

## Enlever Trojan-Spy.Win32@mx

Et un article que je n'aurais pas aimé écrire. Si vous tombez dessus.

Télécharger SPyHunter puis recherchez les fichier qui merdent et supprimer les des process du gestionnaire des tâches si vous n'arrivez pas à les supprimer !

Voici ma petite emmerde du vendredi soir ! Voici ici comment enlever le trojen-Spy.Win32@mx (source : <http://www.411-spyware.com/fr/enlever-trojan-spy-win32-greenscreen> )

Recommandation:

Pour économiser le temps et pour éviter le risque de nuire votre ordinateur, on recommande emphatiquement utiliser un scanner d'espionnage, comme SpyHunter, pour détecter Trojan-Spy.Win32.GreenScreen et d'autres espionnages, adware, troyens, un virus, enregistreurs de touches (keyloggers), parmi d'autres, qui peuvent être cachés dans votre PC. On recommande aussi que vous sauvegardez votre système avant d'éliminer manuellement.

Scanne Automatique de SpyHunter

Trojan-Spy.Win32.GreenScreen Scanne gratuit.  
Déterminez Automatiquement Trojan-Spy.Win32.GreenScreen et d'autres espionnages dans votre PC avec le Scanne GRATUIT d'espionnage de SpyHunter.

¿Comment enlever des fichiers Trojan-Spy.Win32.GreenScreen ?

Avez-vous besoin d'aide pour supprimer des fichiers, DLLs, et des clés de registre? Bien qu'il y a un certain risque impliqué quand vous enlevez des fichiers, et que par conséquent vous devriez enlever manuellement des fichiers seulement si vous vous sentez confortable et confiant éditant votre système, vous trouverez qu'il est assez facile

de supprimer des fichiers sous Windows.

¿Comment supprimer les fichiers sous Windows XP et Vista?

- Cliquez sur le menu Démarrer de Windows, choisissez &ldquo;Rechercher&rdquo;, cliquez sur &ldquo;Tous les fichiers et Tous les Dossiers&rdquo;.
- Une fenêtre apparaît qui vous demande: &ldquo;Que voulez-vous rechercher?&rdquo;. Cliquez dans &ldquo;Tous les fichiers et tous les dossiers&rdquo;.
- Écrivez le nom du fichier dans la caisse de recherche et sélectionnez les &ldquo;Disques durs locaux&rdquo;.
- Cliquez le bouton &rdquo;Recherche&rdquo;. Une fois que le dossier est trouvé, supprimez-le.

Comment arrêter des processus:

- Cliquez sur le menu Démarrer, choisissez &ldquo;Exécuter> cmd&rdquo;, cliquez sur &ldquo;OK&rdquo; pour exécuter le Gestionnaire de Tâches de Windows.
- Cliquez sur le &ldquo;Nom d&rsquo;Image&rdquo; pour chercher et pour trouver des processus de nom Trojan-Spy.Win32.GreenScreen.
- Dès que vous trouvez le processus de Trojan-Spy.Win32.GreenScreen, cliquez sur &ldquo;Terminer le processus&rdquo; pour terminer le processus de Trojan-Spy.Win32.GreenScreen.

Comment éliminer les clés de registre:

La base de registre est le coeur du système opérationnel Windows, elle contient les données de configuration du système d&rsquo;exploitation, les configurations d&rsquo;usager, des préférences du système, et du logiciel, et inclus aussi les applications qui sont automatiquement exécutées quand le système s&rsquo;initie. Pour cette raison, le spyware, le malware et l&rsquo;adware fréquemment se trouvent dans une forme dissimulée entre vos registres de Windows, et ainsi exécuter lui-même automatiquement chaque fois que vous allumez votre ordinateur.

Comme le registre est une pièce clef de votre système Windows, vous devez toujours sauvegarder les clés de la base de registre avant d&rsquo;introduire des modifications. Si vous n&rsquo;êtes pas un expert, éditer le registre peut vous intimider. Quand vous éliminez ou changez une clé ou une valeur critique du registre, il peut être nécessaire de réinstaller complètement votre système opérationnel Windows. Assurez-vous de sauvegarder la base de registre avant de l&rsquo;éditer.

