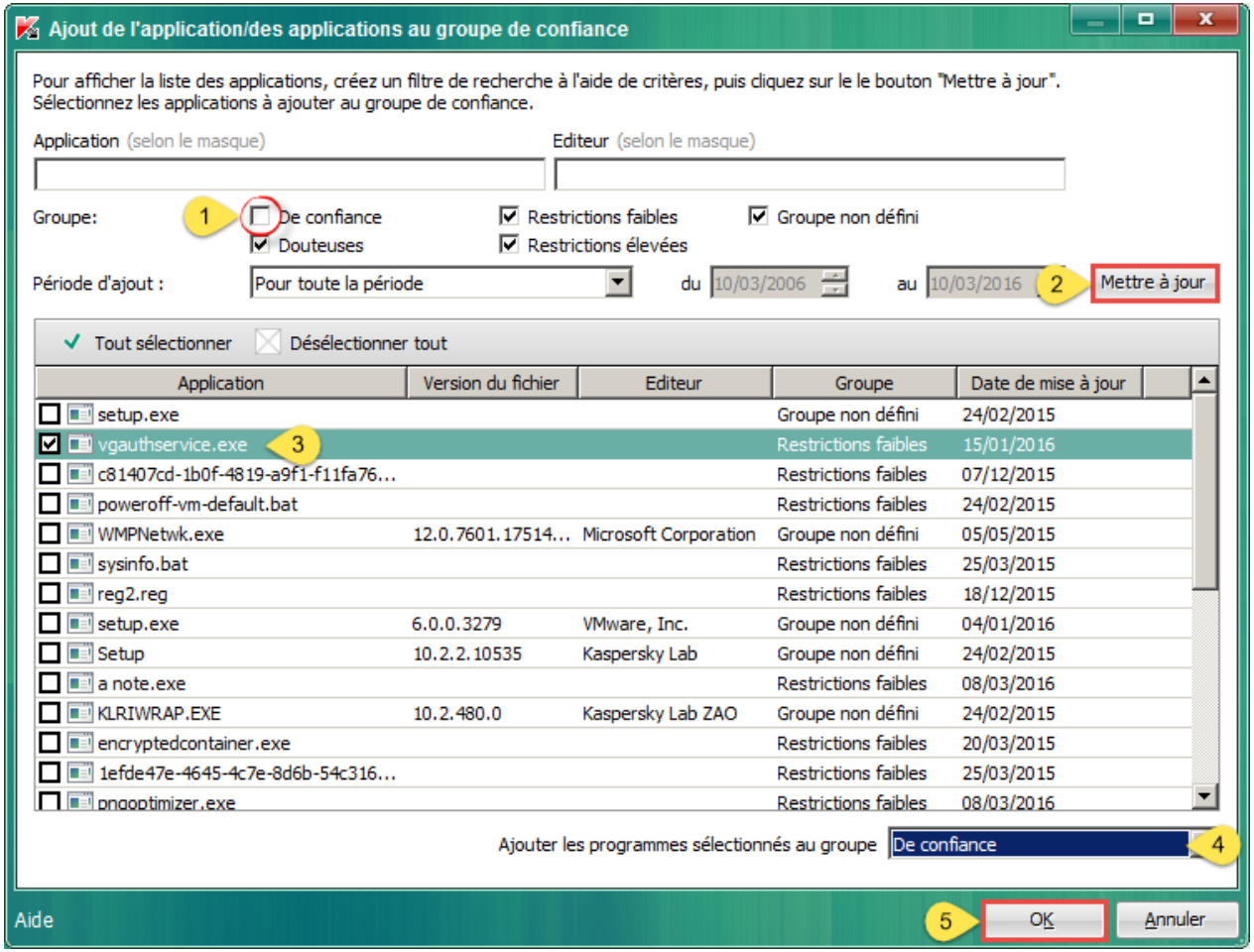


Dans la nouvelle fenêtre apparue, cliquez sur le groupe **De confiance** puis sur le bouton **Ajouter** :



Un moteur de recherche d'applications apparaît, pour visualiser rapidement tous les fichiers qui n'ont pas été ajouté au groupe **De Confiance**, laissez les champs **Application** et **Editeur** vides puis décochez la case **De confiance** (étape n°1) et enfin cliquez sur le bouton **Mettre à jour** (étape n°2).

Parmi la liste des résultats, cochez la ou les applications dont vous souhaitez modifier le groupe d'affectation (étape n°3), assurez-vous que le groupe **De confiance** est bien sélectionné (étape n°4) et cliquez sur le bouton **OK** (étape n°5) :



Une fois la modification effectuée, l’application doit apparaître dans le groupe **De confiance** :

Cliquez sur **OK** pour valider, une fois la stratégie modifiée appliquée sur les machines administrées assurez-vous du bon fonctionnement de l’application concernée.