JTW10

INFO-AIVM37

Divers Sécurité

MAJ le 16/02/2021

Il est important de voir aussi la fiche logiciels pour ceux concernant la sécurité :
http://aivm37.free.fr/BI/JT/JT078_Logiciels.pdf

Voir le sommaire page suivante.

Sommaire

1 Sécurité
1.1 Support de restauration
1.2 Restauration de Windows 10
1.3 Sécurité logiciel
1.3.1 Sauvegarder les clés de mes logiciels avant un problème
1.3.2 Sauvegarde non programmée
1.3.3 Fenêtre de sécurité UAC
1.4 Niveau de sécurité utilisateur
1.5 SmartScreen
1.6 Virus
1.6.1 Télécharger un Setup. Prudence
1.6.2 Les mises en garde de Microsoft
1.6.3 Les produits Piriform.
1.7 Phishing. Protection sites bancaires
1.8 Ransomware
1.8.1 Danger
1.8.2 Ce qu'il faut faire absolument et régulièrement.
1.8.3 Il m'arrive un truc bizarre sur mon PC. Qu'est-ce que je fais ?
1.9 Comment lutter contre le ransomware,
1.9.1 Si votre disque est partitionné
1.9.2 Votre disque n'est pas partitionné.
1.9.3 Je n'ai pas de sauvegarde sur disque dur externe
1.9.4 Voici un exemple d'hoax, envoyé par Colette
1.9.5 CCleaner et Avast
1.9.6 Webcam
1.10 Windows Defender
1.11 Pare-feu de Windows
2 Antivirus
2.1 McAfee
2.2 Antivirus à retirer
2.2.1 McAfee
2.3 Malwarebyte
2.3.1 Avast non sollicité.
2.4 Confusion entre maintenance et sécurité
2.5 Meltdown et Spectre
2.6 Les sites pas toujours net sur Internet

3 Arnaques

1 Sécurité

1.1 Support de restauration

Question

Comment créer un support de restauration depuis un HP neuf sous Windows 10 ?

Réponse

Vous pouvez (vous devez) avec tous les HP neufs, créer un support de « recovery » soit sur une clé USB de 16 Go soit sur 3 DVD. Cela vous permettra en cas de problème de retrouver votre PC HP comme neuf en bootant depuis le support que vous allez créer.

Dans la zone de recherche tapez « Recovery », Hp va vous proposer son logiciel Recovery Manager. Vous trouverez la démarche à suivre pour continuer dans ce « manager ».

1.2 Restauration de Windows 10

Question

Est-il possible de créer une clé de restauration de Windows 10 ?

Réponse

Voici une méthode propose par Microsoft, mais attention, c'est la solution proposée au moment du_ lancement de l'opération Windiows 10 . Je ne sais pas si une clé du logiciel Windows 10 vous sera demandée au moment de la réinstallation. Cette méthode est décrite ici

http://facilepc.fr/newsletter-11-02-2017.html

1.3 Sécurité logiciel

1.3.1 Sauvegarder les clés de mes logiciels avant un problème

Question

Comment sauvegarder les caractéristiques (les clés) de mon PC et des logiciels ?

Réponse

Utilisez le logiciel Belarc Advisor et sauvegardez la page html qu'il vous propose en fin d analyse et mettez la de côté sur une clé USB, elle contient toutes les clés de Windows et des logiciels. Téléchargement possible ici :

http://www.01net.com/telecharger/windows/Utilitaire/optimiseurs_et_tests/fiches/33701.html

http://www.clubic.com/telecharger-fiche18178-belarc-advisor.html

Testez le setup BelarcAdvisor nommé AdvisorInstaller.exe sur le site virustotal avant de l'installer. Personnellement je n'ai trouvé aucun danger.

Autre solution : utilisez Speccy et sauvegardez les résultats avec File → Save en mode texte. Placez ce fichier sur la même clé USB à mettre de côté.

1.3.2 Sauvegarde non programmée

Question

I semble que Windows fasse des sauvegardes sans mon consentement. Comment remédier à ce problème ??

Réponse

A vous de réfléchir si cette sauvegarde est utile ou non ?

Si vous pensez que c'est inutile car vous faites vos propres sauvegardes :

Paramètres → Mise à jour et sécurité → Sauvegarde dans l'écran de gauche.

Si vous trouvez mieux, merci de m'en informer pour en faire profiter tout le monde.

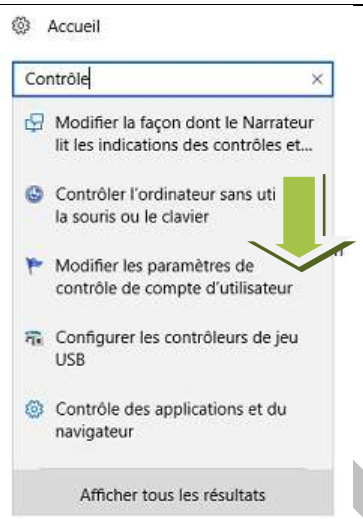
1.3.3 Fenêtre de sécurité UAC

Question

Je souhaite ne plus avoir en permanence les fenêtres de sécurité dès que j'ouvre une application. Comment faire avec les dernières versions de W10 ?

