

AdwCleaner v6.046 - Rapport créé le 26/04/2017 à 20:09:55
Mis à jour le 24/04/2017 par Malwarebytes
Base de données : 2017-04-25.1 [Locale]
Système d'exploitation : Windows 10 Pro (X64)
Nom d'utilisateur : yvonm - DESKTOP-5JT1D4V
Exécuté depuis : E:\Téléchargements\adwcleaner_6.046.exe
Mode: Scan
Support : <https://www.malwarebytes.com/support>

***** [Services] *****

Aucun service malveillant trouvé.

***** [Dossiers] *****

Aucun dossier malveillant trouvé.

***** [Fichiers] *****

Aucun fichier malveillant trouvé.

***** [DLL] *****

Aucune DLL patchée trouvée.

***** [WMI] *****

Aucune clé malveillante trouvée.

***** [Raccourcis] *****

Aucun raccourci infecté trouvé.

***** [Tâches planifiées] *****

Aucune tâche malveillante trouvée.

***** [Registre] *****

Aucun élément malveillant trouvé dans le registre.

***** [Navigateurs web] *****

Aucune préférence Firefox malveillante trouvée.

Aucune préférence Chromium malveillante trouvée.

Malwarebytes
www.malwarebytes.com

-Détails du journal-

Date de l'analyse: 26/04/2017

Heure de l'analyse: 19:29

Fichier journal: Rapport Malwarebyte.txt

Administrateur: Oui

-Informations du logiciel-

Version: 3.0.6.1469

Version de composants: 1.0.50

Version de pack de mise à jour: 1.0.1814

Licence: Premium

-Informations système-

Système d'exploitation: Windows 10

Processeur: x64

Système de fichiers: NTFS

Utilisateur: DESKTOP-5JT1D4V\yvonm

-Résumé de l'analyse-

Type d'analyse: Analyse des menaces

Résultat: Terminé

Objets analysés: 415412

Temps écoulé: 24 min, 1 s

-Options d'analyse-

Mémoire: Activé

Démarrage: Activé

Système de fichiers: Activé

Archives: Activé
Rootkits: Activé
Heuristique: Activé
PUP: Activé
PUM: Activé

-Détails de l'analyse-

Processus: 0
(Aucun élément malveillant détecté)
Module: 0
(Aucun élément malveillant détecté)
Clé du registre: 0
(Aucun élément malveillant détecté)
Valeur du registre: 0
(Aucun élément malveillant détecté)
Données du registre: 0
(Aucun élément malveillant détecté)
Flux de données: 0
(Aucun élément malveillant détecté)
Dossier: 0
(Aucun élément malveillant détecté)
Fichier: 1
RiskWare.DontStealOurSoftware, C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS, Aucune action de l'utilisateur, [685], [353143],0.0.0
Secteur physique: 0
(Aucun élément malveillant détecté)

RogueKiller V12.10.6.0 (x64) [Apr 24 2017] (Gratuit) par Adlice Software
email : <http://www.adlice.com/contact/>
Remontées : <https://forum.adlice.com>
Site web : <http://www.adlice.com/fr/download/roguekiller/>
Blog : <http://www.adlice.com>

Système d'exploitation : Windows 10 (10.0.15063) 64 bits version
Démarré en : Mode normal
Utilisateur : yvonm [Administrateur]
Démarré depuis : C:\Program Files\RogueKiller\RogueKiller64.exe
Mode : Scan -- Date : 04/26/2017 18:23:29 (Durée : 01:35:50)

Processus : 0 ###
Registre : 0 ###
Tâches : 0 ###
Fichiers : 1 ###
[PUP.Gen1][Répertoire] C:\Program Files\Windows Security -> Trouvé(e)
WMI : 0 ###
Fichier Hosts : 0 ###
Antirootkit : 0 (Driver: Chargé) ###
Navigateurs web : 2 ###
[PUM.HomePage][Firefox:Config] yhizu3qh.default : user_pref("browser.startup.homepage", "http://startpage.com/fra"); -> Trouvé(e)
[PUM.HomePage][Chrome:Config] ChromeDefaultData [SecurePrefs] : session.startup_urls [https://startpage.com/fra|http://www.symbaloo.com/home/mix/13ePQJ4B36] -> Trouvé(e)
Vérification MBR : ###
++++ PhysicalDrive0: Hitachi HDP725032GLA380 ATA Device ++++
--- User ---
[MBR] 2f2476a2262d7f63976ac59f4224a5e3
[BSP] c855bb00c997976c02b782196056eb6f : Windows Vista/7/8 MBR Code
Partition table:
0 - [ACTIVE] NTFS (0x7) [VISIBLE] Offset (sectors): 63 | Size: 305243 MB [Windows Vista/7/8 Bootstrap | Windows Vista/7/8 Bootloader]

