Les 10 tactiques les plus communes utilisées par les PUPs. Et comment les éviter.

In by Slade on January 27, 2015 du site http://blog.emsisoft.com

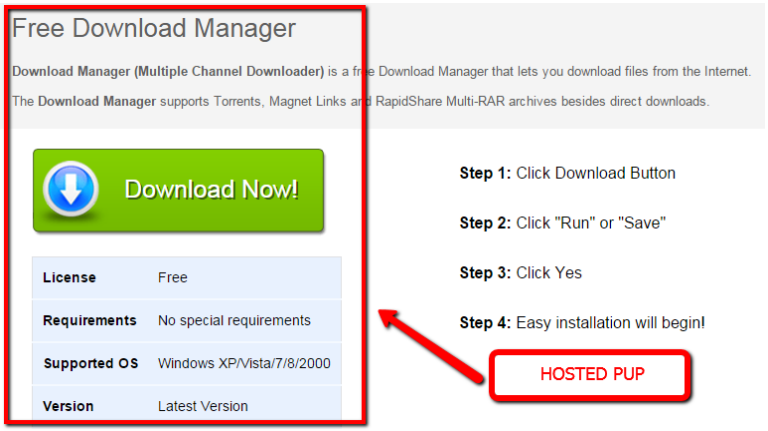
L'autre jour, nous avons parlé de logiciels potentiellement non voulus (PUPs), ce qu'ils sont et comment les fournisseurs de logiciels anti-virus gratuits eux-même vous en donnent. Cet article vous explique en détails la façon dont les PUPs sont livrés. Bien entendu, toute application peut être considérée comme potentiellement non voulue si elle est installée sans que l'utilisateur n'ait donné **« son accord explicite »**.

Cependant, vu les milliers de nouveaux PUPs qui aparaissent chaque jour et la zone floue dans laquelle les PUPs opèrent (entre les logiciels énervants et les vrais malwares), il y a toujours une possibilité que vous soyez confronté à un PUP tôt ou tard. Voici quelques manières par lesquelles ils réussissent à s'incruster :

Exemple 1 : La propagation via les portails de téléchargement

Lors d'une visite de Filehippo.com, un des portails de téléchargement les plus populaires, vous verrez les plus jolis boutons de téléchargement que vous ayez jamais vus. Cependant, tout n'est plus si joli si vous cliquez sur le mauvais bouton. Ci-dessous, le résultat :

Mmmmh…. C'est intéressant, je peux avoir un « Free Download Manager »… Génial ! C'est vraiment gentil de la part de « Filehippo ». Je veux vraiment installer Utorrent… allons-y !"



Un moment – je voulais installer Utorrent, mais cela n'a pas l'air d'Utorrent… Qu'est-ce que j'ai fait de mal ? Ce scénario est une méthode très commune pour mener chaque jour les utilisateurs à télécharger des PUPs. Un portail de téléchargement héberge des gratuiciels. C'est vrai, les logiciels sont « gratuits » (et c'est une bonne chose, non ?). Vous cliquez sur « Télécharger » sans faire attention ou ne remarquez pas la

