Possibilités de Security Task Manager

Security Task Manager fournit des informations avancées sur les programmes et processus lancés sur l'ordinateur. Pour chaque processus il affiche des informations supplémentaires qui ne sont pas fournies par le gestionnaire de tâches de Windows:

- Nom et localisation (répertoire) du fichier
- Taux de risques pour la sécurité
- Description
- Date et heure du lancement
- Taux d'utilisation du processeur (CPU)
- Icône du programme
- Fonctions cachées intégrées

(Surveillance des entrées clavier, surveillance du navigateur, manipulations de données)

- Type de processus

(Fenêtre visible, programme dans barre des tâches, DLL, plugins du navigateur, services)

Security Task Manager identifie aussi les pilotes virtuels, services, BHO ou processus cachés du gestionnaire de tâches de Windows.

{button Utilisation de Security Task Manager ,JI(`',`condaypds')}

 Sujets en relation

Utilisation de Security Task Manager

Security Task Manager affiche tous les processus actifs sur l'ordinateur. Le taux de risques vous renseigne sur la dangerosité des fonctions que contient un processus et qui pourraient altérer la sécurité de votre ordinateur. Les processus listés peuvent afficher les propriétés suivantes. Cliquez dans le menu sur **Afficher** afin de choisir quelles propriétés vous souhaiter afficher sous forme de colonnes.

{button ,PI(`',`Name')} Nom
{button ,PI(`',`Bewertung')} Taux
{button ,PI(`',`CPU')} CPU
{button ,PI(`',`mem')} Mémoire
{button ,PI(`',`Datei')} Fichier
{button ,PI(`',`Typ')} Type
{button ,PI(`',`Titel')} Titre et description
{button ,PI(`',`Hersteller')} Fabricant et produit

Clic droit sur un processus pour obtenir un menu contextuel permettant d'obtenir plus d'informations sur ce processus ou le stopper. Possibilités de ce menu:

 Afficher les propriétés
 Terminer un processus
 Placer un processus en quarantaine

Astuce

- Cliquez sur le bouton  **Processus Windows** pour afficher également tous les processus internes de Windows. Ces processus appartiennent au système de Windows. Les processus systèmes de Windows ne sont pas visibles par défaut.

 Sujets en relation

Afficher les détails de processus

Cliquez sur un processus pour obtenir plus d'informations sur celui-ci. Les propriétés suivantes sont affichables:

{button ,PI(`',`Name')} Nom
{button ,PI(`',`Bewertung')} Taux
{button ,PI(`',`Datei')} Fichier
{button ,PI(`',`Typ')} Type
{button ,PI(`',`Titel')} Titre et description
{button ,PI(`',`Hersteller')} Fabricant et produit

Obtenir d'autres informations ou stopper le processus:

 Information provenant d'Internet sur un processus
 Terminer un processus
 Placer un processus en quarantaine

Astuce

- Cliquez sur le bouton **Processus Windows** pour afficher également tous les processus internes de Windows. Ces processus appartiennent au système de Windows. Les processus systèmes de Windows ne sont pas visibles par défaut.
- Cliquez dans le menu sur **Afficher** afin de choisir quelles propriétés vous souhaiter afficher sous forme de colonnes.

Sujets en relation

Apprendre plus sur un processus (recherche Google)

1 Cliquez sur le processus que vous voulez examiner.

2 Cliquez sur le bouton **Google** dans la barre d'outils.

Une page d'information WEB est affichée chez www.neuber.com/taskmanager dans laquelle vous pouvez donner votre opinion sur ce processus ou consulter les commentaires des autres utilisateurs. Vous pouvez rechercher depuis cette page d'autres informations sur ce processus avec Google.com.

Astuce

- Votre navigateur Internet Browser transmet des informations (par ex. Windows utilisé, paramètre de langage). Le programme Security Task Manager ou un de ses composants n'effectue aucune connection à Internet.
- Google.fr est un des moteurs de recherche les plus utilisés et vous donne les meilleurs résultats.

{button ,AL("Prozess")} Sujets en relation

Terminer un processus

1 Cliquez sur le processus que vous voulez supprimer.
2 Cliquez sur bouton **Supprimer**.
3 Choisissez alors une des options suivantes:

Terminer le processus
Placer le processus en quarantaine

Astuce

- Terminer un processus peut engendrer une instabilité du système ou même le bloquer. les logiciels ayant besoins de programmes additionnels de type Adware peuvent ne plus fonctionner. Sauvegardez auparavant vos documents ouverts !