- Cliquez sur le menu &ldquo;Démarrer,&rdquo; et cliquez &ldquo;Exécuter&rdquo;. Dans la fenêtre tapez &ldquo;regedit&rdquo; et cliquer &ldquo;OK&rdquo;, pour ouvrir l&rsquo;Editeur de registre.
- L&rsquo;Editeur de registre s&rsquo;ouvrira comme fenêtre avec deux panneaux. Le côté gauche vous permet de sélectionner une des clés de registre, et le côté droit montre les valeurs de registre de la clé de registre sélectionnée.

- Pour trouver une clé de registre, n'importe laquelle clé de registre, sélectionnez «Editer», tout de suite sélectionnez «Rechercher», et dans la caisse de recherche écrivez le nom de la clé de registre.

- Dès que vous voyez la clé de registre, vous pouvez la supprimer en cliquant sur le bouton droit de la souris et en choisissant « Modifier » et après «Supprimer».

¿ Est-ce que votre ordinateur se comporte d'une manière rare après avoir édité le registre et après avoir supprimé les clés de registre ? Vous devez tout simplement restaurer votre registre de la copie de sauvegarde.

¿ Comment supprimer des fichiers DLL ?

Comme la plupart des logiciels, le spyware, l'adware, et le malware utilisent aussi des fichiers DLL. DLL est le sigle de «dynamically linked library» (une bibliothèque liée dans une forme dynamique), et les fichiers DLL de Trojan-Spy.Win32.GreenScreen, ainsi comme d'autres DLL, font des tâches prédéterminées. Pour supprimer manuellement les archives DLL Trojan-Spy.Win32.GreenScreen, vous devrez utiliser Regsvr32, un outil de Windows dessiné pour vous aider à supprimer des fichiers DLL et d'autres fichiers.

- D'abord vous devez trouver les fichiers DLL de Trojan-Spy.Win32.GreenScreen que vous voulez supprimer. Cliquez le menu Démarrer de Windows, ensuite cliquez «Exécuter», écrivez «cmd» et cliquez «OK».

- Pour changer le dossier actuel, tapez «cd» dans la ligne de command, après laissez un espace en blanc, et tapez le chemin d'accès complet au dossier où sont placés les fichiers DLL Trojan-Spy.Win32.GreenScreen. Si vous n'êtes pas sûr si les fichiers DLL de Trojan-Spy.Win32.GreenScreen sont placés dans un dossier en particulier, tapez «dir» dans la ligne de commande, et pressez la touche «Enter». Pour aller à un dossier antérieur, tapez «cd ..» dans la ligne de commande et ensuite pressez la touche «Enter».

- Quand vous avez trouvé les fichiers DLL de Trojan-Spy.Win32.GreenScreen que vous voulez supprimer, tapez «regsvr32/u SampleDLLName.dll» (e.g., «regsvr32/u j127script.dll») et après appuyez la touche d'entrée «Enter».

C'est tout. Si vous voulez récupérer les fichiers DLL de Trojan-Spy.Win32.GreenScreen supprimés, tapez «regsvr32 DLLJustDeleted.dll» (e.g., «regsvr32 j127script.dll») dans la ligne de commande, et appuyez la touche «Enter».

¿ Comment est-ce que mon ordinateur s'est infecté avec Trojan-Spy.Win32.GreenScreen ?

Vous vous demanderez comment est-ce que votre ordinateur a été

infecté avec Trojan-Spy.Win32.GreenScreen. En général, si votre ordinateur est infecté par Trojan-Spy.Win32.GreenScreen, malware ou espioniciel, c'est parce que les configurations de sécurité de votre système et de votre navigateur web ont été établis dans un niveau bas, probablement vous n'avez pas suivi de pratiques de navigation web et des habits sûrs avec le courrier électronique, et pour cette raison vous avez besoin d'utiliser régulièrement une bonne application anti-espioniciel. Quelques pratiques incertaines qui peuvent infecter votre ordinateur avec Trojan-Spy.Win32.GreenScreen sont:

#### Graticiel Ou Partagiel:

Avez-vous téléchargé ou avez installé shareware ou freeware ? Les applications de logiciel de prix bas (partagiel) ou gratuites (graticiel) peuvent inclure spyware, adware ou des logiciels comme Trojan-Spy.Win32.GreenScreen. Dans quelques occasions l'adware vient adjoint au logiciel gratuit comme une forme de "paiement" aux développeurs par le prix de création du logiciel, et fréquemment l'espioniciel vient adjoint d'une forme secrète et malicieuse au logiciel gratuit afin de nuire.