Réponse

Et oui, Les choses ont encore été modifiées pour nous simplifier la vie…
Menu Windows → Paramètres → Comptes. Puis dans la zone de recherche tapez « Contrôle »
Cliquez sur Modifier les paramètres de contrôle de compte d'utilisateur.
(figure ci-jointe). La fenêtre de la figure 2 s'ouvre.
Personnellement je mets à 0.
<u>Mais attention, il faut être conscient des risques encourus</u>



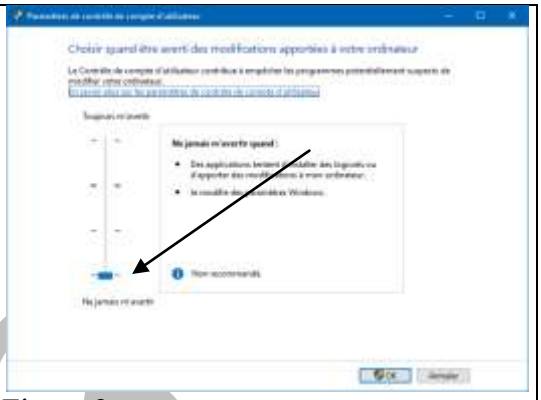


Figure 2

1.4 Niveau de sécurité utilisateur

Question

J'en ai assez de cette fenêtre qui s'ouvre « Voulez-vous autoriser cette application à apporter des modifications à cet appareil » ou il faut répondre Oui ou OK avant de pouvoir poursuivre le travail ? Même pour cCleaner cette question est posée. Est-il possible de la supprimer définitivement ?

Réponse

OUI, en baissant le niveau de sécurité et donc en faisant attention ensuite à ce que l'on fait ?
Ouvrez le panneau de configuration → Compte d'utilisateurs
Cliquez sur Modifier les paramètres de contrôle du compte d'utilisateur
Mettre le niveau au plus bas.
Vous ne serez plus empoisonné.
A vous d'être prudent par la suite.

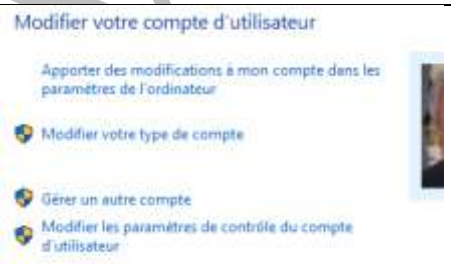
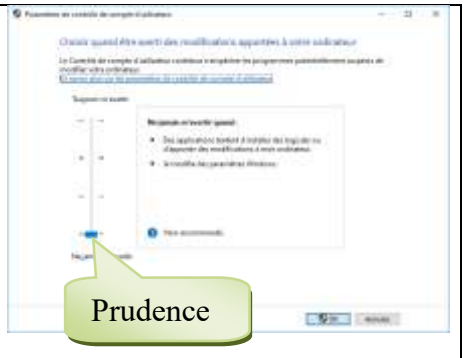


Fig 1



1.5 SmartScreen

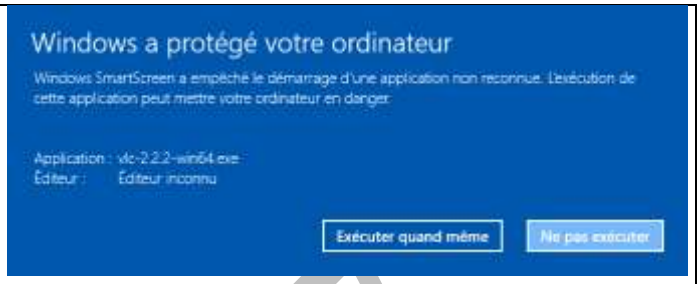
Question

A quoi sert Windows SmartScreen sur W8.1 ou W10?

Réponse

Ce logiciel sert à filtrer les logiciels potentiellement dangereux. Vous avez intérêt à l'activer dans les paramètres de confidentialité (cest bien le seul !). Cependant ce logiciel confond malheureusement logiciel dangereux et logiciel inconnu. Ainsi Adwcleaner, Filezilla ou JtUtil sont considérés comme dangereux, c'est absurde. Lorsque vous avez un doute sur un logiciel que vous venez de télécharger, testez son setup sur le site suivant :