Sujets en relation

Utilisation du répertoire de quarantaine

Le répertoire de quarantaine travaille comme la poubelle de Windows (recycle bin). Lorsque vous placez un fichier en quarantaine, le fichier est renommé et déplacé dans un répertoire isolé. La clé correspondante d'auto-démarrage est effacée (base de registres). Ainsi le processus ne pourra redémarrer.
Une restauration du processus est possible:

Restauration de processus

1 Cliquez sur le bouton **quarantaine** dans la barre d'outils.
2 Dans le répertoire de quarantaine cliquez sur le processus que vous voulez restaurer.
3 Cliquez sur le bouton **Restaurer**.

Sujets en relation

Imprimer la liste des processus

1 Dans le menu Fichier cliquez sur **Imprimer**.
2 Choisissez une imprimante et corrigez éventuellement les propriétés nécessaires (par ex. recto-verso).

Astuce

- Cliquez sur le bouton **Processus Windows** pour afficher également tous les processus internes de Windows. Ces processus appartiennent au système de Windows. Les processus systèmes de Windows ne sont pas visibles par défaut.

Sujets en relation

Exporter la liste des processus

1 Dans le menu Fichier cliquez sur **Exporter sous...**
2 Choisissez le type de fichier:

Fichier texte (*.txt)
Fichier WEB (*.html)

Astuce

- Cliquez sur le bouton **Processus Windows** pour afficher également tous les processus internes de Windows. Ces processus appartiennent au système de Windows. Les processus systèmes de Windows ne sont pas visibles par défaut.
- Sauvegardez régulièrement la liste des processus. Vous trouverez ainsi plus facilement de nouveaux processuses. Une sauvegarde de la liste des processus peut servir à des fins de démonstration.

Sujets en relation

Ecrire un commentaire

Vous pouvez écrire vos propres remarques sur chaque processus. Ce sera visible dans les propriétés du processus. Vous pouvez également ré-évaluer la dangerosité du processus afin de changer la valeur de taux de risques.

Pour écrire un commentaire

1 Clic droit sur le processus concerné.
2 Cliquez sur **Commentaire...** dans le menu contextuel qui apparait ensuite.
3 Entrez votre commentaire et éventuellement votre opinion sur la dangerosité de ce processus. Le taux de risque affiché changera sur la valeur 0 si vous choisissez "Pas dangereux" et sur 100 si vous optez pour "Dangereux". Le choix de "Ne sais pas ou sans opinion" laissera le taux à la valeur existante.

{button ,AL("Shareware")} Sujets en relation

Changer le langage

Security Task Manager reconnait automatiquement la langue utilisée par défaut dans Windows (Français, Anglais, Allemand, ...).

Pour changer de langage:

1. Dans le menu **Afficher** cliquez sur Langage
2. Choisissez ensuite le langage désiré.

Astuce

- Le logiciel peut facilement être transcrit dans une autre langue. Traduisez simplement le fichier lgs_english.txt dans le dossier du programme et envoyez-le à info@neuber.com. Vous recevrez gratuitement un code d'enregistrement en récompense de votre travail.

Sujets en relation

Types de processus

Security Task Manager fait la distinction entre diverses sortes de processus. Cliquez sur **Type** dans le menu **Afficher**, pour afficher ou cacher la/les colonne(s) dans la fenêtre principale.

Les différentes sortes de processus:

Logiciels

Programme
Icône de la barre de tâches

Fichiers DLL

DLL
"ShellExecute"

PlugIns Internet

PlugIns du navigateur

Services et pilotes

Pilote de périphérique
Fichier pilote
Service (processus indépendant)
Service (processus indépendant en interaction avec le bureau)
Service (processus partagé)
Service (processus partagé en interaction avec le bureau)

Cliquez sur une des sortes de processus ci-dessus pour obtenir plus d'informations.

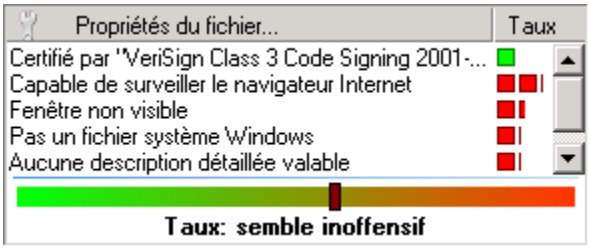
Astuce

- Cliquez sur le bouton **Processus Windows** pour afficher également tous les processus internes de Windows. Ces processus appartiennent au système de Windows. Les processus systèmes de Windows ne sont pas visibles par défaut.