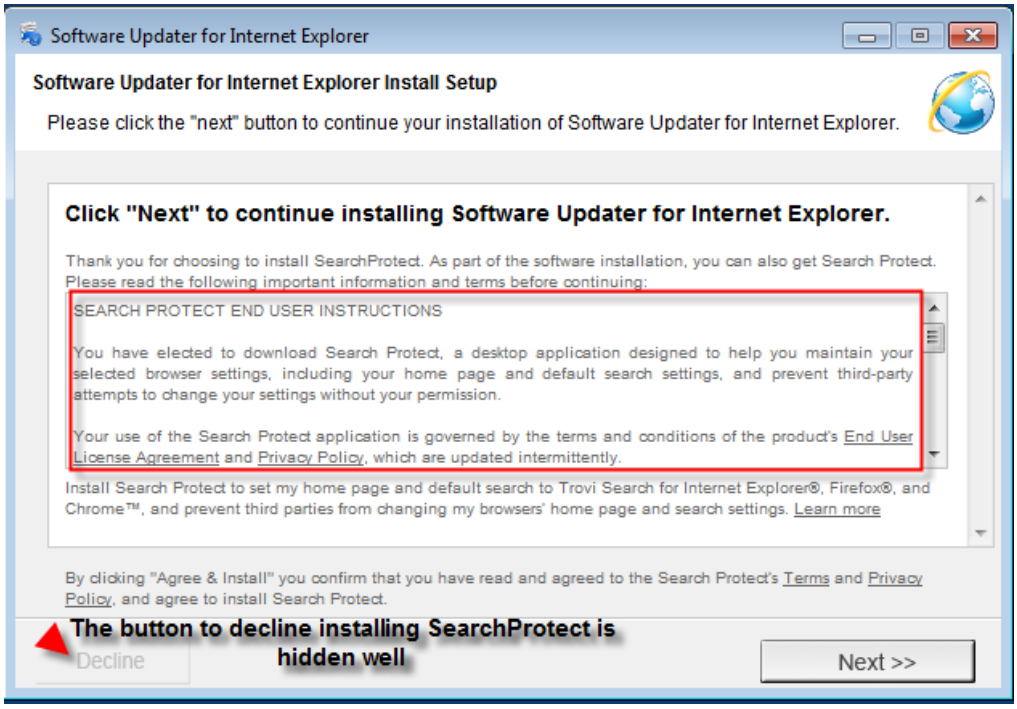
différence entre le téléchargement direct et la deuxième option de téléchargement, apparemment légitime. Félicitations, l'invasion des PUPs vient de commencer ! Mais ne vous en faites pas, il y a une issue de secours.

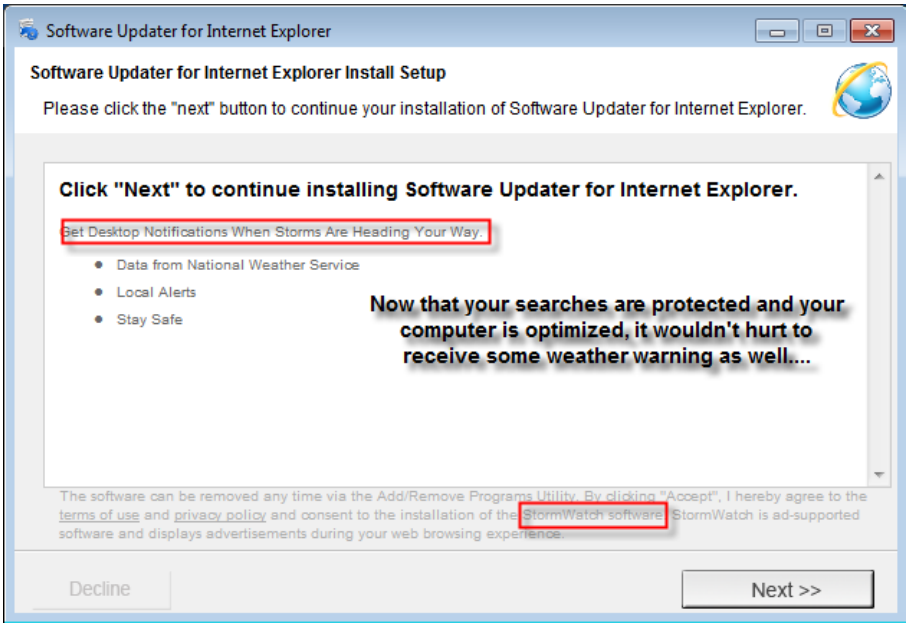
Comment éviter : Le meilleur moyen pour éviter les fraudes par PUPs consiste à éviter les portails de téléchargement. Si jamais vous y allez, soyez très prudent lorsque vous téléchargez des fichiers, veillez à utiliser une solution anti-virus à jour munie d'une protection contre les PUPs activée, contrôlez les noms des fichiers et assurez-vous que c'est vraiment le logiciel que vous désirez. Si celui-ci n'a pas le bon nom de fichier tel que Utorrent, ne l'exécutez pas.

Exemple 2 : Via des fausses mises à jour, souvent proposées par des sites web temporaires

Les mises à jour sont souvent proposées par des sites web temporairement créés, développés pour Adsense, livrant souvent des logiciels au code source ouvert, déguisés en téléchargeurs incitant les utilisateurs à mettre à jour Flash Player, Java, des services packs etc… Il y a des entreprises qui créent des centaines de sites web chaque jour afin de duper les utilisateurs et générer du trafic pour leur site web.