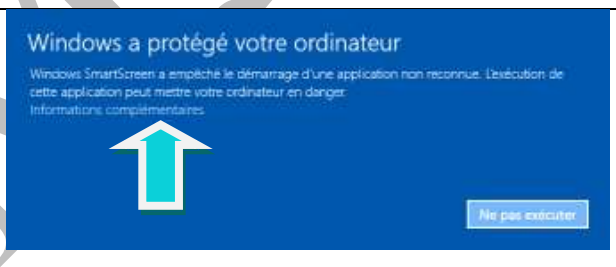
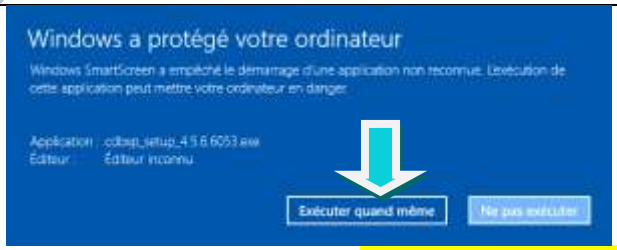
https://www.virustotal.com/ Vous aurez un test depuis une cinquantaine d'antivirus. Vous saurez immédiatement si le logiciel est dangereux ou non. Soyez toujours prudent avec des logiciels inconnus. Lorsque vous êtes sûr que le logiciel est sain, avec SmartScreen, cliquez « Renseignements complémentaires » puis « Exécuter quand même »

	
Si vous voulez « Vraiment télécharger » : Cliquez information complémentaire.	Si vous êtes sûr de vous, tapez « Exécuter quand même » sinon allez sur le site Virustotal ci-dessus pour analyser le setup que vous venez de télécharger

Voir la page http://jean.thiou.free.fr/CentreIndex.htm qui vous donne les détails.

Question

Lorsque je lance AdwCleaner Windows intervient pour l'interrompre ? Je télécharge CDBurnerXpPro ou AdwCleaner ou JtUtil…et j'obtiens cet écran. Parfois j'obtiens cet écran au moment de l'installation. Que dois-je faire ?

Réponse Evidemment, car AdwCleaner ne fait pas de cadeaux et supprime toutes les pourritures installées de façon crapuleuses. Alors évidemment MIcrosoft, Google et les autres tentent à tout prix de le stopper. Passer en force en cliquant alors sur « Plus d'informations » et « Exécuter quand même ».	
Microsoft ne connait pas (ou en veut pas connaître le logiciel que vous téléchargez). Comment ignorer Adwcleaner, Stinger (McAfee) où chaque nouvelle version est téléchargée au moins 20.000.000 de fois !!! Si vous êtes sûr, cliquez sur « Informations complémentaires » puis sur « Exécuter quand même ». Si vous avez un doute, ouvrez le site virustotal.com et tester le fichier EXE ou MSI que vous venez de télécharger et que vous souhaitez installer. Je vais faire ce contrôle avec CdBurner (image ci-jointe et analyse ci-dessous) qui contient parfois des suppléments toxiques	 En cas de doute cliquez sur « Ne pas Exécuter » afin de faire le test sur virustotal.com

Cas particulier : Voici les résultats pour CDBurnerXP le logiciel de gravure : https://www.virustotal.com/fr/file/2b6aa71c46492054b32b1959d118300c62412bb4d48795f0f299e7ef0891856d/analysis/ Ces résultats étant catastrophiques je suis surpris, alors que le logiciel lui-même n'est vraisemblablement pas en cause. Je pense que les logiciels parasites sont les uniques responsables, mais je n'en n'ai pas la preuve. J'ai décidé de l'installer quand même en décochant les logiciels supplémentaires. Puis j'ai fait une analyse avec Windows Defender, antivirus de Windows 10, et Stinger. J'ai passé l'exécutable de CDBurner chez VirusTotal, plus rien. Donc pour moi, le fait de faire attention, de bien décocher les logiciels inutiles, permet d'avoir quelque chose de propre.

1.6 Virus

Question

J'au un logiciel qui systématiquement déclenche l'annonce d'un cheval de Troie depuis la sécurité Windows. Après vérification sur plusieurs sites du type www.virustotal.com, il semble en fait que ce soit un faux positif. Comment régler définitivement ce problème ?

Réponse

On appelle faux positif, un logiciel dont la signature est semblable à celle d'un virus ou d'un cheval de Troie, et qui déclenche automatiquement l'antivirus de votre PC sans pour cela être dangereux.
Assurez-vous déjà en se testant sur virustotal.com et sur d'autres sites semblables qu'il s'agit bien d'un faux positif.
Voici une fiche de Mediaforma qui explique cette situation et vous donne la solution pour être tranquille.
https://www.mediaforma.com/windows-10-en-finir-avec-les-faux-positifs-dans-securite-windows/

1.6.1 Télécharger un Setup. Prudence

Question

Puis-je télécharger un logiciel depuis n'importe quel site ?. Lesquels sont à éviter ?