Sujets en relation

Taux de risques des processus

Security Task Manager estime le taux de risques des processus selon des critères objectifs. Pour ceci Security Task Manager examine si un processus contient des appels à une fonction critique ou des propriétés douteuses. En fonction de la dangerosité potentielle de ces fonctions et propriétés douteuses un certain nombre de points est alloué au processus. La somme est affichée dans la colonne Taux de la fenêtre principale de Security Task Manager (de 0 jusqu'à un maximum de 100 points).



Security Task Manager examine les processus pour chercher les fonctionnalités suivantes (dans l'ordre de dangerosité):

{button ,PI(`',`Name')} Capable d'enregistrer les entrées au clavier
{button ,PI(`',`Name')} Fichier caché
{button ,PI(`',`Name')} Pilote de clavier, pouvant enregistrer les entrées
{button ,PI(`',`Name')} Capable de manipuler d'autres programmes
{button ,PI(`',`Name')} Capable de surveiller le navigateur Internet
{button ,PI(`',`Name')} Démarre lors du démarrage de programmes
{button ,PI(`',`')} Ecoute sur le port <N°>
{button ,PI(`',`')} Envoie vers <nom d'ordinateur> sur port <N°>
{button ,PI(`',`')} Programme inconnu qui écoute ou envoie
{button ,PI(`',`Name')} Surveillance du démarrage des programmes
{button ,PI(`',`Name')} Fenêtre non visible
{button ,PI(`',`Name')} Démarre au démarrage de Windows
{button ,PI(`',`Name')} Aucune description détaillée valable
{button ,PI(`',`Name')} Pas un fichier système Windows
{button ,PI(`',`Name')} Aucune description du programme
{button ,PI(`',`')} Fonctions: Internet, moniteur de surveillance, enregistrement d'entrées, caché, manipulateur
{button ,PI(`',`')} Fonctions: indéterminable
{button ,PI(`',`')} Fabricant inconnu

Propriétés partagées (risques réduits):

{button ,PI(`',`')} Fichier signé Microsoft
{button ,PI(`',`')} Fichier certifié Verisign
{button ,PI(`',`')} Certifié par <autorité d'enregistrement> pour la compagnie <fabricant>
{button ,PI(`',`')} Commentaire personnel

Cliquez sur une des propriétés ci-dessus pour obtenir plus d'informations.

Astuce

- Les programmes avec un haut taux de risque ne sont pas forcément dangereux: ils utilisent peut-être seulement une propriété espion (Spyware).
- Cliquez sur le bouton **Processus Windows** pour afficher également tous les processus internes de Windows. Ces processus appartiennent au système de Windows. Les processus systèmes de Windows ne sont pas visibles par défaut.

{button ,PI(`',`Name')} Sujets en relation

Contacter le team de Security Task Manager

Contact technique:

Adresse:	Alexander and Matthias Neuber GbR PF 11 05 25 D-06019 Halle Germany
fax:	(+49) 0700-11 777 000
Internet:	
WWW:	www.neuber.com/taskmanager
email:	info@neuber.com

L'enregistrement est effectué par le service d'enregistrement international ShareIt (Greensburg/U.S.A, Köln/Germany, London/UK, Roissy/France, Upplands Väsby/Sweden).

Vous trouverez une version allemande sous http://www.neuber.com/taskmanager

{button ,AL("Info;Shareware")} Sujets en relation

Désinstallation de Security Task Manager

1 Cliquez sur **Démarrer-Paramètres-Panneau de configuration**.
2 Double-cliquez sur **Ajout/Suppression de programmes**.
4 Cliquez sur **Security Task Manager**.
3 Cliquez sur le bouton **Supprimer** pour désinstaller Security Task Manager de votre ordinateur.

Astuce

- Vous pouvez aussi lancer uninstal.exe dans le répertoire de Security Task Manager.

Effacer les traces de votre activité sur Internet et l'ordinateur

Pour lancer SpyProtector, cliquez sur l'icône dans la barre de tâches.

SpyProtector contient les outils suivants pour protéger votre ordinateur des surveillants d'entrées clavier (keyloggers), logiciels espions (Spyware) et chevaux de Troie (Trojans):

- Effacer les divers historiques
- Désactiver la surveillance du clavier
- Désactiver les autres surveillances
- Mise en garde quand la base de registres est modifiée

{button ,PI(`',`Name')} Sujets en relation

Désactiver la surveillance du clavier

Pour lancer SpyProtector, cliquez sur l'icône dans la barre de tâches.