#### Un logiciel Point par point (Peer-to-Peer, P2P):

Avez-vous utilisé un programme peer-to-peer ou d'autres applications dans un réseau partagé ? Quand vous utilisez ces applications, votre système cours le risque de télécharger des archives infectées, en incluant des applications comme Trojan-Spy.Win32.GreenScreen.

#### Des sites Web douteux:

Avez-vous visité un site Web de nature douteuse ? Quand vous visitez les sites malicieux qui sont suspects, ils peuvent automatiquement télécharger et installer sur votre ordinateur des troyens, espioniciel et adware, et parfois ils peuvent inclure des applications comme Trojan-Spy.Win32.GreenScreen.

Il est important de pratiquer des habits sûrs quand vous êtes en ligne pour prévenir des infections avec Trojan-Spy.Win32.GreenScreen . Peut-être vous voulez scanner votre ordinateur pour chercher la dernière version de Trojan-Spy.Win32.GreenScreen et d'autres menaces à la sûreté.

Détecter Trojan-Spy.Win32.GreenScreen et d'Autre Malware  
Est-ce que votre ordinateur est infecté avec Malware?

Quand votre ordinateur est infecté avec Malware, tant si c'est espioniciel, adware ou troyens, faux anti-espioniciel, enregistreurs de touches (keyloggers), vers, ou un virus, il y a quelques symptômes que vous expérimenterez dans le système de votre ordinateur. Si vous percevez un ou plus de symptômes mentionnés dessous, peut-être votre PC est infecté par Trojan-Spy.Win32.GreenScreen et d'autres Malware. Continuez à lire, ou cliquez ici pour un scanne gratuit.

#### La performance de l'ordinateur diminue:

Il est suffisant d'avoir un ou deux parasites d'espioniciel pour notablement ralentir votre ordinateur. Si votre PC prend plus longtemps

que l'habituel pour réinitialiser ou si votre connexion internet est exceptionnellement lente, probablement votre ordinateur est infecté de Malware.

Nouveaux raccourcis sur votre bureau ou page d'accueil modifiée: Malware peut changer votre configuration d'Internet ou rediriger votre page d'accueil vers un autre site Web. Malware peut aussi ajouter des nouveaux raccourcis de bureau sur votre ordinateur.

Des ennuyeuses fenêtres Pop-up sur votre ordinateur: Malware peut bombarder votre ordinateur avec les annonces automatiques, même si vous n'êtes pas en ligne. Malware peut enregistrer votre activité régulière sur l'Internet, suivre vos habitudes de navigation et recueillir les informations personnelles au sujet de vous, mettant en danger votre information personnelle et financière.

En comprenant Trojan-Spy.Win32.GreenScreen et Spyware

Si votre ordinateur est infecté par et Spyware, vous aidera de comprendre les définitions de espioiciel rattachées à Trojan-Spy.Win32.GreenScreen

Trojan-Spy.Win32.GreenScreen Peut-être un faux anti-espioiciel  
Quel est faux anti-espioiciel?

Le faux anti-espioiciel - ou le anti-espioiciel suspect - fait allusion au logiciel anti-espioiciel de discutable valeur. Le faux anti-espioiciel ne protège pas votre ordinateur contre espioiciel, il peut déployer de fausses alertes ou créer de faux positifs d'infection dans votre PC, ou il peut utiliser des tactiques pour vous effrayer et vous pousser à l'achat de leur logiciel. Le faux anti - espioiciel peut être installé par un troyen, ou par un autre logiciel, ou peut s'installer lui même par des trous de sûreté des navigateurs web. Bien que ce soit peu commun, certains faux anti-espioiciel sont créés et distribués par des entreprises connues d'espioiciel et adware, et ils peuvent être installés par le propre espioiciel ou adware.

Fréquemment, quand vous êtes infecté par un faux anti-espioiciel vous verrez un faux alerte de sûreté comme cela:

Les tactiques des faux anti-espioiciels

En général, les faux anti-espioiciels ont l'un ou plus de caractéristiques nommées plus bas, raison par laquelle ils sont considérés logiciels anti-espioiciel de douteuse valeur.

» De faux positifs / des alertes fictives:

Il peut produire un grand nombre de faux positifs ou d'alertes non réelles, en vous alertant que votre ordinateur a été infecté par des parasites ou d'autres menaces qui n'existent pas en réalité.