Un exemple : Enfin, ce que tout utilisateur d'Internet Explorer désire depuis bien longtemps, une mise à jour de leur navigateur. Je me demande si cette mise à jour m'apporte la dernière version d'Internet Explorer. Attendez, cela n'a pas vraiment l'air d'un programme de mise à jour. C'est gentil de la part d'Internet Explorer de me proposer Search Protect et d'afficher la météo sur mon bureau. Ouais, cette version mise à jour d'Internet Explorer ne sera pas comme les autres !



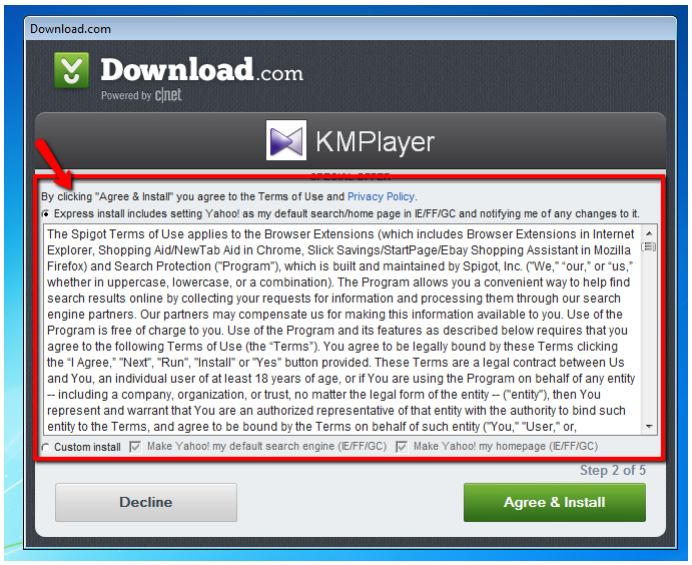


Les deux programmes d'installation proposent de jolies offres aux utilisateurs. Cependant, ces offres sont loin d'être nettes. Une fois installé, Search Protect modifie les paramètres de votre navigateur (moteur de recherche, page d'accueil, paramètres des onglets) et envoie même les données relatives à votre navigation vers des sources inconnues. StormWatch vous impose des pubs pendant la navigation et d'innombrables pop-ups non voulus « sur la météo ». Attention ! De faux programmes de mise à jour sont susceptibles de changer le statut de votre ordinateur en « potentiellement non voulus »!

Comment éviter : Sans aucun doute, personne ne désire recevoir des mises à jour ou prévisions météorologiques de ce programme de mise à jour. Le meilleur moyen pour éviter ce genre de logiciels poubelle consiste à cliquer sur « Refuser » et décocher toute case éventuellement présente. Avant tout : SOYEZ PRUDENT !

Exemple 3 : Programmes d'installation – la propagation par téléchargeurs et CLUFs

Un des logiciels les plus populaires de tous les temps… KMPlayer. Wouah, il y a beaucoup de choses à lire. Je préfère plutôt cliquer sur « Accepter » et « Installer »! BOUM ! Spigot est en train d'installer des extensions dans votre navigateur, Shopping Aid, NewTab, eBay Shopping Assistant et Search Protect. Ce n'est pas tout – votre page d'accueil et moteur de recherche seront désormais Yahoo.