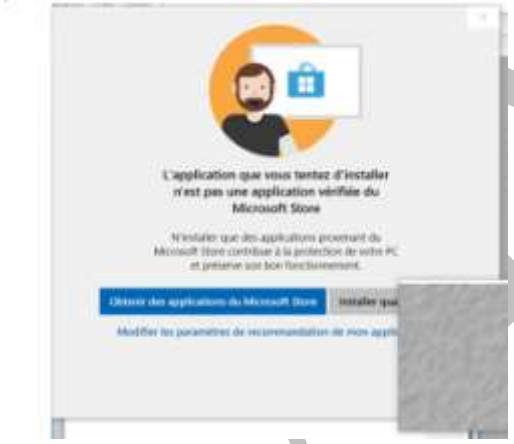
Réponse

Non. Soyez prudent. J'ai beaucoup râlé contre PcAsuces qui nous forçcait à attendre 30 secondes, mais je pense qu'il est resté l'un des sites les plus sûrs et le plus sérieux, concernant les téléchargements des free-wares. Evitez les sites Softonic et Clubic qui vous forcent à télécharger en même temps, des logiciels non sollicités. Même 01net devient limite à cet égard. Le site CCM (Commeznt çà marche) fait beaucoup de pubs, mais reste correcte sur les téléchargements. Dans tous les cas, quelque soit le site un contrôle sur virustotal.com est nécessaire. Des logiciels, comme cdex.exe, autre fois sains, sont maintenant truffés de malwares. Ils devront donc être évités sur tous les sites.

1.6.2 Les mises en garde de Microsoft

Question

Dés que je veux installer un logiciel j'ai droit à ce type de message ?



Réponse

Bien oui quoi, vous exagérez..

1. Vous n'achetez pas vos logiciels sur le Store de Microsoft, vous les prenez sur un autre site.
2. En plus, ils sont gratuits.

C'est donc honteux. Que la planète ne soit plus habitable dans 50 ans, Microsoft s'en moque. La seule chose qui compte c'est de faire du fric et maintenant.
Suite à des soucis avec mon PC, la carte mère a été changée. Immédiatement Microsoft m'a signalé que j'avais 48h pour acheter un nouvelle licence de MsOffice 2016. Depuis j'utilise la version 2007 devenue très lente et je suppose que ce n'est pas un hasard... Merci Microsoft.
La seule chose qui compte c'est que le setup du logiciel que vous allez installer soit sain. Il faut donc le tester sur virustotal.com par exemple avant de l'installer. Ce que dit Microsoft n'a aucun intérêt. Cliquez sur Installer quand même.

Malheureusement j'ai oublié, comment dans les paramètres on peut interdire ce type de message. Si vous retrouvez, comment faire, merci de nous le dire…

1.6.3 Les produits Piriform.

Question

Microsoft Windows Defender me signale comme dangereux le setup de cCleaner ?

Réponse

C'est parfois exact lorsqu'il permet d'installer d'autres produits aussi inutiles qu'indésirables. Il faut aussi être prudent contre les avis de Microsoft, qui ne supporte pas que l'on installe des produits qui ne provien-

nent pas de son store. Décochez toujours les produits supplémentaires au moment de l'installation. Les PUA signalés ne sont pas dangereux.

Définition des PUA :

https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/criteria#potentially-unwanted-application-pua

Voici la liste des produits Piriform à surveiller et a passez dans virustotal.com comme tous les autres logiciels gratuits. Refusez les versions gratuites d'essai pendant 14 jours.

Le risque encouru est limité (Produits nommés PUA).

En effet, Windows Defender peut détecter un fichier isolé sans qu'aucune infection et menaces ne soit active sur votre PC. PUA est le nom donné à un publicité non souhaitée. En cas de doute, Il faut donc jeter un œil à l'emplacement de la menace détectée par Windows Defender. Testez avec Malware bytes, puis Malware Hubter, AdwCleaner et Rogue killer, ces logiciels suspects en utilisant le menu contextuel du bouton droit lorsque c'est possible.

Selon son emplacement, on peut avoir une idée si un logiciel malveillant est actif sur le PC.

J'en conclue que W10 lui-même vous propose d'installer votree Smaertphone (avec Hello et termine en vous proposant MSOFFICE 365 utilise lui-même les PUA.

Voici le contre-rendu de Microsoft :

Certains installateurs pour les versions d'essai gratuites et de 14 jours de CCleaner, Defraggler, Recuva et Speccy sont fournis avec des applications groupées, y compris des applications qui ne sont pas requises ou développées par le même éditeur Piriform. Alors que les applications groupées elles-mêmes sont légitimes, le groupage de logiciels, en particulier de produits d'autres fournisseurs, peut entraîner une activité logicielle inattendue qui peut avoir un impact négatif sur l'expérience utilisateur. Pour protéger les utilisateurs Windows, Microsoft Defender Antivirus détecte les programmes d'installation des applications Piriform qui présentent potentiellment des PUAt .

1.7 Phishing. Protection sites bancaires

Question

Comment lutter contre le phishing (hameçonnage) ?

Réponse

Une réponse de la banque Boursorama (Société Générale).

https://www.boursorama.com/aide-en-ligne/securite-informatique/phishing-email-frauduleux-et-escroquerie/question/comment-reagir-au-phishing-847653

1.8 Ransomware

Un **ransomware**, ou rançongiciel en français, est un logiciel informatique malveillant, prenant en otage les données. Le **ransomware** chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer.