SpyProtector contient les outils suivants pour protéger votre ordinateur des surveillants d'entrées clavier (keyloggers), logiciels espions (Spyware) et chevaux de Troie (Trojans):

- Effacer les divers historiques
- Désactiver la surveillance du clavier
- Désactiver les autres surveillances
- Mise en garde quand la base de registres est modifiée

{button ,PI(`',`Name')} Sujets en relation

Désactiver les autres surveillances

Pour lancer SpyProtector, cliquez sur l'icône dans la barre de tâches.

SpyProtector contient les outils suivants pour protéger votre ordinateur des surveillants d'entrées clavier (keyloggers), logiciels espions (Spyware) et chevaux de Troie (Trojans):

 Effacer les divers historiques
 Désactiver la surveillance du clavier
 Désactiver les autres surveillances
 Mise en garde quand la base de registres est modifiée

{button ,PI(`',`Name')} Sujets en relation

Mise en garde quand la base de registres est modifiée

Pour lancer SpyProtector, cliquez sur l'icône dans la barre de tâches.

SpyProtector contient les outils suivants pour protéger votre ordinateur des surveillants d'entrées clavier (keyloggers), logiciels espions (Spyware) et chevaux de Troie (Trojans):

- Effacer les divers historiques
- Désactiver la surveillance du clavier
- Désactiver les autres surveillances
- Mise en garde quand la base de registres est modifiée

{button ,PI(`',`Name')} Sujets en relation

Remarques au sujet de la version d'évaluation

Security Task Manager est distribué en tant que Shareware. Le principe du Shareware est une méthode de distribution basée sur l'honneur, et n'est pas un type de logiciel. Vous êtes libres de l'utiliser pour une période d'évaluation de 30 jours.Si vous trouvez ce programme utile et convivial, et que vous décidez de continuer à utiliser Security Task Manager, il vous sera alors demandé de l'enregistrer pour seulement $29 (ou 29 EURO). Vous recevrez alors un code d'enregistrement qui vous permet de libérer le shareware. Le code d'enregistrement supprimera les messages d'avertissement et les limitations du logiciel, et restera valable pour toutes les futures mises à jour.

En tant qu'utilisateur enregistré, vous disposez de:

- Licence légale pour le logiciel
- Votre propre code d'enregistrement vous permettant de libérer la version Shareware
- Mises à jour gratuites à vie
- Utilisation libre du logiciel SpyProtector
  Spyprotector élimine vos traces Internet, vous avertit si des clés de la base de registre (zones de lancement automatique) sont modifiées et désactive les surveillances clavier et souris.
- Support technique libre (via email ou mail)

Cliquez sur **A propos...** dans le menu **Aide** pour vérifier si votre version est enregistrée.

{button ,AL("Team;Shareware")} Sujets en relation

Obtenez Security Task Manager maintenant !

Obtenez aujourd'hui votre propre code d'enregistrement pour seulement **$29** (ou 29 EURO) auprès de notre distributeur ShareIt ! ShareIt accepte les cartes de crédit, les transferts ou virements bancaires, les chèques ou l'argent liquide.

Vous pouvez l'obtenir par:

 Internet: Site d'achat sécurisé
 mail/fax: Bon de commande
 phone: +1-800-903-4152 (achats seulement)
+1-724-850-8186 (support client ShareIt)
+49-221-3108820 (ShareIt Allemagne)
+33-1-491926-54 (ShareIt France)
program ID: 174510

 **Astuces**

- Si vous payez par carte de crédit, vous recevrez votre code d'enregistrement immédiatement. Le code libère le Shareware.
- Si vous avez des questions sur le programme, contactez le développeur.
- Si vous avez des questions sur l'achat lui-même, contactez: ShareIt! Inc., PO Box 844, Greensburg, PA 15601-0844, U.S.A., phone: 724-850-8186, support@shareit.com (ShareIt a des agences aux U.S.A, en Allemagne, en Angleterre, France et Suède)

{button ,AL("Shareware;Team")} Sujets en relation

Comment libérer la version Shareware ?

1 Cliquez sur **Entrer le code d'enregistrement...** dans le menu **ENREGISTREMENT**.
2 Entrez le code d'enregistrement exactement comme vous l'avez reçu dans la boîte de dialogue.
3 Cliquez sur le bouton **Libérer**.

 **Astuces**

- Si vous avez des questions contactez-nous.
- Vous pouvez obtenir votre code d'enregistrement pour $29 (ou 29 Euro).