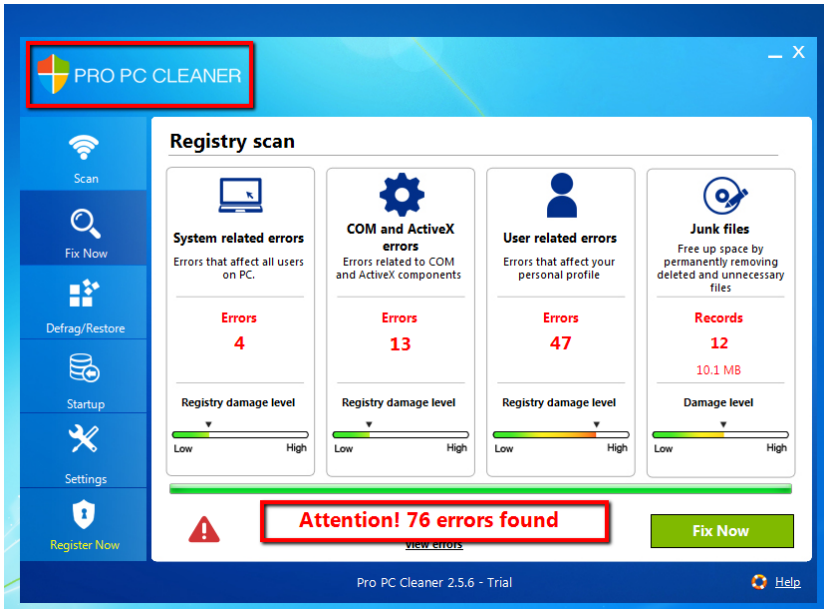


C’est la deuxième vague d’« offres spéciales potentiellement non voulues avant de passer au programme d’installation légitime. Pro PC Cleaner s’installe en toute discrétion sur votre PC et puis vous mitraille de faux résultats qui embêtent d’une manière ou d’une autre. Les offres contenues dans des téléchargeurs (également nommés « wrappers ») provenant de sites web tels que Download.com, Filehippo, Brothersoft et d’autres vous incitent à installer et accepter l’installation de logiciels poubelle. Aucun utilisateur ne veut lire des tonnes de bêtises. Il préfére installer le logiciel désiré.

Comment éviter : Un moyen pour éviter ce genre de logiciels potentiellement non voulus consiste à cliquer sur « Refuser », lire attentivement et ne rien installer sans lire d’abord et à veiller ce qui vient avec. De même, consultez le portail de téléchargement pour trouver des informations relatives au programme d’installation vous expliquant ce qui vient en pack avec le logiciel.

Exemple 4 : des PUPs et encore des PUPS – un PUP installe un autre ?

Selon nos recherches, Pro PC Cleaner est un logiciel potentiellement non voulu très commun, livré en pack avec des gratuiciels sur de nombreux portails de téléchargement. Il faut se demander : est-il vraiment efficace pour nettoyer un PC ? En théorie, ce PUP ressemble beaucoup à une produit falsifié (« rogue »). Voyons donc :

