Corriger la lenteur au démarrage d'un PC avec CCE

« *[Fix pfSense] Unable to check for updates*
(modifié le 7 août 2013 à 17:33)

Comodo Cleaning Essentials (CCE) est un **puissant outil** que j'utilise très fréquemment sur des machines infestées par un malware, virus, toolbar ou autre joyeuseté. L'outil est gratuit et proposé par l'éditeur antivirus Comodo (vous l'auriez deviné). Il permet d'identifier les programmes, services et processus à l'origine des **lenteurs au démarrage** d'un PC (avec **autoruns**).

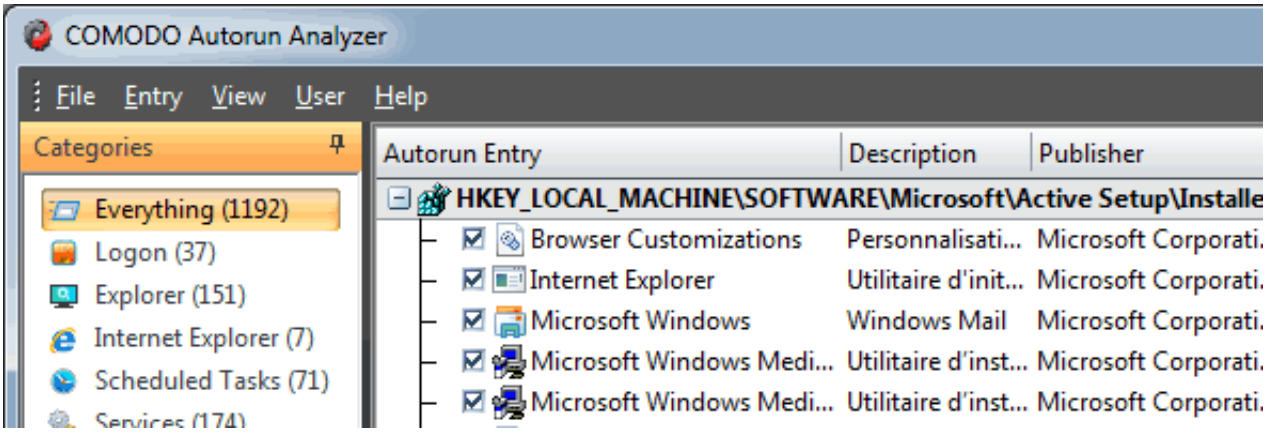
Aucune installation n'est nécessaire, il suffit de lancer les binaires qui sont donc portables. Je vous conseille de copier CCE **sur un disque dur ou clé USB** que vous utilisez déjà comme trousse à outils de dépannage.

Comodo Cleaning Essentials est composé de trois outils qui peuvent fonctionner de façon indépendante.

Autorun Analyzer

Autorun Analyzer analyse **tout ce qui se lance avec Windows** (comme CodeStuff Starter et SysInternal AutoRuns) mais il va plus loin en allant chercher quelques clés de registre bien spécifiques.

C'est un logiciel gratuit **très efficace** qui permet de faire un **état des lieux très rapide sur une machine infectée**. Le menu "User" permet de voir les clés programmes et processus de lancement pour l'utilisateur courant mais également pour les utilisateurs systèmes "autorite NT système / service local / service réseau".

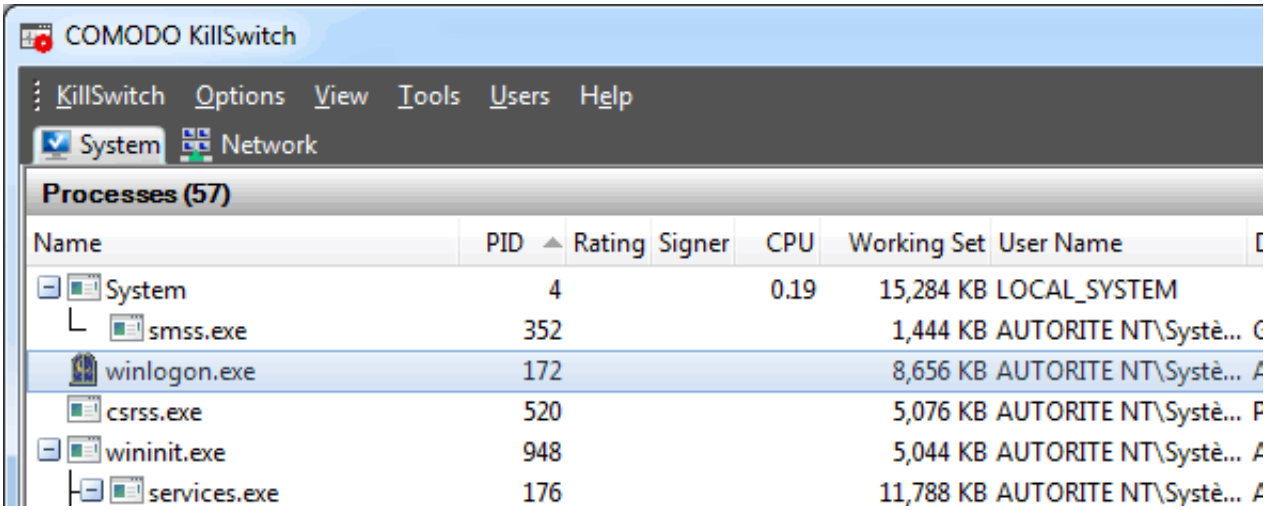


Des codecs aux drivers en passant par les DLL, Winlogon, les services où les tâches, tout y est. Un clic droit "jump to entry" permet de lancer Regedit et de localiser la clé concernée.

S'il ne fallait garder qu'un seul outil dans CCE, ce serait celui-là. **Je n'ai jamais trouvé d'équivalent, c'est un must-have.**

KillSwitch

KillSwitch un **gestionnaire de processus et de flux réseaux**, une sorte de mélange entre les populaires *Process Explorer* et *TcpView*.



L'onglet "Network" s'avère très utile si un **botnet tourne sur votre machine**, ou un processus de fond qui communique avec un serveur sans raison. Car... oui ce genre de comportement arrive aussi avec des logiciels tout à fait légaux, et si vous n'avez pas un pare-feu sortant restrictif vous ne verrez jamais ces flux, d'où l'intérêt de KillSwitch pour préserver votre vie privée.

J'apprécie particulièrement le clic droit "Jump to folder" pour localiser le binaire qui est à l'origine d'un flux réseau.

Ne pas hésite à fouiller dans les options qui sont nombreuses. Vous pouvez faire de

KillSwitch votre gestionnaire de tâches par défaut, en lieu et place de celui de Windows.

Comodo Cleaning Essentials

Enfin, le dernier outil est un antimalware. 3 scans sont possibles : rapide, complet et à la demande. Il vous proposera les dernières mises à jour de sa base si vous êtes connectés à internet.

Je l'ai rarement utilisé car *MalwareBytes Antimalware* (dans sa version gratuite) suffit à venir à bout des véroles dans **99% des cas**. De plus j'ai constaté que de nombreux faux positifs (logiciel de gestion de ma carte mère Asus par exemple) étaient détectés.

Conclusion

Vous l'aurez compris, cette suite permet d'**analyser une machine en profondeur** mais nécessite de solides connaissances pour pouvoir être exploitée à 100%.

A ne pas mettre entre toutes les mains, et avant toute modification pensez à faire une sauvegarde de votre machine avec Acronis ou à minima un point de restauration Windows.

Télécharger CCE (32 et 64 bit)

[Android] Réveillez votre ordinateur à distance »