DERNIER RAPPORTS MALWAREBYTES :

Malwarebytes Anti-Malware 1.75.0.1300

www.malwarebytes.org

Version de la base de données: v2014.02.16.05

Windows XP Service Pack 3 x86 NTFS

Internet Explorer 8.0.6001.18702

Propriétaire :: VINY-YANN [administrateur]

18/02/2014 21:13:13

mbam-log-2014-02-18 (21-13-13).txt

Type d'examen: Examen complet (A:\|C:\|D:\|E:\|F:\|G:\|)

Options d'examen activées: Mémoire | Démarrage | Registre | Système de fichiers | Heuristique/Extra | Heuristique/Shuriken | PUP | PUM | P2P

Options d'examen désactivées:

Elément(s) analysé(s): 343587

Temps écoulé: 1 heure(s), 56 minute(s), 8 seconde(s)

Processus mémoire détecté(s): 0

(Aucun élément nuisible détecté)

Module(s) mémoire détecté(s): 0

(Aucun élément nuisible détecté)

Clé(s) du Registre détectée(s): 0

(Aucun élément nuisible détecté)

Valeur(s) du Registre détectée(s): 0

(Aucun élément nuisible détecté)

Elément(s) de données du Registre détecté(s): 0

(Aucun élément nuisible détecté)

Dossier(s) détecté(s): 0

(Aucun élément nuisible détecté)

fichier(s) détecté(s): 0

(Aucun élément nuisible détecté)

(fin)

RAPPORT avant-hier AVEC UNE TONNE DE MERDOUILLES :

Malwarebytes Anti-Malware 1.75.0.1300

www.malwarebytes.org

Version de la base de données: v2014.02.16.05

Windows XP Service Pack 3 x86 NTFS

Internet Explorer 8.0.6001.18702

Propriétaire :: VINY-YANN [administrateur]

16/02/2014 21:30:43

mbam-log-2014-02-16 (21-30-43).txt

Type d'examen: Examen complet (A:\|C:\|D:\|E:\|F:\|G:\|)

Options d'examen activées: Mémoire | Démarrage | Registre | Système de fichiers | Heuristique/Extra | Heuristique/Shuriken | PUP | PUM | P2P

Options d'examen désactivées:

Elément(s) analysé(s): 343324

Temps écoulé: 1 heure(s), 54 minute(s), 34 seconde(s)

Processus mémoire détecté(s): 0

(Aucun élément nuisible détecté)

Module(s) mémoire détecté(s): 0

(Aucun élément nuisible détecté)

Clé(s) du Registre détectée(s): 4

HKLM\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{68B81CCD-A80C-4060-8947-5AE69ED01199} (PUP.Optional.Iminent.A) -> Mis en quarantaine et supprimé avec succès.

HKLM\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{E6B969FB-6D33-48d2-9061-8BBD4899EB08} (PUP.Optional.Iminent.A) -> Mis en quarantaine et supprimé avec succès.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{84FF7BD6-B47F-46F8-9130-01B2696B36CB} (PUP.Optional.Iminent.A) -> Mis en quarantaine et supprimé avec succès.

HKLM\Software\Iminent (PUP.Optional.Iminent.A) -> Mis en quarantaine et supprimé avec succès.

Valeur(s) du Registre détectée(s): 2

HKCU\SOFTWARE\Microsoft\Internet Explorer\URLSearchHooks|{84FF7BD6-B47F-46F8-9130-01B2696B36CB} (PUP.Optional.Iminent.A) -> Données: -> Mis en quarantaine et supprimé avec succès.

HKCU\SOFTWARE\Microsoft\Internet Explorer\URLSearchHooks\{84FF7BD6-B47F-46F8-9130-01B2696B36CB} (PUP.Optional.Iminent.A) -> Données: -> Mis en quarantaine et supprimé avec succès.

Elément(s) de données du Registre détecté(s): 0

(Aucun élément nuisible détecté)

Dossier(s) détecté(s): 11

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0 (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\userCode (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\icons (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\icons\actions (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\api (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\popupResource (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

Fichier(s) détecté(s): 65

C:\Documents and Settings\Propriétaire\Bureau\SoftonicDownloader_pour_in-poculis-mahjong.exe (PUP.Optional.Softonic.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Temp\Umbrella.exe2ca87e (PUP.Optional.Iminent) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Temp\IMsetup.exe (PUP.Optional.Iminent.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Mes documents\Téléchargements\SoftonicDownloader_pour_in-poculis-mahjong.exe (PUP.Optional.Softonic.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\background.html (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\crossriderManifest.json (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\manifest.json (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\popup.html (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\manifest.xml (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins.json (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\22_resources.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\102_dealply_m.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\104_jollywallet_m.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\13_CrossriderAppUtils.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\14_CrossriderUtils.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\177_crossriderDashboard.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\17_jQuery.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\182_openUrl.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\183_tabsWrapper.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\198_superfish_no_search_no_coupons_plushd_m.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\19_CHAppAPIWrapper.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\1_base.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\21_debug.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\28_initializer.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\47_resources_background.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\4_jquery_1_7_1.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\64_appApiMessage.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\72_appApiValidation.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\78_CrossriderInfo.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\80_CHPopupAppAPI.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\91_monetizationLoader.js.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\plugins\97_resourceApiWrapper.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\userCode\background.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\extensionData\userCode\extension.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\icons\icon128.png (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\icons\icon16.png (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\icons\icon48.png (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\icons\actions\1.png (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\background.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\main.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\platformVersion.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\api\chrome.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\api\cookie.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\api\message.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\api\pageAction.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\api\pageActionBG.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\app_api.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\bg_app_api.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\consts.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\cookie_store.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\crossriderAPI.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\delegate.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\events.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\extensionDataStore.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\installer.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\logFile.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\logging.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\onBGDocumentLoad.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\reports.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\storageWrapper.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\updateManager.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\util.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\xhr.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\popupResource\newPopup.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\extensions\eeibjhjmddgcdbniedjoghdgbofbecad\1.26.12_0\js\lib\popupResource\popup.js (PUP.Optional.CrossRider.A) -> Mis en quarantaine et supprimé avec succès.