» Il simule être autre:

Il peut copier l'apparence d'autres logiciels anti-espionnage soient ils faux ou non. Fréquemment, le faux logiciel anti-espionnage apparaisse comme clone proche d'un autre faux logiciel anti-espionnage.

» Un marketing Insistant:

Il peut utiliser des tactiques pour provoquer une crainte ou d'autres tactiques d'annonces et de marketing agressif avec le but de vous tromper et de vous pousser à l'achat d'une faux application anti-espionnage. Il peut produire de faux positifs ou alertes fictives sur une infection dans votre ordinateur.

» Une pauvre information de détection/scan:

Quand il scanne votre ordinateur, il peut créer des reports de mauvaise qualité. Par exemple il peut indiquer que votre ordinateur a été par 11 parasites, mais ne pas spécifier quels sont les parasites ou de quel type sont ils. Il peut aussi, faire un report et vous informer que votre ordinateur a été infecté par SafeAndClean, mais ne pas dire quels sont les archives, DLLs, etc., qui ont été trouvés dans votre ordinateur.

» Faible détection et scan du PC:

Le faux anti-espionnage non seulement vous informe pauvrement des infections, aussi il scanne pauvrement votre ordinateur. Il peut omettre des dossiers et fichiers importants qui doivent être scannés pour détecter l'espionnage dans votre ordinateur.

Trojan-Spy.Win32.GreenScreen Peut-être un Troyen

Quel est un Troyen

Les troyens sont un type de virus qui s'installent secrètement sur votre ordinateur, fréquemment quand vous téléchargez un courrier électronique avec un attachement (par exemple .avi, .pif, .exe et même les fichiers.jpg.) . La Plupart de Troyens sont capables, un fois installés, de contrôler complètement votre ordinateur. Dès qu'ils gagnent le contrôle sur votre ordinateur, le troyen et le pirate informatique derrière le virus peuvent changer votre configuration de système, effacer des fichiers importants, voler vos mots de passe et épier l'activité de votre ordinateur.

Certains troyens peuvent également tomber sous la catégorie d'espionnage. L'espionnage est n'importe quel logiciel ou malware (« logiciel malveillant ») employé pour épier ou dépister votre activité sur l'ordinateur. Quelquefois l'espionnage est légitimement et intentionnellement installé par les parents ou par des employeurs pour surveiller l'activité d'Internet sur un ordinateur, mais il peut être aussi installé avec malveillance. Fréquemment l'espionnage peut venir empaqueté avec téléchargements de logiciel gratuit ou venir sous forme de cookie par l'intermédiaire d'un site Web. Ce type

d'espionnage peut détecter votre activité d'Internet ou peut voler des noms de l'utilisateur et des mots de passe de compte secret, des nombres de la carte de crédit, et d'autre information personnelle et financière.

Méthodes de Trojan-Spy.Win32.GreenScreen et d'autres infections troyens

Plusieurs troyens infectent votre ordinateur chaque fois qu'ils vous trompent et vous font exécuter une application infectée. Cette application infectée peut se déguiser sous forme de petit fichier, comme un jpeg ou un attachement d'un e-mail, ou peut être téléchargé sur un site Web ou FTP.

» Courriel électronique:

Votre ordinateur peut être infecté par un troyen quand vous téléchargez un fichier infecté attaché d'un e-mail, ou parfois quand vous simplement ouvrez un courriel électronique. Quelques troyens profitent des trous de sûreté de Microsoft Outlook. Vous pouvez réduire vos chances d'être infecté par un troyen si vous utilisez un logiciel spam-bloquant.

» Sites web: Votre

ordinateur peut être infecté avec un troyen quand vous visitez un site trompeur. Plusieurs troyens exploitent des trous de sécurité dans le navigateur Internet Explorer. Il suffit que vous simplement visitez un site web infecté pour que vous déchargiez un Troyen sans le savoir.

» Ports ouverts : Si

votre ordinateur exécute des programmes avec fonctions pour partager les fichiers - comme AOL Instant Messenger, MSN Messenger, et d'autres, vous pouvez exposer votre ordinateur à des vulnérabilités. Partager les fichiers en utilisant ces applications peut créer un réseau qui permet aux agresseurs l'opportunité d'accéder d'une forme lointaine à votre ordinateur.

peut avoir infecté votre ordinateur par une de ces méthodes. Les Troyens sont un des plus sophistiqué et dangereux type de malware, capable de contrôler votre système. C'est pour cela que le meilleur que vous pouvez faire est éliminer immédiatement les et les Troyens de votre ordinateur.