{button ,AL("Shareware")} Sujets en relation

Validez cette option pour bloquer la plupart des moniteurs d'entrées clavier (keyloggers) pour la session Windows en cours. La redirection de toutes les entrées clavier par un moniteur d'entrées clavier est bloquée. Une telle redirection du clavier est obtenue en programmant une fonction de boucle. Même des utilitaires clavier telle qu'une macro ou un programme inscrivant du texte automatiquement (autotext) n'utilisent pas une telle mauvaise boucle.

Validez une ou plusieurs de ces options pour bloquer les programmes qui surveillent les éléments suivants pour la session Windows en cours:

Entrées de clavier (indirectes)
Cela désactive la surveillance des messages internes Windows messages (par ex. entrées clavier) par d'autres programmes.

Activités de la souris
Cela désactive la surveillance des mouvements et clics de la souris.

Macro
Cela désactive la surveillance des activités de l'utilisateur. Cette méthode est souvent utilisée par les programmes macros mais généralement pas par les moniteurs d'entrées clavier (keyloggers).

Démarrage et fermeture de programmes
Les démarrages et fermetures de programme sont surveillés. Les programmes d'apprentissage (tutoriaux, CBT) utilisent souvent ce genre de surveillance pour interagir avec le programme à apprendre.

Attention: Quelques programmes sérieux (par ex. quelques programmes macro) utilisent cette "mauvaise" fonction de boucle. Si vous constatez qu'un programme ne fonctionne plus, réactivez alors l'option correspondante et redémarrez votre ordinateur.

Validez cette option pour éliminer les traces d'activités Internet (cookies, cache, historique, URLs tapées) dans Internet Explorer. Vous pouvez également effacer la liste des fichiers récemment utilisés (par ex. Word, ACDSee, PDF, WinZip, Mediaplayer) ainsi que la liste des programmes récemment lancés depuis le menu Démarrer.

Validez cette option pour obtenir un message d'avertissement si un programme essaie d'écrire son nom dans la base de registres dans la section démarrage automatique. Le logiciel est démarré secrètement avec une telle entrée à chaque démarrage de Windows. Tous les programmes dangereux ont besoin d'une telle clé pour être actifs lorsque l'ordinateur redémarre !

Security Task Manager

Security Task Manager détecte et supprime les logiciel espion (spyware), les chevaux de Troie (trojans), les espions des entrées clavier (keyloggers) et les logiciels parasites additionnels (adware).

Informations supplémentaires

Enregistrez Security Task Manager SVP. L'enregistrement est facile. Vous pouvez acheter en ligne via Internet, par email, par fax, par téléphone ou par mail ordinaire.

Merci d'avoir choisi d'évaluer Security Task Manager. Vous êtiez libre de l'utiliser pendant une période d'essai de 30 jours. Maintenant cette période est terminée. SVP enregistrez aujourd'hui Security Task Manager pour seulement $29 ou 29 EURO !

Security Task Manager

Security Task Manager n'est pas un logiciel gratuit. Votre période d'évaluation de 30 jours a expiré. Si vous voulez continuer à utiliser Security Task Manager, vous devez l'enregistrer pour $29 (ou 29 Euro).

Pour plus d'informations, cliquez ici.

Version d'évaluation de Security Task Manager

L'analyse de tous les services et pilotes de votre ordinateur est valable dans la version complète.

Comment acheter la version complète

Avec votre enregistrement vous obtenez le libre usage du logiciel supplémentaire SpyProtector. Spyprotector élimine vos traces Internet, vous avertit quand la zone de lancement de la base de registres est modifiée et désactive les surveillances de la souris et du clavier dans votre ordinateur. Toutes les mises à jour sont gratuites à vie. Ce sont de bonnes raisons pour acheter Security Task Manager aujourd'hui.

Bienvenue

Nous vous remercions pour votre enregistrement.

Security Task Manager va vous aider à trouver et supprimerles logiciels indésirables. Tous les messages et limitations du Shareware limitations seront désactivés. SpyProtector est libéré et peut maintenant éliminer vos traces Internet, vous avertir quand la zone de lancement de la base de registres est modifiée et désactiver les surveillances de la souris et du clavier dans votre ordinateur.

Gardez précieusement votre code d'enregistrement. Ce code fonctionnera pour toutes les futures mises à jour.

Si vous avez des questions, contactez-nous

Un processus peut être un programme, un pilote, un service ou un PlugIn - de même que tout code exécutable qui serait actif dans la mémoire de votre ordinateur.

Affiche le nom du logiciel ou du pilote.