(fin)

RESULTAT ADW CLEANER

AdwCleaner v3.019 - Rapport créé le 19/02/2014 à 11:32:48

Mis à jour le 17/02/2014 par Xplode

Système d'exploitation : Microsoft Windows XP Service Pack 3 (32 bits)

Nom d'utilisateur : Propriétaire - VINY-YANN

Exécuté depuis : C:\Documents and Settings\Propriétaire\Mes documents\Téléchargements\adwcleaner.exe

Option : Nettoyer

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

***** [Fichiers / Dossiers] *****

Dossier Supprimé : C:\Documents and Settings\Propriétaire\Application Data\Windows Net Data

Dossier Supprimé : C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\Extensions\EFGLQA@78ETGYN-0W7FN789T87.COM

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

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

Clé Supprimée : HKCU\Software\Softonic

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

-\\ Internet Explorer v8.0.6001.18702

-\\ Mozilla Firefox v27.0.1 (fr)

[Fichier : C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\prefs.js]

Ligne Supprimée : user_pref("extensions.crossrider.bic", "14420433e12ccc5b810e9160271503ef");

Ligne Supprimée : user_pref("iminent.LayoutId", "28");

Ligne Supprimée : user_pref("iminent.adapters", "{\"avira\":{\"CountryCode\":\"FR\",\"NoAds\":false,\"Status\":2,\"expireTime\":\"13921107027581814400\"}}");

Ligne Supprimée : user_pref("iminent.enabledAds", "false");

Ligne Supprimée : user_pref("iminent.version", "8.4.3.1");

Ligne Supprimée : user_pref("iminent.versioning", "{\"CurrentVersion\":\"8.4.3.1\",\"InstallEventCTime\":1392110680250,\"InstallEvent\":\"True\"}");

-\\ Google Chrome v

[Fichier : C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\Default\preferences]

****

AdwCleaner[R0].txt - [9487 octets] - [07/02/2014 10:59:56]

AdwCleaner[R1].txt - [1361 octets] - [09/02/2014 20:45:31]

AdwCleaner[R2].txt - [2140 octets] - [19/02/2014 11:29:46]

AdwCleaner[S0].txt - [9665 octets] - [07/02/2014 11:04:00]

AdwCleaner[S1].txt - [1424 octets] - [09/02/2014 20:54:27]

AdwCleaner[S2].txt - [2078 octets] - [19/02/2014 11:32:48]

########## EOF - C:\AdwCleaner\AdwCleaner[S2].txt - [2138 octets] ##########

RAPPORT ZHPDiag

~ Rapport de ZHPDiag v2014.2.17.15 - Nicolas Coolman (17/02/2014)

~ Lancé par Propriétaire (19/02/2014 12:18:46)

~ Adresse du Site Web http://nicolascoolman.webs.com

~ Forums gratuits d'Assistance à la désinfection : http://nicolascoolman.webs.com/apps/links/

~ Traduit par Nicolas Coolman

~ Etat de la version :

~ Liste blanche : Activée par le programme

~ Elévation des Privilèges : OK

~ User Account Control (UAC): Not Found

---\\ Navigateurs Internet

MSIE: Internet Explorer v8.0.6001.18702

MFIE: Mozilla Firefox 27.0.1 (Defaut)

---\\ Informations sur les produits Windows

~ Langage: Français

Microsoft Windows XP, 32-bit Service Pack 3 (Build 2600)

Windows Automatic Updates : OK

Windows Genuine Advantage : OK

---\\ Logiciels de protection du système

Avira Free Antivirus v14.0.2.286

Malwarebytes Anti-Malware version 1.75.0.1300

ESET Online Scanner v3

---\\ Logiciels d'optimisation du système

CCleaner v4.09 =>Piriform Ltd

---\\ Logiciels de partage PeerToPeer

---\\ Surveillance de Logiciels

Adobe Flash Player 12 Plugin

Adobe Reader X

Java 7 Update 45

---\\ Informations sur le système

~ Processor: x86 Family 15 Model 2 Stepping 7, GenuineIntel

~ Operating System: 32 Bits

Boot mode: Normal (Normal boot)

Total RAM: 1023 MB (22% free)

System Restore: Activé (Enable)

System drive C: has 28 GB (40%) free of 70 GB

---\\ Mode de connexion au système

~ Computer Name: VINY-YANN

~ User Name: Propriétaire

~ All Users Names: SUPPORT_fddfa904, SUPPORT_388945a0, Propriétaire, HelpAssistant, ASPNET, Administrateur,

