tutoriel

Logiciel malveillant : " Votre système d'exploitation Windows est endommagé "

Cette arnaque affiche un faux avertissement système, affirmant que le système d'exploitation de la victime a été compromis pour lui faire télécharger un faux logiciel antivirus :

Ce faux pop-up « Votre système d'exploitation Windows est endommagé » vise à effrayer la victime :

- en prétendant que le système d'exploitation en cours d'exécution sur le PC concerné court un risque.
- pour vous faire cliquer sur le bouton Mettre à Jour pour télécharger un pseudo-logiciel de sécurité qui fait plus de mal que de bien.

Symptômes :

- annonces multiples du même caractère
- Ralentissement des performances de l'ordinateur de la victime
- L'onglet contextuel est nommé “Mettez à jour votre Flash Player” pour tromper la victime en lui faisant croire que le pop-up ne fait pas partie de la page Web

??? Comment ai-je “ attrapé ” ce logiciel malveillant ?

Le plus souvent, ce pop-up suspect apparaît sur l'ordinateur depuis un programme indésirable déjà installé.

Ces programmes prétendent être utiles (comme optimiser la vitesse et de la performance ou autre chose) mais ils font plus de mal que de bien et sont souvent glissés dans d'autres programmes gratuits que vous avez téléchargé en ligne (souvent un programme, un pilote, lecteur multimédia et autres logiciels).

Le logiciel indésirable qui affiche le pop-up « Votre système d'exploitation Windows est endommagé » est souvent difficile à détecter car il se cache habituellement au plus profond de la procédure d'installation d'un programme que vous avez volontairement téléchargé et installé. Vérifiez toujours soigneusement ce que vous installez pour éviter que cela ne se reproduise, car les antivirus ne détectent pas toujours ces programmes intrusifs.

Effets et objectifs de ce pop-up

Le logiciel suspect, une fois installé sur votre ordinateur, laisse des fichiers dans plusieurs répertoires Windows, comme **Program Files**.

Il peut aussi créer des tâches planifiées qui s'exécutent automatiquement au démarrage de l'ordinateur.

Son but principal est d'afficher des publicités sur votre ordinateur.

En général, ces programmes potentiellement indésirables modifient fortement les paramètres de votre navigateur pour afficher des annonces, même si vous avez un logiciel de protection comme AdBlock.

Les publicités affichées peuvent varier, mais sont du même type que le pop-up « Votre système d'exploitation Windows est endommagé », qui ressemble à ce qui suit:

Ce message vise à effrayer les utilisateurs inexpérimentés qui croient ce message authentique. L'objectif final est de faire cliquer sur le bouton METTRE À JOUR pour vous faire télécharger ce qui semble être un logiciel de sécurité ou une mise à jour avec des risques différents pour l'ordinateur de la victime, comme :

- Télécharger de faux programmes d'aide dont le but principal est d'afficher de fausses détections de logiciels malveillants pour faire payer les victimes pour une version « licensed » du programme…
- Infecter l'utilisateur avec d'autres logiciels malveillants comme Les chevaux de Troie,

Ransomware et même des virus mineurs de crypto-monnaie.

- vous conduire à d'autres pop-ups de même nature, comme les escroqueries de support technique, par exemple.

???

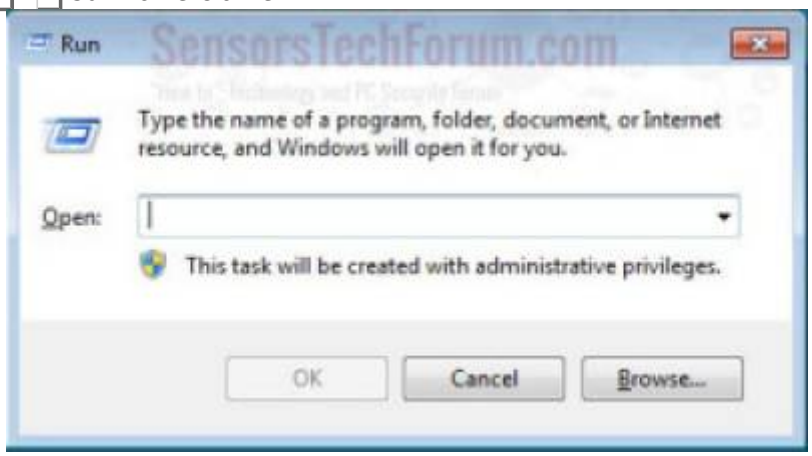
Si vous voyez ce message sur votre navigateur web, supprimez ce logiciel qui affiche des publicités sur votre PC en suivant bien cet article.