Posts Liés à Trojan-Spy.Win32.GreenScreen

No related posts

Niveaux de menaces de Trojan-Spy.Win32.GreenScreen

Trojan-Spy.Win32.GreenScreen est une moindre peste

Le parasite n'est pas une menace réelle, mais Trojan-Spy.Win32.GreenScreen peut suivre à la trace vos activités sur l'Internet. Trojan-Spy.Win32.GreenScreen peut être facilement éliminé avec la fonction "Ajout/Suppression" de votre système.

Trojan-Spy.Win32.GreenScreen est une peste

Le parasite peut tracer un profil de vos activités sur le web et il peut s'installer lui même sur votre PC quand vous avez faites un téléchargement. Probablement vous même pouvez éliminer Trojan-Spy.Win32.GreenScreen manuellement.

Trojan-Spy.Win32.GreenScreen est une moindre menace

Le parasite peut tracer un profil de vous et d'autres utilisateurs de votre PC et Trojan-Spy.Win32.GreenScreen peut envoyer cette information vers un serveur parent.

Trojan-Spy.Win32.GreenScreen est une menace moyenne

Le parasite peut tracer un profil de vous et d'autres utilisateurs de votre ordinateur, et Trojan-Spy.Win32.GreenScreen peut envoyer cette information vers un serveur parent. " Trojan-Spy.Win32.GreenScreen peut être très difficile d'éliminer manuellement.

Trojan-Spy.Win32.GreenScreen est une menace

Le parasite peut tracer un profil de vous et d'autres utilisateurs de votre ordinateur, et Trojan-Spy.Win32.GreenScreen peut envoyer cette information vers un serveur parent. Trojan-Spy.Win32.GreenScreen peut télécharger et installer des logiciels malicieux sur votre PC, et cela peut sembler très difficile d'éliminer manuellement Trojan-Spy.Win32.GreenScreen.

Trojan-Spy.Win32.GreenScreen est un moindre danger

Le parasite peut tracer un profil de vous, enregistrer chaque pulsation que vous réalisez sur le clavier, et capturer des images de l'activité de votre ordinateur. Trojan-Spy.Win32.GreenScreen est difficile d'éliminer manuellement.

Trojan-Spy.Win32.GreenScreen est un danger moyen

Le parasite peut tracer un profil de vous, enregistrer chaque pulsation que vous réalisez sur le clavier, et capturer des images de l'activité de votre ordinateur. Trojan-Spy.Win32.GreenScreen peut télécharger d'autres logiciels malveillants (malware) et c'est très difficile d'éliminer manuellement.

Trojan-Spy.Win32.GreenScreen est un danger

Le parasite peut tracer un profil de vous, enregistrer chaque pulsation que vous réalisez sur le clavier, et capturer des images de l'activité de votre ordinateur. Ces données peuvent être envoyées à l'agresseur anonyme et Trojan-Spy.Win32.GreenScreen peut télécharger encore plus logiciels malveillants (malware). Trojan-Spy.Win32.GreenScreen est difficile d'éliminer manuellement.

Trojan-Spy.Win32.GreenScreen est un plus grand danger

Le parasite peut suivre la piste de toute l'activité de votre ordinateur, et Trojan-Spy.Win32.GreenScreen permettre à l'hacker d'accéder à votre PC. Trojan-Spy.Win32.GreenScreen peut canaliser plus de malware vers votre ordinateur et désactiver votre logiciel anti - espioniciel et votre anti-virus. Trojan-Spy.Win32.GreenScreen peut être très difficile d'éliminer manuellement.

Trojan-Spy.Win32.GreenScreen est un danger extrême

Le parasite peut suivre la piste de toute l'activité de votre ordinateur, et Trojan-Spy.Win32.GreenScreen permettre à l'hacker d'accéder à votre ordinateur. Trojan-Spy.Win32.GreenScreen peut canaliser plus de logiciels malveillants (malware) vers votre ordinateur, et désactiver votre logiciel anti - espioniciel ou votre anti-virus et votre pare feu, en plus de bloquer l'accès aux sites anti - espioniciel. Trojan-Spy.Win32.GreenScreen peut être très difficile d'éliminer manuellement.