~ Unselected Option: None

Logged in as Administrator

---\\ Variables d'environnement

~ System Unit : C:\

~ %AppZHP% : C:\Documents and Settings\Propriétaire\Application Data\ZHP\

~ %AppData% : C:\Documents and Settings\Propriétaire\Application Data\

~ %Desktop% : C:\Documents and Settings\Propriétaire\Bureau\

~ %Favorites% : C:\Documents and Settings\Propriétaire\Favoris\

~ %LocalAppData% : C:\Documents and Settings\Propriétaire\Local Settings\Application Data\

~ %StartMenu% : C:\Documents and Settings\Propriétaire\Menu Démarrer\

~ %Windir% : C:\WINDOWS\

~ %System% : C:\WINDOWS\system32\

---\\ Enumération des unités disques

A: Floppy drive, Flash card reader, USB Key (Not Inserted)

C: Hard drive, Flash drive, Thumb drive (Free 28 Go of 70 Go)

D: Hard drive, Flash drive, Thumb drive (Free 1 Go of 5 Go)

E: CD-ROM drive (Not Inserted)

F: CD-ROM drive (Not Inserted)

G: Hard drive, Flash drive, Thumb drive (Free 206 Go of 233 Go)

---\\ Etat du Centre de Sécurité Windows

~ Security Center: 42 Legitimates Filtered in 00mn 00s

---\\ Recherche particulière de fichiers génériques

[MD5.F2317622D29F9FF0F88AEECD5F60F0DD] - (.Microsoft Corporation - Explorateur Windows.) (.14/04/2008 - 03:34:03.) -- C:\WINDOWS\Explorer.exe [1037824]

[MD5.2988BFF8257A55EA8AFD038F49F81A34] - (.Microsoft Corporation - Internet Extensions for Win32.) (.06/02/2014 - 00:20:01.) -- C:\WINDOWS\system32\wininet.dll [920064]

[MD5.DD73D6B9F6B4CB630CF35B438B540174] - (.Microsoft Corporation - Application d'ouverture de session Windows NT.) (.14/04/2008 - 03:34:28.) -- C:\WINDOWS\system32\Winlogon.exe [512000]

[MD5.1E44BC1E83D8FD2305F8D452DB109CF9] - (.Microsoft Corporation - Ancillary Function Driver for WinSock.) (.17/08/2011 - 14:49:54.) -- C:\WINDOWS\system32\Drivers\AFD.sys [138496]

[MD5.9F3A2F5AA6875C72BF062C712CFA2674] - (.Microsoft Corporation - IDE/ATAPI Port Driver.) (.13/04/2008 - 19:40:30.) -- C:\WINDOWS\system32\Drivers\atapi.sys [96512]

[MD5.C885B02847F5D2FD45A24E219ED93B32] - (.Microsoft Corporation - CD-ROM File System Driver.) (.13/04/2008 - 20:14:21.) -- C:\WINDOWS\system32\Drivers\Cdfs.sys [63744]

[MD5.1F4260CC5B42272D71F79E570A27A4FE] - (.Microsoft Corporation - SCSI CD-ROM Driver.) (.13/04/2008 - 19:40:46.) -- C:\WINDOWS\system32\Drivers\Cdrom.sys [62976]

[MD5.31F923EB2170FC172C81ABDA0045D18C] - (.Microsoft Corporation - Pilote de cryptographie FIPS.) (.14/04/2008 - 02:57:38.) -- C:\WINDOWS\system32\Drivers\Fips.sys [44672]

[MD5.573C7D0A32852B48F3058CFD8026F511] - (.Windows (R) Server 2003 DDK provider - High Definition Audio Bus Driver v1.0a.) (.13/04/2008 - 17:36:05.) -- C:\WINDOWS\system32\Drivers\HDAudBus.sys [144384]

[MD5.A09BDC4ED10E3B2E0EC27BB94AF32516] - (.Microsoft Corporation - Pilote de port i8042.) (.14/04/2008 - 03:00:52.) -- C:\WINDOWS\system32\Drivers\i8042prt.sys [54144]

[MD5.083A052659F5310DD8B6A6CB05EDCF8E] - (.Microsoft Corporation - IMAPI Kernel Driver.) (.13/04/2008 - 19:40:58.) -- C:\WINDOWS\system32\Drivers\Imapi.sys [42112]

[MD5.CC748EA12C6EFFDE940EE98098BF96BB] - (.Microsoft Corporation - IP Network Address Translator.) (.13/04/2008 - 19:57:15.) -- C:\WINDOWS\system32\Drivers\IpNat.sys [152832]

[MD5.23C74D75E36E7158768DD63D92789A91] - (.Microsoft Corporation - IPSec Driver.) (.13/04/2008 - 20:19:42.) -- C:\WINDOWS\system32\Drivers\IPSec.sys [75264]

[MD5.7D304A5EB4344EBEEAB53A2FE3FFB9F0] - (.Microsoft Corporation - Windows NT SMB Minirdr.) (.15/07/2011 - 14:29:31.) -- C:\WINDOWS\system32\Drivers\MRxSmb.sys [456320]

[MD5.74B2B2F5BEA5E9A3DC021D685551BD3D] - (.Microsoft Corporation - MBT Transport driver.) (.13/04/2008 - 20:21:00.) -- C:\WINDOWS\system32\Drivers\netBT.sys [162816]