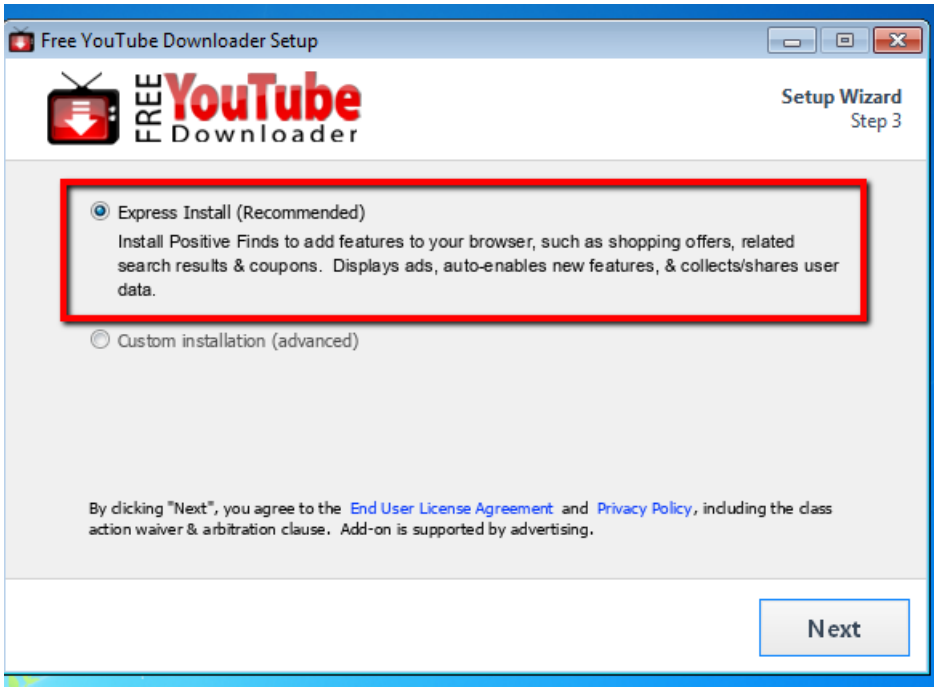


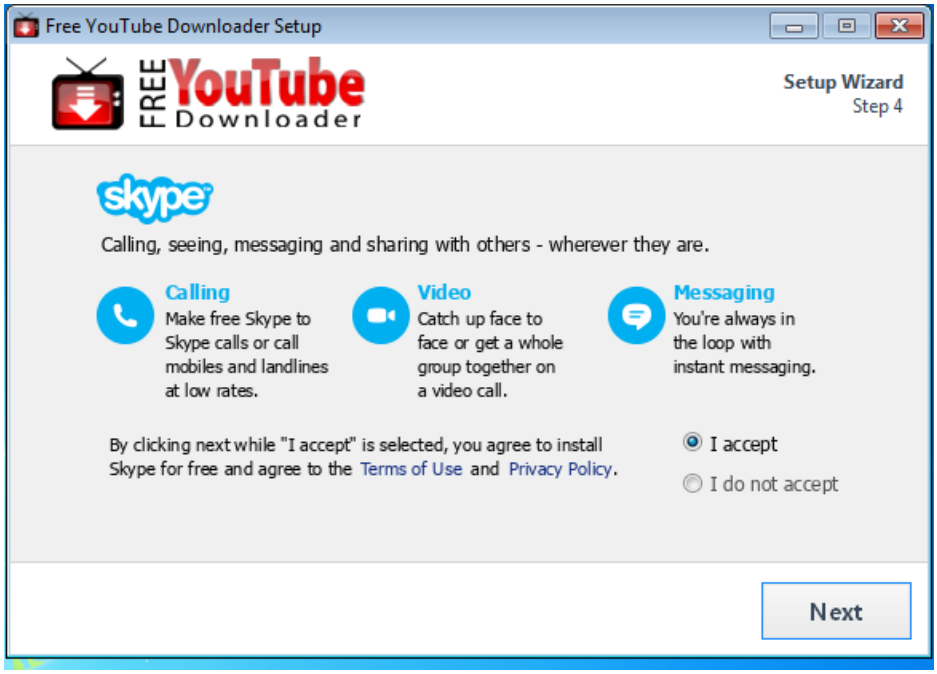
Le PUP ci-dessus a en fait été téléchargé en arrière-plan lorsque vous acceptez les conditions du CLUF du téléchargeur proposé par Download.com pour KMPlayer. C’est un scénario vraiment inquiétant, mais tout à fait réel. Un logiciel potentiellement non voulu en télécharge un autre. Pro PC Cleaner tente d’inciter l’utilisateur à acheter la version payante (ce qui le fait ressembler énormément à un rogue). Il suffit d’installer une fois depuis Download.com, et voilà, vous aurez des PUPs s’affichant partout.

Comment éviter : Soyez vigilant, fiez-vous à votre bon sens et lisez attentivement TOUT avant de passer à l’installation. Comme précédemment dit, veuillez garder votre solution anti-virus à jour et activer sa détection de PUPs.

Exemple 5 : Installation express = infection express ?

Dans cet exemple, nous utilisons Free YouTube Downloader, une application gratuite très populaire sur CNET.com, vous permettant de télécharger des vidéos sur YouTube. Cependant, je parie que CNET ne vous informe pas des offres potentiellement non voulues comprises. Voyons donc :