1.8.1 Danger

Les attaques sont mondiales et nous pouvons tous en être victime. L'un des Etats responsables, soupçonné par les spécialistes serait (entre autres) la Corée du Nord. Cette dénonciation, d'attaque mondiale par ce pays, est faite par les informaticiens spécialistes des attaques...bref ce n'est pas une affirmation stupide de Monsieur Trump.

1.8.2 Ce qu'il faut faire absolument et régulièrement.

- Sauvegarder son système
- Sauvegarder ses données (doc, musique, vidéo…)

Vous devez pour cela utiliser des disques durs externes USB, non branchés en permanence.

1.8.3 Il m'arrive un truc bizarre sur mon PC. Qu'est-ce que je fais ?

Généralement vous êtes sur un navigateur et des fenêtres s'ouvrent à la volée, avec des menaces, des virus annoncés et je dois a^^emer un numéro de téléphone, bref des arnaques.
Vous éteignez le plus rapidement possible, en force, votre PC en coupant le courant afin que ces saloperies m'aient pas le temps de s'installer dans le système. Ce sera le cas si vous éteignez en passant par les étapes habituelles.
En suite, essayez de redémarrer en mode sans échec. Je sais ce n'est pas facile depuis que le BIOS a disparu, mais il faut avoir prévu ce genre de situation avant que cela ne vous arrive. Lisez votre écran bleu, juste dans la seconde qui précédent le démarrage de Windows, pour savoir sur quelle touche il faut appuyer. Essayez par avance. Testez le lacement au pas à pas, pour éviter de lancer un programme qui vous semble suspect.
Une autre personne connectée à Internet sur un autre PC pourra peut-être vous être utile dans ce genre de situation,, pour vous dire qui fait quoi ? A quoi correspond un programme donné qui veut se lancer.

1.9 Comment lutter contre le ransomware,

Il n'y a pas 36 solutions. Payer n'est pas la bonne.

1.9.1 Si votre disque est partitionné

- Sauvegardez le système avec True Image ou EaseUS Backup
- Sauvegardez vos données avec le module de sauvegarde différentielle contenu dans mon logiciel JTUTIL. Beaucoup de personnes qui l'on essayé le trouve indispensable et très commade pour la sauvegarde des données. En effet de lui-même il recherche les nouveaux fichiers, ceux qui sont modifiés, ceux qui ne sont plus sur votre PC. Vous n'avez donc pas à essayer de vous rappeler, ce que vous avez fait depuis les dernières sauvegardes, lle logiciel le fait pour vous. Vous décidez alors de la suite à donner.
- Cette sauvegarde doit se faire par séquence, on ne sauvegarde pas « Mes documents » en même temps que « Ma musique ». On sauvegarde par thème, que vous choisissez vous même avec sauvegarde des paramètres pour chaque thème (répertoire(s) choisi(s).

1.9.2 Votre disque n'est pas partitionné.

Je vous souhaite bien du plaisir.

- L'ensemble du disque C doit être sauvegardé avec True Image ou EaseUS

1.9.3 Je n'ai pas de sauvegarde sur disque dur externe

- Payez la rançon (le résultat n'est pas certain et le bitcoin vaut actuellement 11000 €) ou allez chez un spécialiste qui vous prendra au minimum 100 € pour remettre Windows en place, à condition de lui donner la clé de W10.
- Vous devrez réinstaller tous vos logiciels. Donc vous devez avoir les clés d'installation.
- Vous n'aurez que vos yeux pour pleurer pour tous les fichiers que vous aurez perdus.

Bien sur, un disque dur externe de 1 To vaut entre 70 et 80 euros. Il faut savoir ce que l'on veut. Il faut comprendre aussi que le monde informatique est de plus en plus pourri et dangereux.

Question

Quelle différence peut-on faire entre spam, hoax, et arnaque ?

Réponse

Déjà ils ont en commun de vous pourrir la vie.

- Le spam est une publicité que l'on vous impose, même si vous remplissez la zone demandant de ne plus la recevoir. L'adresse de l'expéditeur sera modifiée c'est tout. La CNIL ne dira rien car on ne lui donne pas les moyens de faire son boulot, de même que le site officiel antispam, qui au lieu de

vous demander une simple copie de l'email, vous demande de justifier notre nom adresse etc… comme si vous étiez le coupable. Ils refusent les pièces jointes donc ils refusent la preuve que vous pouvez donner. Ainsi sans doute, ils peuvent dormir plus tranquille derrière leurs bureaux et leurs PC…

- L'hoax (Canular) est une fausse information qui circule sur Internet et qui revient régulièrement avec quelques modifications. Pour avoir des renseignements, recopiez une partie du document que vous recollez dans les sites http://www.hoaxbuster.com/ ou http://www.hoaxkiller.fr/
- L'arnaque est plus grave : elle sert surtout à obtenir des infos sur vos comptes bancaires, mots de passe et autres…Bref comme c'est ce qu'il y a de plus dangereux, je parle chaque semaine de celles que je reçois ou de celles que des lecteurs ont reçues et me font parvenir.