[MD5.78A08DD6A8D65E697C18E1DB01C5CDCA] - (.Microsoft Corporation - NT File System Driver.) (.13/04/2008 - 20:15:53.) -- C:\WINDOWS\system32\Drivers\ntfs.sys [574976]

[MD5.8FD0BDBEA875D06CCF6C945CA9ABAF75] - (.Microsoft Corporation - Pilote de port parallèle.) (.14/04/2008 - 03:09:40.) -- C:\WINDOWS\system32\Drivers\Parport.sys [80384]

[MD5.11B4A627BC9614B885C4969BFA5FF8A6] - (.Microsoft Corporation - RAS L2TP mini-port/call-manager driver.) (.13/04/2008 - 20:19:43.) -- C:\WINDOWS\system32\Drivers\Rasl2tp.sys [51328]

[MD5.15CABD0F7C00C47C70124907916AF3F1] - (.Microsoft Corporation - Microsoft RDP Device redirector.) (.13/04/2008 - 19:32:51.) -- C:\WINDOWS\system32\Drivers\rdpdr.sys [196224]

[MD5.D8EB2A7904DB6C916EB5361878DDCBAE] - (.Microsoft Corporation - Pilote de filtre audio Livre rouge.) (.14/04/2008 - 02:57:34.) -- C:\WINDOWS\system32\Drivers\redbook.sys [58752]

[MD5.46DE1126684369BACE4849E4FC8C43CA] - (.Microsoft Corporation - Pilote de cliché instantané du volume.) (.14/04/2008 - 02:56:04.) -- C:\WINDOWS\system32\Drivers\volsnap.sys [53376]

~ Generic Processes: Scanned in 00mn 00s

---\\ Etat des fichiers cachés (Caché/Total)

~ Mes images (My Pictures) : 2/6

~ Mes musiques (My Musics) : 1/10

Mes Videos (My Videos) : 2/2   (Modified)

~ Mes Favoris (My Favorites) : 1/53

~ Mes Documents (My Documents) : 2/362

~ Mon Bureau (My Desktop) : 10/3382

~ Menu demarrer (Programs) : 1/64

~ Hidden Files: Scanned in 00mn 14s

---\\ Processus lancés

[MD5.BBA22521D24625C7A7B8D57FB20A812E] - (.ATI Technologies Inc. - ATI External Event Utility EXE Module.) -- C:\WINDOWS\system32\Ati2evxx.exe   [405504] [PID.748]

[MD5.FE79366FECD444A16CCA9979134DBEA8] - (.Avira Operations GmbH & Co. KG - Antivirus Host Framework Service.) -- C:\Program Files\Avira\AntiVir Desktop\sched.exe   [440376] [PID.1520]

[MD5.06A1ECB63DF139EC639E084D4AB3C9D7] - (.Hewlett-Packard Company - hpsysdrv.) -- C:\windows\system\hpsysdrv.exe   [52736] [PID.1708]

[MD5.6D21F9202A24B36E7CB10E8ED9F9DE37] - (.VERITAS Software, Inc. - Direct Access Component.) -- C:\WINDOWS\system32\dla\tfswctrl.exe [106549] [PID.1720]

[MD5.2BA1FC996B80F56FFED7CD232F57731E] - (.ATI Technologies, Inc. - ATI Desktop Control Panel.) -- C:\Program Files\ATI Technologies\Panneau de contrôle ATI\atiptaxx.exe [290816] [PID.1760]

[MD5.D40191AA225638AB20E59524CDD74030] - (.THOMSON Telecom Belgium - SpeedTouch Statistics.) -- C:\Program Files\Thomson\SpeedTouch USB\Dragdiag.exe [866816] [PID.1768]

[MD5.5B6E8E09BE6401A7E022F52FDFCB2FF8] - (.Oracle Corporation - Java(TM) Update Scheduler.) -- C:\Program Files\Fichiers communs\Java\Java Update\jusched.exe [254336] [PID.1792]

[MD5.DD231039B13EC2ABDE315D76E658EF0E] - (.Avira Operations GmbH & Co. KG - Antivirus System Tray Tool (Desktop).) -- C:\Program Files\Avira\AntiVir Desktop\avgnt.exe [684600] [PID.1804]

[MD5.E13EA4860E8F2AA845B53BFD2B6FEC5B] - (.Microsoft Corporation - Windows Messenger.) -- C:\Program Files\Messenger\msmsgs.exe [1695232] [PID.1832]

[MD5.D5D8A5E87D3C32C516E5B5E2BA5B0DBF] - (.TomTom - System Tray application for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMERunner.exe [247768] [PID.1840]

[MD5.39FDFD34F7B04290D1BC53E3D6EC7D83] - (.Microsoft® Corporation - Microsoft® Works Calendar Reminder Service.) -- C:\Program Files\Fichiers communs\Microsoft Shared\Works Shared\wkcalrem.exe [24633] [PID.1900]

[MD5.C12EF776375161398861D819139D84C5] - (.Nikon Corporation - Nikon Transfer Monitor.) -- C:\Program Files\Fichiers communs\Nikon\Monitor\NkMonitor.exe [479232] [PID.1948]

[MD5.32C26797AB646074A2BB562F9D10ADB5] - (.Microsoft Corporation - Microsoft Office OneNote Quick Launcher.) -- C:\Program Files\Microsoft Office\Office12\ONENOTEM.exe [97680] [PID.1988]