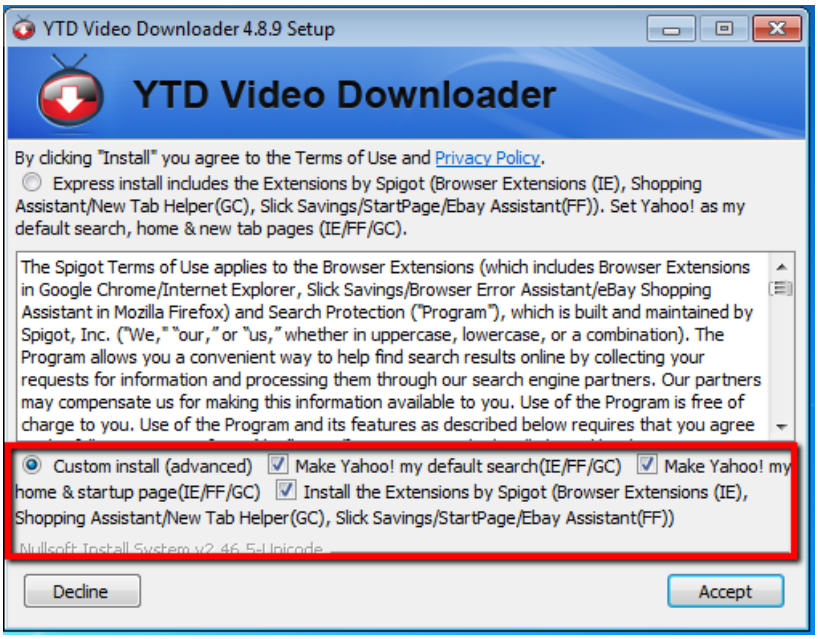


Voilà ! L'installation express n'est pas toujours la meilleure façon. Oui, lors d'une installation express, il suffit de quelques clics, et voilà, c'est fini. Pourtant, vaut-elle vraiment le risque d'installer des logiciels potentiellement non voulus ? Skype est une application légitime, qui peut s'avérer non désirable pour tous ceux qui n'en ont pas besoin. L'installation express apporte des logiciels potentiellement non voulus dans votre navigateur, affichant des pubs et collectant/partageant vos données. Cela ne semble pas sympa.

Comment éviter : Ne jamais opter pour l'installation express ou recommandée car celle-ci l'est en tenant compte des intérêts de son créateur, et non des vôtres.

Exemple 6 : Installation personnalisée – meilleure qu'une installation express ?

YTD Video Downloader est une autre application gratuite populaire. Voyons donc si ses options d'installation vous apportent moins de PUPs lors d'une installation personnalisée que Free YouTube Downloader. L'installation personnalisée fera-t-elle une différence ? Voyons cela :

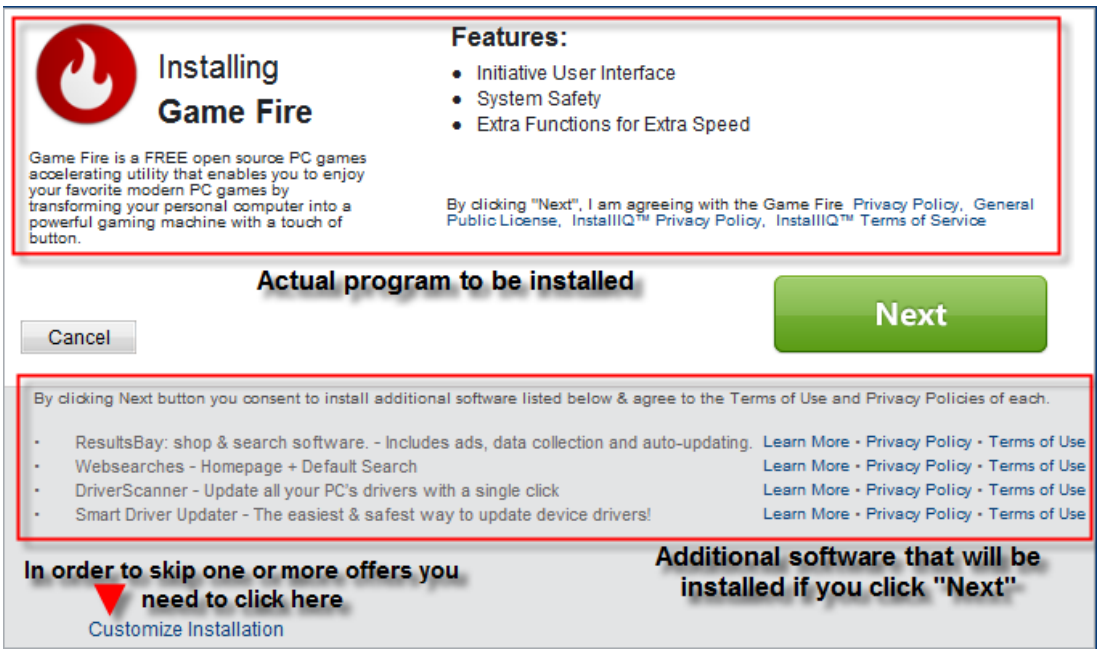


Il ne faut pas être une lumière pour voir qu'une installation personnalisée propose également des logiciels potentiellement non voulus. Cependant, il y a une différence notable entre l'installation express et l'installation personnalisée : une installation express ne vous laisse pas le choix de modifier l'installation tandis qu'une installation personnalisée vous permet au moins de choisir exactement ce qui sera installé sur votre système. Il est facile de décocher toutes les offres non voulues si vous êtes prudent et n'optez pas pour l'installation express.