Tant qu'une loi ne sera pas rédigée pour respecter votre vie privée sur Internet, ce problème ne changera pas. Ce n'est pas avec des députés « en marche » dans tous les sens, mais incompétents, que les choses change-ront.

1.9.4 Voici un exemple d'hoax, envoyé par Colette

Un hoax qui circule actuellement.
(sur fond vert, les commentaires que j'ai ajoutés)
ATTENTION !!!
Provenance : Courrier < https://go.microsoft.com/fwlink/?LinkId=550.....Donc cela commence ici avec une; fausse adresse microsoft> pour Windows **(je l'ai modifiée, mais à ne pas essayer)**
Vérification faite sur "Hoaxkiller" - Ce n'est pas une fausse info ! **?????**
FAUX : hoaxkiller dit exactement le contraire ici ;
http://www.hoaxkiller.fr/hoax/2010/virus-actualisation-windows-live.htm
Le texte du message ci-dessous

Attention
> >
> > **Pour ton ordinateur et le mien, fais circuler cet avis à tes amis, famille, contacts.**
> > **Dans les prochains jours sois attentif : n'ouvre aucun message avec une archive annexe appelée "Actualisation de Windows live", indépendamment de qui que ce soit qui te l'envoie.**
> > **C'est un virus qui bloque ton pc. > Ce virus viendra d'une personne connue que tu as dans ta liste d'adresses. C'est pour cela que tu dois envoyer ce message à tous tes contacts. Si tu reçois le message appelé : "Actualisation de Windows live", même si c'est envoyé par un ami, ne l'ouvre pas et arrête immédiatement ton ordinateur. C'est le pire virus annoncé par CNN.**
> >
> > **Il a été classé par Microsoft comme le virus le plus destructeur qui ait existé.**
> >
> > **Ce virus fut découvert lundi après-midi par Mc Afee. Il n'y a pas de possibilité de dépannage pour ce genre de virus. Il détruit simplement le Secteur Zéro du disque dur.**
> >
> > **Souviens-toi : si tu l'envoies à tes connaissances cela bénéficiera à tous.**

REMARQUE : Lorsque vous recevez ce type de message vérifiez vous-même immédiatement sur HoaxKiller et sur HoaxBuster et surtout n'utilisez jamais les faux liens proposés comme ici :
https://go.microsoft.com/fwlink/?LinkId=550.....

1.9.5 CCleaner et Avast

Question

Avast vient s'installer régulièrement sans me demander mon avis ?

Réponse

Vous avez installé cCleaner sans décocher en bas à droite le fait de ne pas installer AVAST.
Voilà de sales méthodes que l'on subit en utilisant des logiciels gratuits (freewares).
Comme vous pouvez le constater tout est en français sauf ce lien qui est en anglais. Curieux non !
Pour désinstaller AVAST complétement
AIVM → Téléchargements → Sécurité Antivirus → Désinstallation d'un antivirus.
N'hésitez à dire à Avast ce que vous pensez de ce comportement dans la petite enquête faite après la désinstallation.

1.9.6 Webcam

Question

Un pirate peut-il accéder à la webcam de mon PC, à mon insu ?

Réponse

Oui si votre ordinateur est une poubelle jamais nettoyée, une machine jamais protégé contre les malware et les virus et si votre adresse IP, elle non plus n'est pas protégée. En principe une protection de l'adresse IP existe chez les 4 grands FAI français, mais…
Il n'est même pas nécessaire d'aller sur le Darknet pour trouver ce type de logiciel de piratage, permettant d'explorer un PC en passant par l'adresse IP utilisée par votre box ou par votre Wifi si celui-ci n'est pas protégé (Wifi public).

1.10 Windows Defender

Voir aussi la fiche Logiciels : http://aivm37.free.fr/BI/JT/JT078_Logiciels.pdf

Question

Ou puis-je trouver les logiciels interceptés par Windows Defender ?

Réponse

Après passage de l'antivirus, allez dans les paramètres → Historique de protection. (En bleu sur la même page que Windows Defender). Pour chaque logiciel intercepté, cliquez le bouton Base afin d'ouvrir les détails.
Vous constaterez que souvent, Microsoft considère comme dangereux des logiciels qui ne proviennent pas de son Store. Parfois c'est exact : par exemple le Setup de cCleaner peut contenir une installation d'un navigateur, ou d'une autre application non désirée, mais que vous pouvez désactiver, si vous portez attention lors de l'installation. Sur la figure qui suit, le logiciel considéré comme dangereux est Filezilla. Ce logiciel est conçu pour mettre à jour ses sites Internet. Cela semble déplaire à Microsoft. J'ai alors cliqué sur le bouton Action puis sur Autoriser

1.11 Pare-feu de Windows

Question

Comment accéder aux réglages du pare-feu de Windows 10 ?