Affiche de façon objective le taux de risques du processus. Plus la barre rouge est grande, plus le processus contient des fonctions dangereuses. Les programmes avec un haut taux de risque ne sont pas forcément dangereux: ils utilisent peut-être seulement une propriété espion (Spyware).

Cliquez sur un processus pour en apprendre plus sur lui. Vous pourrez ainsi évaluer la fiabilité de ce logiciel.

Affiche le taux d'utilisation du processeur (CPU). Un programme actif utilise plus de temps processeur qu'un processus inactif.

Affiche l'utilisation de la mémoire vive (RAM).

Affiche le chemin de répertoire et le nom du fichier.

Affiche le type de fichier. Le type de fichier peut être un programme, une icône d'un programme réduit dans la barre de tâches, un PlugIn du navigateur, un pilote ou un service.

Types de processus détectés par Security Task Manager

Affiche le titre et la description du fichier contenus dans le fichier. Pour une fenêtre visible le titre correspond au texte existant dans la barre de titre de la fenêtre.

Affiche le nom du fabricant et la description du produit trouvés dans le fichier.

Programme avec fenêtre visible ou programme invisible sans fenêtre.

Programme avec une icône dans la barre de tâches (à gauche à côté de l'horloge). Un clic droit sur cette icône dans la barre de tâches ouvre un menu contextuel et donne des informations supplémentaires.

Lien de librairie dynamique (Dynamic Link Library / DLL) qui exécute un code de programme comme un autre programme. Un fichier DLL contient rarement une fonction externe utilisée par le programme principal.

Fichier ayant été démarré par une boucle utilisant la commande ShellExecute dans la base de registres Windows. La fonction ShellExecute lance un processus (presque comme une DLL) quand n'importe quel programme Windows est lancé. Ce processus doit être examiné attentivement.

PlugIn de navigateur (Browser Helper Object / BHO): c'est une DLL qui permet aux développeurs de personnaliser et contrôler Internet Explorer. Alexa, GetRight, Go!Zilla et d'autres gestionnaires de téléchargement utilisent un BHO. Les BHOs peuvent surveiller toutes vos activités Internet. Pour désactiver les BHOs, cliquez dans Internet Explorer sur le menu **Outils** puis choisissez **Options Internet**. Cliquez sur l'onglet **Avancés**. Désactivez la case **Activer les extensions tierce partie du navigateur (nécessite un redémarrage)**.

PlugIn de navigateur (Browser Helper Object / BHO): c'est une DLL qui permet aux développeurs de personnaliser et contrôler Internet Explorer. Alexa, GetRight, Go!Zilla et d'autres gestionnaires de téléchargement utilisent un BHO. Les BHOs peuvent surveiller toutes vos activités Internet. Pour désactiver les BHOs, cliquez dans Internet Explorer sur le menu **Outils** puis choisissez **Options Internet**. Cliquez sur l'onglet **Avancés**. Désactivez la case **Activer les extensions tierce partie du navigateur (nécessite un redémarrage)**.

Pilotes et Services exécutant des fonctions système au niveau matériel. (valable seulement dans la version libérée)

Fanion de type de service qui indique qu'il s'agit d'un pilote de périphérique de Windows NT qui contrôle un composant matériel (par ex. une carte graphique ou un scanner). Plusieurs modules logiciels (par ex. Pare-feu, Anti-Virus) ont des pilotes de périphériques que les utilisateurs ne peuvent fermer.

Fanion de type de service qui indique qu'il s'agit d'un fichier de pilote système de Windows NT.

Fanion de type de service qui indique qu'il s'agit d'un service Win32 qui fonctionne dans son propre processus. Un service Win32 démarre automatiquement au démarrage de Windows, est toujours lancé et ne doit pas dépendre des utilisateurs.

Fanion de type de service qui indique un service Win32 (par ex. Pare-Feu, Anti-Virus) qui fonctionne dans son propre processus et peut interagir avec le bureau. Un service Win32 démarre automatiquement au démarrage de Windows, est toujours lancé et ne doit pas dépendre des utilisateurs.

Fanion de type de service qui indique un service Win32 qui partage son processus avec d'autres services. Un service Win32 démarre automatiquement au démarrage de Windows, est toujours lancé et ne doit pas dépendre des utilisateurs.

Fanion de type de service qui indique un service Win32 qui partage son processus avec d'autres services et peut intéragir avec le bureau. Un service Win32 démarre automatiquement au démarrage de Windows, est toujours lancé et ne doit pas dépendre des utilisateurs.