User = LL1 ... OK
User = LL2 ... OK
+++++ PhysicalDrive1: WDC WD10EZEX-22BN5A0 ATA Device +++++
--- User ---
[MBR] b098be33222efad83d166244799b5771
[BSP] 4bd8e2cff4a920d64bd673d40f3b528b : Windows Vista/7/8 MBR Code
Partition table:
0 - [ACTIVE] NTFS (0x7) [VISIBLE] Offset (sectors): 2048 | Size: 476934 MB [Windows Vista/7/8
Bootstrap | Windows Vista/7/8 Bootloader]
1 - [XXXXXX] NTFS (0x7) [VISIBLE] Offset (sectors): 976762880 | Size: 476932 MB [Windows Vista/7/8
Bootstrap | Windows Vista/7/8 Bootloader]
User = LL1 ... OK
User = LL2 ... OK
+++++ PhysicalDrive2: ST3200826AS ATA Device +++++
--- User ---
[MBR] 26a9628e9f932b9aece4eaab2479cf80
[BSP] cd6fa63a7a0228ba2cd33d3dbaecd512 : Windows Vista/7/8 MBR Code
Partition table:
0 - [ACTIVE] NTFS (0x7) [VISIBLE] Offset (sectors): 2048 | Size: 500 MB [Windows Vista/7/8 Bootstrap |
Windows Vista/7/8 Bootloader]
1 - [XXXXXX] NTFS (0x7) [VISIBLE] Offset (sectors): 1026048 | Size: 189813 MB [Windows Vista/7/8
Bootstrap | Windows Vista/7/8 Bootloader]
2 - [XXXXXX] ACER (0x27) [VISIBLE] Offset (sectors): 389765120 | Size: 466 MB
User = LL1 ... OK
User = LL2 ... OK
+++++ PhysicalDrive3: Samsung M3 Portable SCSI Disk Device +++++
--- User ---
[MBR] e675fefbc5b31fb8762e6a0194ae0982
[BSP] e5df95155939c0faf6e0db7183156bd4 : Windows XP MBR Code
Partition table:
0 - [ACTIVE] NTFS (0x7) [VISIBLE] Offset (sectors): 64 | Size: 953867 MB [Windows Vista/7/8 Bootstrap
| Windows Vista/7/8 Bootloader]
User = LL1 ... OK
Error reading LL2 MBR! ([1] Fonction incorrecte.)

~ ZHPCleaner v2017.4.26.70 by Nicolas Coolman (2017/04/26)
~ Run by yvonm (Administrator) (26/04/2017 19:23:42)
~ Web: <https://www.nicolascoolman.com>
~ Blog: <https://nicolascoolman.eu/>
~ Facebook : <https://www.facebook.com/nicolascoolman1>
~ State version : Version KO
~ Type : Scanner
~ Report : C:\Users\yvonm\Desktop\ZHPCleaner.txt
~ Quarantine : C:\Users\yvonm\AppData\Roaming\ZHP\ZHPCleaner_Reg.txt
~ UAC : Activate
~ Boot Mode : Normal (Normal boot)
Windows 10 Pro, 64-bit (Build 15063)

---\\ Service. (0)
~ Aucun élément malicieux ou superflu trouvé.

---\\ Navigateur internet. (0)
~ Aucun élément malicieux ou superflu trouvé.

---\\ Fichier hôte. (0)
~ Aucun élément malicieux ou superflu trouvé.

---\\ Tâche planifiée. (0)
~ Aucun élément malicieux ou superflu trouvé.

---\\ Explorateur (Dossiers, Fichiers). (0)
~ Aucun élément malicieux ou superflu trouvé.

---\\ Base de Registres (Clés, Valeurs, Données). (0)
~ Aucun élément malicieux ou superflu trouvé.

---\\ Nettoyage Additionnel. (10)
~ Suppression des Clés de registre Tracing. (9)
~ Suppression des anciens rapports ZHPCleaner. (1)

---\\ Bilan de la réparation
~ Aucune réparation effectuée.
~ Ce navigateur est absent (Opera Software)

---\\ Statistiques
~ Items scannés : 807
~ Items trouvés : 0
~ Items annulés : 0
~ Items réparés : 0