Réponse

Dans la zone de recherche tapez Pare, cela suffit pour faire apparaître le lien sur le pare-feu.-En cliquant sur ce lien, vous pouvez alors accéder aux différents réglages. Pour plus de détails,
http://www.mediaforma.com/windows-10-le-pare-feu-de-windows-10/

2 Antivirus

2.1 McAfee

2.2 Antivirus à retirer

2.2.1 McAfee

Question

Comment désinstaller McAfee sur un PC neuf (payant) pour le remplacer par Windows Defender (gratuit) ?

Réponse

Télécharger l'outil de désinstallation ici :
http://download.mcafee.com/products/licensed/cust_support_patches/MCPR.exe

1. Procédez à la désinstallation de McAfee depuis ce logiciel.
2. Lancez Windows defender pour pouvoir l'activer définitivement

2.3 Malwarebyte

Question

Malwarebytes veut installer une nouvelle version. Que faire ?

Réponse

Date de l'événement : 06/10/18.

Vous avez cette première fenêtre ci-jointe. Cliquez sur Accepter et Installer.

Au bout d'un certain temps, il vous dit que l'installation est terminée sans vous demander d'acheter la licence, alors …

Un nouvel essai premium va commencer pour 14 jours, avec le risuqe d'avoir à récativer Windwos Defender après cette date. Personnelement j'accepte, mais he refuserai la licence dans 14 jours

Pour rétablir Windows Defender. Cliquez sur l'icpone de Windows defender (proposé dans les raccourcis de bureau sur le site AIVM et vérifiez que tout est activé.

Vous pouvez aussi tapez Centre de sécurité et cloquez sur Centre de sé&cuité Windows. Vous avccedez à la même fenpetre

2.3.1 Avast non sollicité.

Question

J'ai Avast antivirus qui c'est installé sans mon accord ?

Réponse

Oui, il est apparu en installant CCleaner

Vous voulez installer cCleaner, vous avez raison, il est pratique et non dangereux. Evitez cependant le nettoyage de la base de registre (prenez Glary pour cela)..

Mais attention

Au moment de l'installation, il vous propose Avast, parfaitement inutile et encombrant, si vous avez choisi d'utiliser l'antivirus Defender de Microsoft.

Si vous avez commis l'erreur d'installer Avast, pour le désinstaller il faut absolument utiliser l'outil prévu par Avast. Vous le trouverez sur la page téléchargements du site AIVM.

Vous y trouvez aussi les désinstalleur des autres antivirus très connus comme Norton, Kapersky, McAfee.

2.4 Confusion entre maintenance et sécurité

Question

Je possède Norton antivirus. Quelqu'un m'a dit que je pouvais me dispenser de CCleaner, Glary Malwarebyte?

Réponse

Si vous n'avez acheté qu'une licence antivirus la réponse est non, on vous a dit n'importe quoi. ***Si votre licence Norton prévoit aussi la maintenance des fichiers sur le disque dur, la réponse est plus nuancée***, mais je n'ai pas trouvé sur le site de Norton des détails sur ces points précis. Il n'est question que de prix et de durée de contrat…Pour les contenus, c'est plus difficile. En fait, vous ne savez pas trop ce que vous payez…
Personnellement je ne vois pas l'intérêt de prendre un antivirus payant. La protection ne sera pas meilleure. D'autre part, penser que la licence antivirus (et elle seule) suffit pour nettoyer votre PC est absurde. Le travail d'un antivirus n'est pas de nettoyer les fichiers temporaires et les cookies. Chacun son boulot, et ce travail là, c'est celui des logiciels gratuits cCleaner et Glary ou Glary Pro. Dans le cas contraire, c'est confondre maintenance et sécurité. Il serait tout aussi absurde de penser que cCleaner et Glary vous protège des virus. D'autre part Malwarebytes n'est pas incompatible avec votre antivirus, il ne fait que renforcer la surveillance. Là encore, la version gratuite suffit.
Pour finir, quelque soit l'antivirus en votre possession, si vous ne faites pas un scan régulièrement, votre antivirus ne sert pas à grand-chose. Si vous pensez que votre PC est mieux protégé parce que vous avez payé une licence, cela me fait doucement rigoler. Les antivirus connus comme Norton, McAfee, Defender, Avast , AVG, Kapersky sont efficaces. Certains sont pauants, d'autres gratuits avec des publicités pénible et Défender de Microsoft est gratuit sans pub et il a bien progressé.

2.5 Meltdown et Spectre

A SAVOIR : Les attaques par ces deux Malwares peuvent très mal se terminer. Ils sont les plus dangereux du moment. Vous devez donc être très prudent.