Comment éviter : Appuyez-vous sur les mêmes tactiques déjà mentionnées et optez pour une installation personnalisée. Comme dit auparavant, une installation personnalisée est à conseiller vu que vous gardez le contrôle sur ce qui est installé sur votre système. Veuillez donc, si possible, toujours choisir l'installation personnalisée.

Exemple 7 : Nouvelle page d'accueil, nouveau moteur de recherche et pilotes mis à jour

Normalement, la capacité de modifier la page d'accueil et le moteur de recherche est une bonne chose. Cependant, les logiciels potentiellement non voulus s'appuient sur cette méthode pour modifier votre page d'accueil, moteur de recherche et même les paramètres des onglets. Même les installations personnalisées ne sont pas immunisées contre les fraudes vicieuses des PUPs.

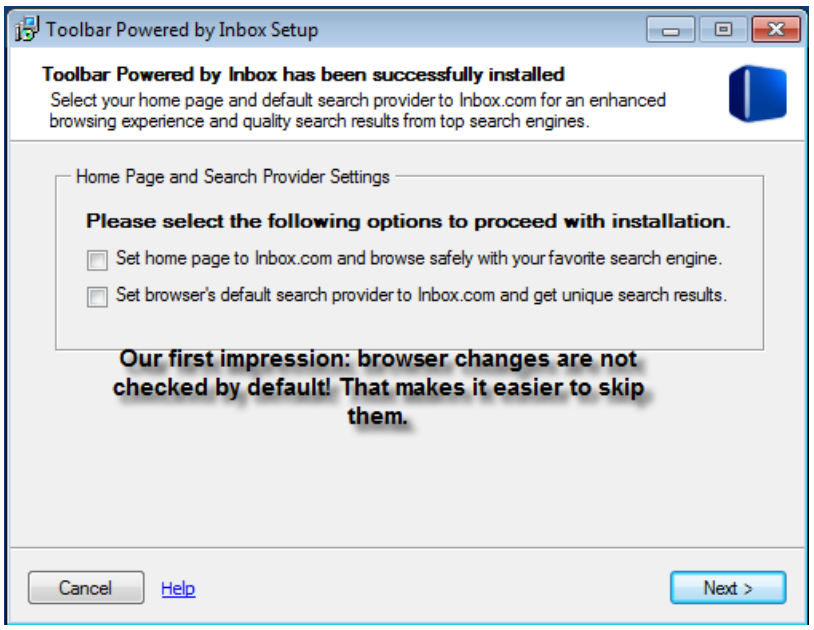


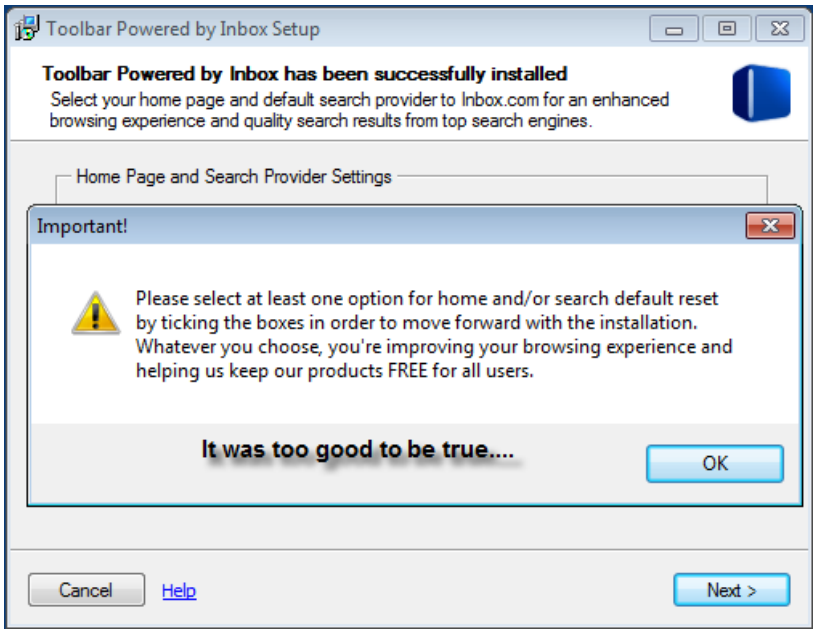
Comme vous voyez dans la capture d'écran ci-dessus, plusieurs offres potentiellement non voulues vous sont proposées. L'image montre : Game Fire, ResultsBay, WebSearches, Driver Scanner et Smart Driver Updater, tous issus d'une seule et même installation. Wouah ! C'est impressionnant ! Les PUPs prennent le dessus sur les programmes d'installation. Procédez avec prudence ! Les installations personnalisées ne sont pas aussi « sûres » que certains pensent.