[MD5.FDE9C7030FB1E9E2715E113EE6A10F90] - (.Avira Operations GmbH & Co. KG - Antivirus Host Framework Service.) -- C:\Program Files\Avira\AntiVir Desktop\avguard.exe [440376] [PID.248]

[MD5.DB5BEA73EDAF19AC68B2C0FAD0F92B1A] - (.Apple Inc. - Bonjour Service.) -- C:\Program Files\Bonjour\mDNSResponder.exe [390504] [PID.264]

[MD5.9D519AAA21E622DF7DF27041E0917499] - (.Pas de propriétaire - DedicarzService.) -- C:\Program Files\Orange\Assistance Livebox\dedicarz\DedicarzService.exe [1966960] [PID.344]

[MD5.EC6A73CD8413F68655E5E0B99C415A21] - (.SEIKO EPSON CORPORATION - EPSON Status Monitor 3.) -- C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40ST7.exe [143872] [PID.392]

[MD5.8FE6AB59CAB8F2C038FEA9522A5EEBA7] - (.SEIKO EPSON CORPORATION - EPSON Status Monitor 3.) -- C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40RP7.exe [113664] [PID.436]

[MD5.C88862F45AC3B447DF50E814BE2F6A13] - (.France Telecom SA - Pas de description.) -- C:\Program Files\Fichiers communs\France Telecom\Shared Modules\FTRTSVC\0\FTRTSVC.exe [65536] [PID.108]

[MD5.80A79264302910C7C24BA7E44267EFEF] - (.Oracle Corporation - Java Quick Starter Service.) -- C:\Program Files\Java\jre7\bin\jqs.exe [182696] [PID.968]

[MD5.F620772888B6E3EDEF5C3E71E3D447F0] - (.TomTom - Windows Service for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe [92632] [PID.2000]

[MD5.6F1E9AB820B3DD8BD38C0190A206205D] - (.Avira Operations GmbH & Co. KG - AntiVir shadow copy service.) -- C:\Program Files\Avira\AntiVir Desktop\avshadow.exe [431672] [PID.3024]

[MD5.29D956C8CB67222D678FAF20D485B25B] - (.Avira Operations GmbH & Co. KG - AntiVir WebGuard Service.) -- C:\Program Files\Avira\AntiVir Desktop\AVWEBGRD.exe [1011768] [PID.3164]

[MD5.7DCE7A74764EB7C67D21A32BC579453D] - (.Oracle Corporation - Java(TM) Update Checker.) -- C:\Program Files\Fichiers communs\Java\Java Update\jucheck.exe [507264] [PID.3256]

[MD5.D9184C5FF3FD526761D518A95ABA74A3] - (.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox.exe [275568] [PID.3704]

[MD5.FF409C974A9AD58B82374DEEF6B44CBB] - (.Mozilla Corporation - Plugin Container for Firefox.) -- C:\Program Files\Mozilla Firefox\plugin-container.exe [18544] [PID.3756]

[MD5.AB44884BC129FC04D75A4649E0710203] - (.Nicolas Coolman - ZHPDiag.) -- C:\Program Files\ZHPDiag\ZHPDiag.exe [8338432] [PID.2560]

~ Processes Running: Scanned in 00mn 01s

---\\ Google Chrome, Démarrage,Recherche,Extensions (G0,G1,G2)

C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\Default\Preferences

~ Google Browser: 0 Legitimates Filtered in 00mn 00s

---\\ Mozilla Firefox, Plugins,Demarrage,Recherche,Extensions (P2,M0,M1,M2,M3)

C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\prefs.js

M2 - MFEP: prefs.js [Propriétaire - cio0qjxf.default\5304cc00-bc6d-40d1-8c6b-457716a1eafc@874ed2aa-e67a-4dd0-9a61-a24d421de244.com] [] Plus-HD-5.7 v (..) =>Adware.PlusHD

M2 - MFEP: prefs.js [Propriétaire - cio0qjxf.default\es-es@dictionaries.addons.mozilla.org] [] Diccionario de EspaÃ±ol/EspaÃ±a v1.7 (..)

M2 - MFEP: prefs.js [Propriétaire - cio0qjxf.default\support@websteroidsapp.com] [] Websteroids v2.6.5367372 (..) =>PUP.TubeDimmer

~ Firefox Browser: 30 Legitimates Filtered in 00mn 00s

---\\ Internet Explorer, Proxy Management (R5)

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = localhost;*.local

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyServer = no key

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyEnable = 0

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,MigrateProxy = 1

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,EnableHttp1_1 = 1

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyHttp1.1 = 1

R5 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,AutoConfigProxy = wininet.dll

~ Proxy management: Scanned in 00mn 00s

---\\ Analyse des lignes F0, F1, F2, F3 - IniFiles, Autoloading programs

F2 - REG:system.ini: USERINIT=C:\WINDOWS\system32\userinit.exe,

F2 - REG:system.ini: Shell=C:\WINDOWS\explorer.exe

F2 - REG:system.ini: VMApplet=rundll32 shell32,Control_RunDLL "sysdm.cpl"

~ Keys: Scanned in 00mn 00s

---\\ Hosts file redirection (O1)

~ Le fichier hosts est sain (The hosts file is clean).