Pré-requis

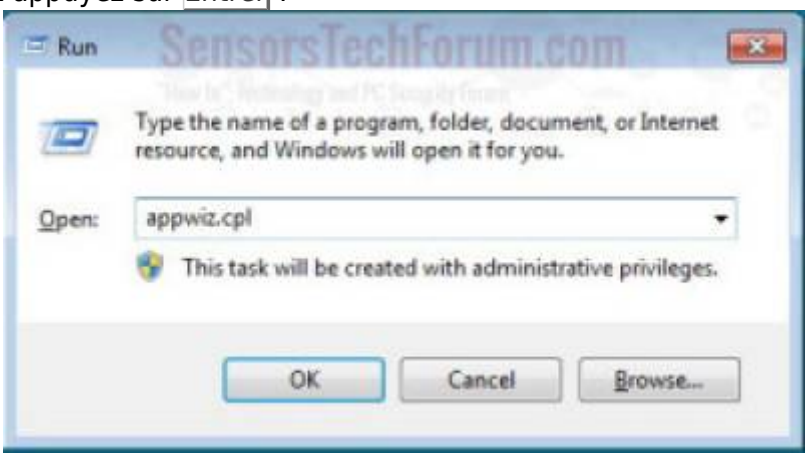
Première étape

Désinstallez le logiciel malveillant :

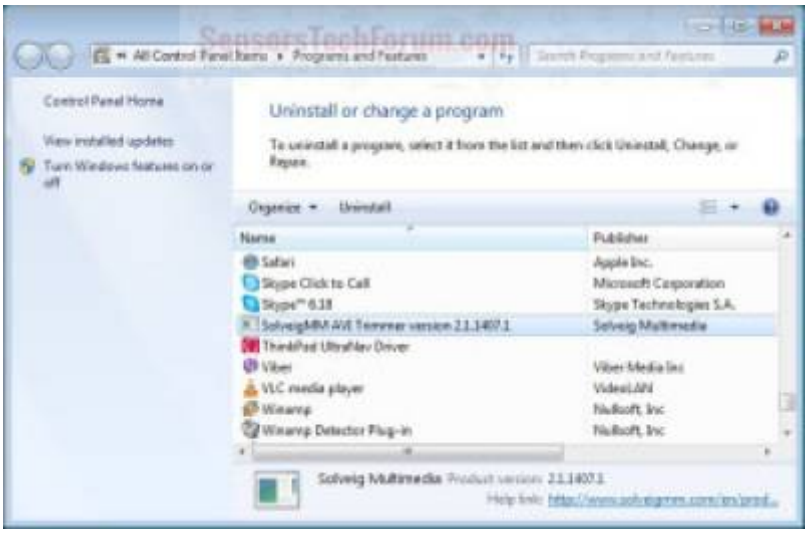
Appuyez sur ⊞ **Win**+**R** sur votre clavier :



Tapez **appwiz.cpl** et appuyez sur Entrer :