Comment éviter : Il est essentiel de pouvoir éviter ce genre d'offres. Veillez à décocher toute case qui semble installer des logiciels poubelle. Vous devez même annuler l'installation de certains programmes pour annuler l'installation de PUPs. Veuillez noter encore une fois qu'il vaut mieux être très prudent et tout lire attentivement avant de passer à l'installation.

Exemple 8 : Propagation par force – la méthode presque dépourvue d'issue de secours

Ce que font ces logiciels potentiellement non voulus, ce n'est pas rigolo du tout. En résumé, Inbox Toolbar tente de s'installer en PUP typique, tout en faisant de sales coups. Lors de l'installation d'Inbox Toolbar, vous êtes forcé de modifier votre page d'accueil ou moteur de recherche avant d'installer le logiciel. La meilleure idée ? Envoyer cette barre d'outils directement dans la corbeille !





Ne désespérez pas, il y a de l'espoir ! Cela semble assez sombre et lugubre. Il est possible de sauter les offres potentiellement non voulues mentionnées ci-dessus. Ce PUP tentait, avec toute finesse, de pousser l'utilisateur à modifier les paramètres de son navigateur. Il conviendrait de manier ce genre de PUP avec beaucoup de prudence sans continuer l'installation.

Comment éviter : Cette offre est plus difficile à éviter que les autres, mais il est possible d'opter contre l'installation.

Exemple 9 : Quelqu'un d'autre utilise votre ordinateur

Vous partagez votre ordinateur avec vos enfants, collègues ou partenaire. Il se peut que ceux-ci ne soient pas aussi prudents que vous et laissent des PUP s'installer sur votre ordinateur. Et cela surtout lorsqu'ils consultent des sites web torrent, streaming ou dédiés aux jeux en ligne qui ont l'habitude de vous mitrailler de téléchargements et pubs.

 **Comment éviter :** Le seul moyen pour les éviter consiste à ne pas partager votre ordinateur.

Exemple 10 : Votre patron vous charge de faire des recherches sur les PUPs ;)

Même si vous êtes comme moi et faites attention à ce que vous installez, cela peut être difficile. Certains créateurs de PUPs s'efforcent de contourner les programmes anti-virus et désinstalleurs, parfois en une seule ligne de code. Certains PUPs sont vraiment difficiles à détecter même pour un utilisateur averti, sans parler de l'utilisateur lambda.

 **Comment éviter :** Appuyez-vous sur une machine virtuelle et/ou faites un snapshot pour restaurer votre système au cas où, avant de lancer vos recherches. Cela peut sembler un peu exagéré, mais représente une manière facile pour ne pas avoir à s'inquiéter pour la santé de votre système – même s'il ne s'agit que de l'ordinateur sur votre poste de travail.

Faits importants à se rappeler pour éviter les PUPs

En fin de compte, nous finissons tôt ou tard par être victimes d'un logiciel potentiellement non voulu. Le secteur devrait tenir à changer ses manières et se défendre contre les PUPs de sorte qu'il n'y ait que l'option de refuser ou que les logiciels anti-virus réussissent à les bloquer tous. Les faits importants à garder en tête pour éviter les PUPs sont comme suit :

- Soyez prudent, fiez-vous à votre bon sens et prenez votre temps.
- Installez, mettez à jour et fiez-vous à un logiciel anti-virus de bonne renommée, tel qu'Emsisoft Anti-Malware, vous proposant la protection en temps réel contre les PUPs.
- Ne vous appuyez que sur les sources de téléchargement fiables.
- **NE JAMAIS** télécharger ou installer des applications qui vous semblent suspectes ou malveillantes.
- Optez toujours pour l'option d'installation personnalisée si possible.
- Cherchez les boutons « Refuser »/« Sauter », pourvus d'habitude, d'une police et de couleurs peu visibles en comparaison avec les boutons « Suivant » bien visibles.
- Analysez et débarrassez votre PC de PUPs régulièrement à l'aide d'Emsisoft Emergency Kit gratuitement.

Passez une excellente journée (sans PUPs) !