~ Hosts File: Scanned in 00mn 00s

~ Nombre de lignes (Lines number): 20

---\\ Internet Explorer Toolbars (O3)

O3 - Toolbar: EPSON Web-To-Page - [HKLM]{EE5D279F-081B-4404-994D-C6B60AAEBA6D} . (.SEIKO EPSON CORPORATION - EPSON Web-To-Page.) -- C:\Program Files\EPSON\EPSON Web-To-Page\EPSON Web-To-Page.dll

O3 - Toolbar: Easy Photo Print - [HKLM]{9421DD08-935F-4701-A9CA-22DF90AC4EA6} . (.SEIKO EPSON CORPORATION / CyCom Technology - Epson Easy Photo Print (TBL).) -- C:\Program Files\Epson Software\Easy Photo Print\EPTBL.dll

O3 - Toolbar: Avira SearchFree Toolbar - [HKLM]{41564952-412D-5637-4300-7A786E7484D7} . (...) -- (.not file.) =>Toolbar.Avira

O3 - Toolbar: (no name) - [HKCU]{1E796980-9CC5-11D1-A83F-00C04FC99D61} Clé orpheline

O3 - Toolbar\WebBrowser: (no name) - [HKCU]{01E04581-4EEE-11D0-BFE9-00AA005B4383} Clé orpheline

O3 - Toolbar\WebBrowser: (no name) - [HKCU]{0E5CBF21-D15F-11D0-8301-00AA005B4383} Clé orpheline

O3 - Toolbar\WebBrowser: (no name) - [HKCU]{2318C2B1-4965-11D4-9B18-009027A5CD4F} Clé orpheline

O3 - Toolbar\WebBrowser: (no name) - [HKCU]{BDAD1DAD-C946-4A17-ADC1-64B5B4FF55D0} Clé orpheline

O3 - Toolbar\WebBrowser: (no name) - [HKCU]{F2E259E8-0FC8-438C-A6E0-342DD80FA53E} Clé orpheline

O3 - Toolbar\WebBrowser: (no name) - [HKCU]{EE5D279F-081B-4404-994D-C6B60AAEBA6D} Clé orpheline

O3 - Toolbar\WebBrowser: (no name) - [HKCU]{EE2AC4E5-B0B0-4EC6-88A9-BCA1A32AB107} Clé orpheline

~ Toolbar: Scanned in 00mn 00s

---\\ Autres liens utilisateurs (O4)

O4 - GS\Program [AllUsers]: Inkscape (2).lnk . (.inkscape.org - Inkscape.) -- C:\Program Files\Inkscape\inkscape.exe

O4 - GS\Program [AllUsers]: Inkscape.lnk . (.inkscape.org - Inkscape.) -- C:\Program Files\Inkscape\inkscape.exe

O4 - GS\Program [AllUsers]: Installation du Contrôle Parental.lnk . (.InstallShield Software Corporation - InstallShield (R) Setup Launcher.) -- C:\Program Files\Securitoo\Controle Parental\Controle_parental.exe

O4 - GS\Program [AllUsers]: Mozilla Firefox.lnk . (.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox.exe

O4 - GS\Program [AllUsers]: MSN Explorer.lnk . (.Microsoft Corporation - msn.) -- C:\Program Files\MSN\MSNCoreFiles\msn6.exe

O4 - GS\Program [AllUsers]: MSN Messenger 6.2.lnk . (...) -- C:\WINDOWS\Installer\{ABEB838C-A1A7-4C5D-B7E1-8B4314600205}\MsblIco.exe (.not file.)

O4 - GS\Program [AllUsers]: My Software Choice.lnk . (...) -- C:\hp\VINETLINK\VINETLINK.exe

O4 - GS\Program [AllUsers]: Windows Messenger.lnk . (.Microsoft Corporation - Windows Messenger.) -- C:\Program Files\Messenger\msmsgs.exe

O4 - GS\Program [Propriétaire]: Installation du Contrôle Parental.lnk . (.InstallShield Software Corporation - InstallShield (R) Setup Launcher.) -- C:\Program Files\Securitoo\Contrôle Parental\securitoo_controle_parental.exe

O4 - GS\Program [Propriétaire]: Internet Explorer.lnk . (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe

~ Global Startup: 25 Legitimates Filtered in 00mn 00s

---\\ Applications lancées au démarrage du sytème (O4)

O4 - GS\Program [AllUsers]: Microsoft Office.lnk . (.Microsoft Corporation - Microsoft Office XP component.) -- C:\Program Files\Microsoft Office\Office10\OSA.exe =>.Microsoft Corporation

O4 - GS\Program [AllUsers]: Rappels du Calendrier Microsoft Works.lnk . (.Microsoft® Corporation - Microsoft® Works Calendar Reminder Service.) -- C:\Program Files\Fichiers communs\Microsoft Shared\Works Shared\wkcalrem.exe =>.Microsoft Corporation

O4 - GS\Program [Propriétaire]: Nikon Monitor.lnk . (.Nikon Corporation - Nikon Transfer Monitor.) -- C:\Program Files\Fichiers communs\Nikon\Monitor\NkMonitor.exe

O4 - GS\Program [Propriétaire]: OneNote 2007 - Capture d'écran et lancement.lnk . (.Microsoft Corporation - Microsoft Office OneNote Quick Launcher.) -- C:\Program Files\Microsoft Office\Office12\ONENOTEM.exe