Cette propriété ne parait pas critique. Pour en apprendre plus sur ce processus utilisez la recherche sur Internet.

Le processus surveille chaque entrée au clavier. Ceci est réalisé au moyen d'une fonction de boucle. Les programmes sérieux n'utilisent pas cette fonction de boucle.

Comment empêcher cette surveillance du clavier ?

Le fichier est caché pour l'explorateur Windows. Ne prenez pas un fichier caché (attribut de fichier: caché) comme étant forcément inoffensif !

C'est un pilote de clavier qui peut lire chaque entrée que vous faites au clavier.

Le processus peut manipuler n'importe quel programme ou système Windows. Une boucle est établie pour effectuer ceci. Une boucle est une fonction interne de Windows qui peut simuler, par exemple, une fausse liste de fichiers par manipulation de la commande DIR. Le programme qui démarre le processus est ainsi invisible pour les autres programmes tel qu'un logiciel Anti-Virus.

Le processus peut recevoir des informations depuis Internet. Les pirates informatiques (Hackers) utilisent de telles fuites pour prendre le contrôle de l'ordinateur. Vous pouvez vous protéger de ces attaques par un bon Pare-Feu (Firewall).

Le processus se connecte à un nom d'ordinateur ou à une adresse IP et peut envoyer n'importe quelle information à celui(celle)-ci. Vous pouvez vous protéger de ces attaques par un bon Pare-Feu (Firewall).

Un port est ouvert pour recevoir ou envoyer des informations sur le réseau ou Internet. Recherchez quel est le programme impliqué. Vous pouvez vous protéger de ces attaques par un bon Pare-Feu (Firewall).

Le processus surveille le démarrage et la fermeture des programmes (Qui et quand).

Le programme n'a aucune fenêtre visible et est lancé en tâche de fond. Dans le meilleur des cas, il s'agit, par exemple, d'un logiciel pilote de périphérique.

Le programme est lancé à chaque démarrage de Windows car il écrit une clé dans la base de registres dans la section de démarrage automatique (Autostart).

Mise en garde quand la base de registres est modifiée

Plusieurs descriptions standard importantes n'ont pas été trouvées dans le fichier. Chaque fichier contient par défaut des champs internes pour ces descriptions.

Le fichier ne fait pas partie du système Windows. Les fichiers système Windows sont vérifiés et protégés spécialement par Windows.

Aucune description n'a été trouvée dans le fichier. Chaque fichier contient par défaut des champs internes pour ces descriptions.

Le fichier contient des appels de fonction avec les propriétés nommées. Mais cela n'a pas beaucoup d'influence sur le taux de risques, dans la mesure où il n'est pas évident que cette ou ces fonctions entre(nt) en action.

Aucun appel de fonctions dangereuses n'a été trouvé dans le fichier. Mais elles peuvent avoir été intégrées de façon cachée.

Le fabricant du logiciel n'a pas été trouvé dans les champs de description du fichier. Chaque fichier contient par défaut un champ interne contenant le nom du développeur du logiciel.

Le fichier a été signé par Microsoft. Vous pouvez avoir confiance dans ce fichier comme vous avez confiance dans Microsoft (?!?).

Le fichier a été signé par VeriSign. Vous pouvez avoir confiance dans ce fichier comme vous avez confiance dans VeriSign.

Le fichier a été signé par une autorité d'enregistrement. Vous pouvez avoir confiance dans ce fichier comme vous avez confiance dans cette autorité d'enregistrement et le fabricant du logiciel.

Le processus sera enlevé de la mémoire. Si le processus écrit une clé dans la base de registres dans la section de démarrage automatique (Autostart), il sera alors à nouveau actif au prochain démarrage de Windows.

Le processus sera enlevé de la mémoire. En plus Security Task Manager met le fichier correspondant dans le répertoire de quarantaine et efface les entrées correpondantes dans la base de registres (section de démarrage automatique / Autostart). Le fichier et les entrées de la base de registres sont sauvegardées; vous pouvez ainsi restaurer le processus n'importe quand.

Protegez votre ordinateur avec SpyProtector

Achetez Security Task Manager aujourd'hui et obtenez gratuitement le logiciel SpyProtector. SpyProtector contient les outils suivants pour protéger votre ordinateur des logiciels de surveillance des entrées clavier (Keyloggers), logiciels espions (Spyware) et chevaux de Troie (Trojans):

- Effacer les divers historiques
- Désactiver la surveillance du clavier
- Désactiver la surveillance de la souris
- Désactiver la surveillance d'utilisation de logiciels
- Mise en garde quand la base de registres est modifiée

{button Comment acheter la version complï¿½te ?,JI(`>main',`Ind42dkl0')}

Sujets en relation

SpyProtector peut neutraliser les programmes de surveillance de la souris pour la session Windows courante. La surveillance de vos mouvements et clics de souris par ces programmes est bloquée.