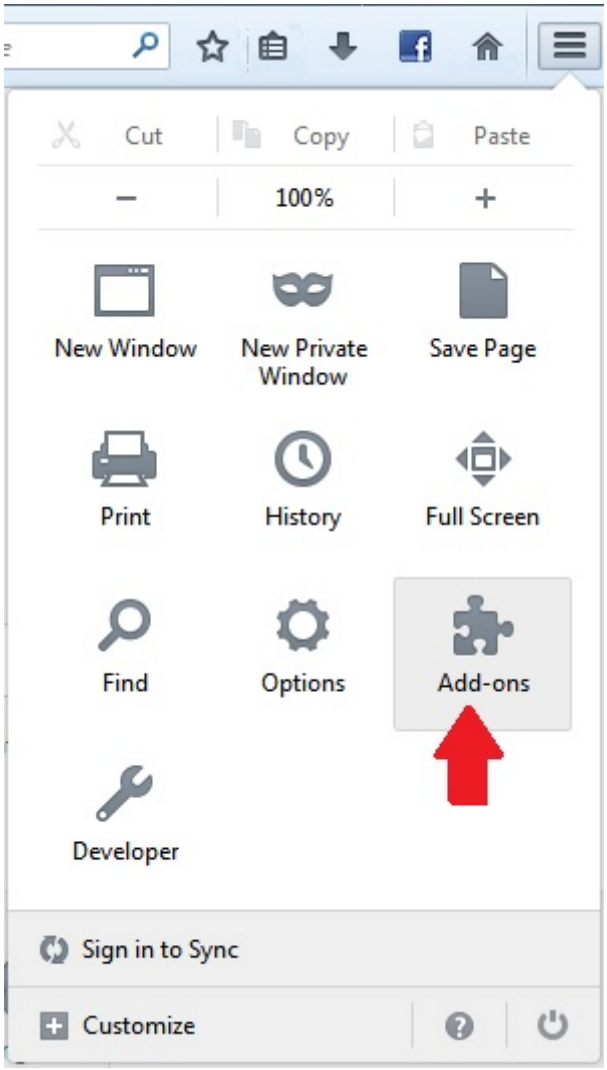
Sélectionnez le programme à supprimer, et appuyez sur **Désinstaller** :



Autres étapes

Retirez le logiciel malveillant de votre navigateur :
Avec Mozilla Firefox :
Dans Mozilla Firefox, ouvrez le menu fenêtre :

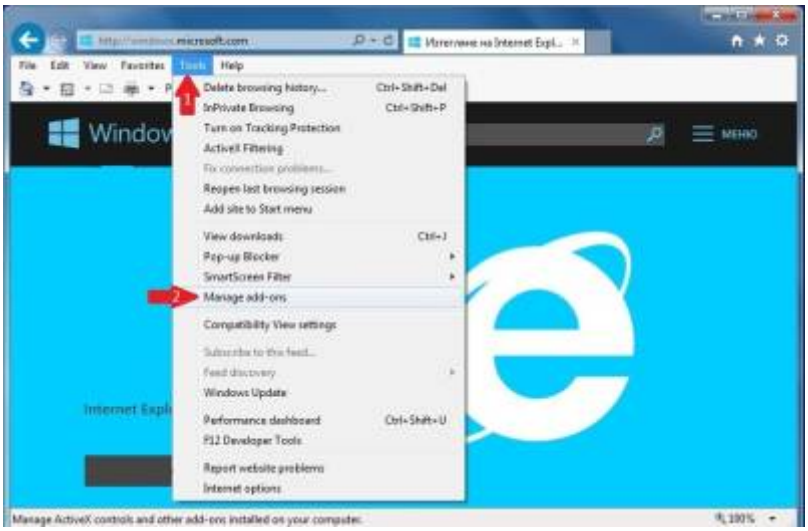
Sélectionnez l'icône **Add-ons** dans le menu :



Sélectionnez le logiciel malveillant (ici « Votre système d'exploitation Windows est endommagé ») et cliquez sur Supprimer

Une fois le logiciel malveillant » retiré, redémarrez Mozilla Firefox par la croix rouge “X” dans le coin en haut à droite et recommencez.

2. **Avec Internet Explorer** :
Dans Internet Explorer, Cliquez sur **Outils → Gérer les modules complémentaires** :



Dans la fenêtre **Add-on Types**, réglez le menu déroulant **Show** à **Tous les add-ons** :

Sélectionnez le logiciel malveillant (ici « Votre système d'exploitation Windows est endommagé » pour l'enlever,

Cliquez sur **Désactiver**.

Une fenêtre vous informe que vous êtes sur le point de désactiver la barre d'outils sélectionnée, et que d'autres barres d'outils peuvent être aussi désactivées. Laissez toutes les cases cochées, et cliquez sur **Désactiver** :

Une fois le logiciel malveillant retiré, redémarrez Internet Explorer en cliquant sur la croix rouge 'X' dans le coin en haut à droite et recommencez.

Conclusion

Problèmes connus

Voir aussi

- **(fr)** http://Article

Basé sur « Article » par Auteur.