O4 - HKLM\..\Run: [hpsysdrv] . (.Hewlett-Packard Company - hpsysdrv.) -- c:\windows\system\hpsysdrv.exe

O4 - HKLM\..\Run: [dla] . (.VERITAS Software, Inc. - Direct Access Component.) -- C:\WINDOWS\system32\dla\tfswctrl.exe

O4 - HKLM\..\Run: [Recguard] . (.Pas de propriétaire - Recguard MFC Application.) -- C:\WINDOWS\SMINST\RECGUARD.exe

O4 - HKLM\..\Run: [ATIPTA] Clé orpheline

O4 - HKLM\..\Run: [SpeedTouch USB Diagnostics] . (.THOMSON Telecom Belgium - SpeedTouch Statistics.) -- C:\Program Files\Thomson\SpeedTouch USB\Dragdiag.exe

O4 - HKLM\..\Run: [QuickTime Task] . (.Apple Inc. - QuickTime Task.) -- C:\Program Files\QuickTime\QTTask.exe

O4 - HKLM\..\Run: [Adobe ARM] . (.Adobe Systems Incorporated - Adobe Reader and Acrobat Manager.) -- C:\Program Files\Fichiers communs\Adobe\ARM\1.0\AdobeARM.exe =>.Adobe Systems Incorporated

O4 - HKLM\..\Run: [SunJavaUpdateSched] . (.Oracle Corporation - Java(TM) Update Scheduler.) -- C:\Program Files\Fichiers communs\Java\Java Update\jusched.exe =>.Oracle Corporation

O4 - HKLM\..\Run: [avgnt] . (.Avira Operations GmbH & Co. KG - Antivirus System Tray Tool (Desktop).) -- C:\Program Files\Avira\AntiVir Desktop\avgnt.exe

O4 - HKCU\..\Run: [EPSON BX300F Series] . (.SEIKO EPSON CORPORATION - EPSON Status Monitor 3.) -- C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FATIEJE.exe =>.Epson Seiko Corporation

O4 - HKCU\..\Run: [ctfmon.exe] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\system32\ctfmon.exe

O4 - HKCU\..\Run: [MSMSGS] . (.Microsoft Corporation - Windows Messenger.) -- C:\Program Files\Messenger\msmsgs.exe

O4 - HKCU\..\Run: [TomTomHOME.exe] . (.TomTom - System Tray application for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMERunner.exe

O4 - HKCU\..\Run: [Microsoft Works Update Detection] c:\Program Files\Microsoft Works\WkDetect.exe (.not file.)

O4 - HKUS\.DEFAULT\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\System32\CTFMON.exe

O4 - HKUS\S-1-5-18\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\System32\CTFMON.exe

O4 - HKUS\S-1-5-19\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\System32\CTFMON.exe

O4 - HKUS\S-1-5-20\..\Run: [CTFMON.EXE] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\System32\CTFMON.exe

O4 - HKUS\.DEFAULT\..\RunOnce: [Suite] regedit -s c:\windows\temp\adj_hp.reg (.not file.)

O4 - HKUS\S-1-5-18\..\RunOnce: [Suite] regedit -s c:\windows\temp\adj_hp.reg (.not file.)

O4 - HKUS\S-1-5-21-1300003180-1421531899-4282951562-1003\..\Run: [EPSON BX300F Series] . (.SEIKO EPSON CORPORATION - EPSON Status Monitor 3.) -- C:\WINDOWS\System32\spool\DRIVERS\W32X86\3\E_FATIEJE.exe =>.Epson Seiko Corporation

O4 - HKUS\S-1-5-21-1300003180-1421531899-4282951562-1003\..\Run: [ctfmon.exe] . (.Microsoft Corporation - CTF Loader.) -- C:\WINDOWS\system32\ctfmon.exe

O4 - HKUS\S-1-5-21-1300003180-1421531899-4282951562-1003\..\Run: [MSMSGS] . (.Microsoft Corporation - Windows Messenger.) -- C:\Program Files\Messenger\msmsgs.exe

O4 - HKUS\S-1-5-21-1300003180-1421531899-4282951562-1003\..\Run: [TomTomHOME.exe] . (.TomTom - System Tray application for TomTom HOME.) -- C:\Program Files\TomTom HOME 2\TomTomHOMERunner.exe

O4 - HKUS\S-1-5-21-1300003180-1421531899-4282951562-1003\..\Run: [Microsoft Works Update Detection] c:\Program Files\Microsoft Works\WkDetect.exe (.not file.)

~ Application: Scanned in 00mn 00s

---\\ Boutons situés sur la barre d'outils principale d'Internet Explorer (O9)

O9 - Extra button: &Envoyer à OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} . (.Microsoft Corporation - Microsoft Office OneNote Internet Explorer Add-in.) -- C:\Program Files\MICROS~3\Office12\ONBttnIE.dll

O9 - Extra button: Uninstall BitDefender Online Scanner v8 - {85d1f590-48f4-11d9-9669-0800200c9a66} -- Clé orpheline

O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} . (...) -- C:\Program Files\Microsoft Office\Office12\REFBARH.ICO

O9 - Extra button: @xpsp3res.dll,-20001 - {e2e2dd38-d088-4134-82b7-f2ba38496583} -- Clé orpheline