Question

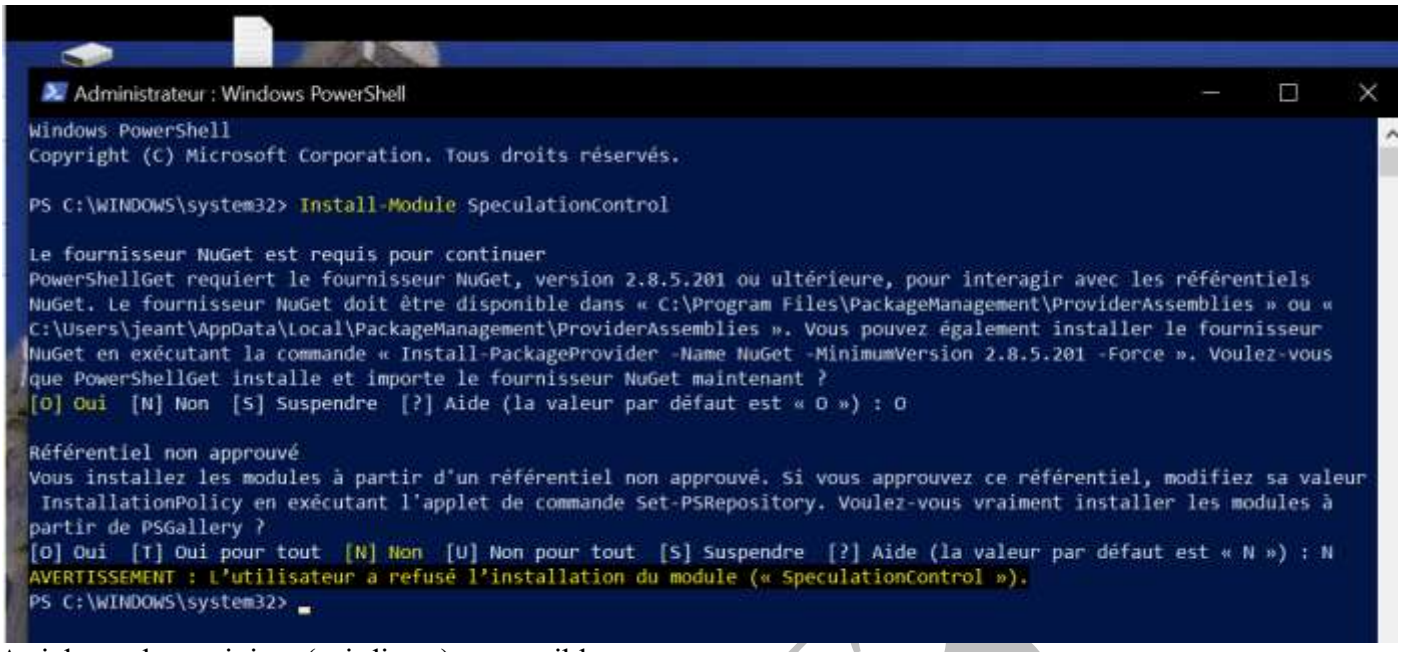
Peut-on résoudre les problèmes contre Meltdown et Spectre?

Réponse

Gros problème cependant : le patch créé par Microsoft peut se terminer sur un écran bleu dans les cas suivants :

1. Le patch n'est pas compatible avec votre antivirus
2. Votre PC possède un processeur AMD
3. Certains logiciels ou drivers anciens peuvent bloquer.

Pour ma part je vais attendre d'en savoir plus. Il faut être très prudent avec les fichiers que vous téléchargez (comme toujours) en attendant une information plus précise.
Quelques articles référents :
http://www.01net.com/astuces/failles-cpu-comment-verifier-le-degre-de-protection-de-votre-pc-windows-10-1347374.html
https://www.numerama.com/tech/322638-meltdown-et-spectre-intel-confirme-un-probleme-de-reboot-avec-les-patchs.html
https://www.numerama.com/tech/322580-comment-savoir-si-son-processeur-est-affecte-par-les-failles-meltdown-et-spectre.html
En attendant : Les manipulations (proposées dans la page ci-dessus) avec le mode Admin Powershel me semblent dangereuses car vous devez tapez Oui à des réponses ou Microsoft propose Non. Personnellement j'ai abandonné en route. Figure ci-dessous :



Article sur les antivirus (soi-disant) compatibles ;
https://docs.google.com/spreadsheets/u/1/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview?sle=true#gid=0
Concernant le logiciel Inspectre, j'attends d'en savoir un peu plus, avant de prendre position.

2.6 Les sites pas toujours net sur Internet

Question

J'ai voulu télécharger CCleaner sur PcAstuces et voila ce qui se passe ?

Réponse

Malheureusement en voulant télécharger CCleaner, sur PCAStuces deux onglets se sont ouverts, dont l'un signalait ceci : 'Que faut-il en penser, même si le risque est signalé comme faible ???

C'est la preuve qu'il faut être prudent sur tous les sites, y compris ceux qui semblent sérieux.

3 Arnaques

http://aivm37.free.fr/BI/JT/JT078_Arnaques.pdf