SpyProtector peut neutraliser les programmes qui surveillent les démarrages et fermetures de programme pour la session Windows en cours.

Ajouter un fichier de langage

Vous pouvez télécharger des fichiers additionnels de langage:

1 Allez à http://www.neuber.com/taskmanager/download.html.
2 Vous voyez dans cette page tous les langages existants.
3 Copiez la dernière version dans le répertoire de Security Task Manager. Par exemple c:\program files\Security Task Manager
4 Changez le langage et redémarrez Security Task Manager.

Astuce

- Divers langages sont déjà contenus par défaut dans Security Task Manager.

Sujets en relation

Compra Security Task Manager!

Ordenar hoy su código de registro para **29 EUR**!

You can order by

Internet:	presione la licencia deseada
mail/fax:	Formato de Orden
telefónica:	+49-221-3108820 (sólo ordenes) número: 174510

Notas

- Después de registrarse, Ud. Recibirá por email, fax o correo postal su código de liberación en un lapso de 24 horas. Si Ud. Se registra en línea y paga con tarjeta de crédito, recibirá el registro inmediatamente.
- El código de registro será válido también para todas futuras actualizaciones.

Related Topics

Buy Security Task Manager now !

Order your own registration code for $29 (29 EURO) from our distributor ShareIt today! ShareIt accepts credit cards, bank/wire transfer, checks or cash.

You can order by:

 Internet: Secure Order Form

 Mail/Fax: Order Form

 Phone: +33-1-491926-54 (ShareIt France)
+1-800-903-4152 (orders only)
+1-724-850-8186 (ShareIt customer support)
+49-221-3108820 (ShareIt Germany)

Program ID: 174510

 **Notes**

- If you pay by credit card, you'll receive the registration code immediately. The code unlocks the shareware.
- If you have questions about the program please ask developer.
- If you have questions about ordering please ask: ShareIt! Inc., PO Box 844, Greensburg, PA 15601-0844, U.S.A., phone: 724-850-8186, support@shareit.com (ShareIt has further offices in U.S.A, Germany, UK, France and Sweden)

 Related Topics

Achetez Security Task Manager

Commander votre code d'installation encore aujourd'hui pour **29 EURO** !

Commander simplement par:

Internet: Commande en ligne
Mail/Fax: Bon de commande
Téléphone: +33-1-491926-54 (ShareIt France)
+1-800-903-4152 (achats seulement)
+1-724-850-8186 (Support client ShareIt)
+49-221-3108820 (ShareIt Allemagne)

N° de commande: 174510

Vous recevrez votre code d'installation immédiatement (en cas de commande en ligne avec une carte de crédit) ou dans les 24 heures après réception de votre paiement. Vous transformerez votre particiel en produit complet avec votre code d'installation. Le code d'installation est valable pour toutes les versions de Security Task Manager.

Notre vendeur en France:

element 5 SA / ShareIt! Le Dôme, BP 10910 1, rue de la Hayey 95731 Roissy CDG Cedex Téléphone : +33 (0)1 49 19 26 54 Télécopie : +33 (0)1 49 19 21 00@element5-france.com

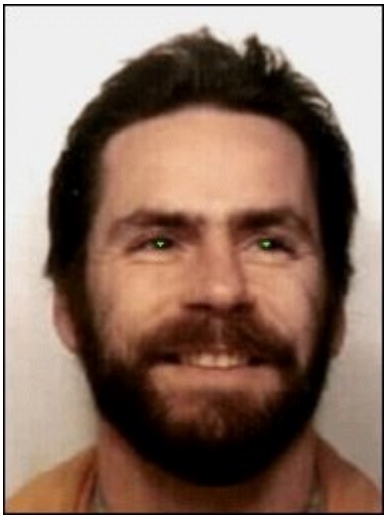
Sujets en relation

Entrez le code d'enregistrement **exactement** tel que vous l'avez reçu. Cliquez alors sur le bouton Libérer pour passer de la version Shareware à la version enregistrée.

Pour plus d'informations cliquez ici.

Le saviez-vous ?

La translation française a été effectuée par Yogi Groumpf en l'an de grasse 2003.



Bonne bourre et bonjour chez vous !