O9 - Extra button: Windows Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} . (.Microsoft Corporation - Windows Messenger.) -- C:\Program Files\Messenger\msmsgs.exe

~ IE Extra Buttons: Scanned in 00mn 00s

---\\ Piratage de l'Option 'Rétablir les paramètres Web' (O14)

O14 - IERESET.INF: START_PAGE_URL=START_PAGE_URL=http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome

~ IE Paramètres WEB: Scanned in 00mn 00s

---\\ Objets ActiveX (Downloaded Program Files)(O16)

O16 - DPF: Microsoft XML Parser for Java - (Microsoft XML Parser for Java) - (.not file.) - file:\\C:\WINDOWS\Java\classes\xmldso.cab

O16 - DPF: {4F1E5B1A-2A80-42CA-8532-2D05CB959537} ((no name)) - http://gfx1.hotmail.com/mail/w3/resources/MSNPUpld.cab

O16 - DPF: {5C051655-FCD5-4969-9182-770EA5AA5565} ((no name)) - http://messenger.zone.msn.com/binary/SolitaireShowdown.cab56986.cab

O16 - DPF: {5D86DDB5-BDF9-441B-9E9E-D4730F4EE499} ((no name)) - http://www.zebulon.fr/scan8/oscan8.cab

O16 - DPF: {6414512B-B978-451D-A0D8-FCFDF33E833C} ((no name)) - http://v5.windowsupdate.microsoft.com/v5consumer/V5Controls/en/x86/client/wuweb_site.cab?1106515282013

O16 - DPF: {C3F79A2B-B9B4-4A66-B012-3EE46475B072} ((no name)) - http://messenger.zone.msn.com/binary/MessengerStatsPAClient.cab56907.cab

O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} ((no name)) - http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab

~ Objets ActiveX: Scanned in 00mn 00s

---\\ Modification Domaine/Adresses DNS (O17)

O17 - HKLM\System\CCS\Services\Tcpip\..\{7ADF5062-0AC0-4BB6-96A5-CF3B41539394}: DhcpNameServer = 192.168.1.1 192.168.1.1

O17 - HKLM\System\CCS\Services\Tcpip\..\{B9EE002A-DDD5-43FF-832C-B8C515F1B5FC}: DhcpNameServer = 192.168.1.1

O17 - HKLM\System\CS1\Services\Tcpip\..\{7ADF5062-0AC0-4BB6-96A5-CF3B41539394}: DhcpNameServer = 192.168.1.1 192.168.1.1

O17 - HKLM\System\CS1\Services\Tcpip\..\{B9EE002A-DDD5-43FF-832C-B8C515F1B5FC}: DhcpNameServer = 192.168.1.1

O17 - HKLM\System\CS2\Services\Tcpip\..\{7ADF5062-0AC0-4BB6-96A5-CF3B41539394}: DhcpNameServer = 192.168.1.1 192.168.1.1

O17 - HKLM\System\CS2\Services\Tcpip\..\{B9EE002A-DDD5-43FF-832C-B8C515F1B5FC}: DhcpNameServer = 192.168.1.1

O17 - HKLM\System\CCS\Services\Tcpip\Parameters: DhcpNameServer = 192.168.1.1 192.168.1.1

~ Domain: Scanned in 00mn 00s

---\\ Protocole additionnel (O18)

O18 - Handler: wia - {13F3EA8B-91D7-4F0A-AD76-D2853AC8BECE} . (.Microsoft Corporation - WIA Scripting Layer.) -- C:\WINDOWS\System32\wiascr.dll

O18 - Filter: text/xml - {807563E5-5146-11D5-A672-00B0D022E945} . (.Microsoft Corporation - Microsoft Office XML MIME Filter.) -- C:\Program Files\Fichiers communs\Microsoft Shared\OFFICE12\MSOXMLMF.dll =>.Microsoft Corporation

~ Protocole Additionnel: Scanned in 00mn 00s

---\\ Valeur de Registre AppInit_DLLs et sous-clés Winlogon Notify (autorun) (O20)

O20 - Winlogon Notify: AtiExtEvent . (.ATI Technologies Inc. - ATI External Event Utility DLL Module.) -- C:\WINDOWS\system32\Ati2evxx.dll

O20 - Winlogon Notify: crypt32chain . (.Microsoft Corporation - Crypto API32.) -- C:\WINDOWS\system32\crypt32.dll

O20 - Winlogon Notify: cryptnet . (.Microsoft Corporation - Crypto Network Related API.) -- C:\WINDOWS\system32\cryptnet.dll

O20 - Winlogon Notify: cscdll . (.Microsoft Corporation - Agent réseau hors connexion.) -- C:\WINDOWS\system32\cscdll.dll

O20 - Winlogon Notify: dimsntfy . (.Microsoft Corporation - DIMS Notification Handler.) -- C:\WINDOWS\system32\dimsntfy.dll

O20 - Winlogon Notify: igfxcui . (.Intel Corporation - igfxsrvc Module.) -- C:\WINDOWS\system32\igfxsrvc.dll

O20 - Winlogon Notify: ScCertProp . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\wlnotify.dll

O20 - Winlogon Notify: Schedule . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\wlnotify.dll

O20 - Winlogon Notify: sclgntfy . (.Microsoft Corporation - DLL secondaire de notification de service d.) -- C:\WINDOWS\system32\sclgntfy.dll

O20 - Winlogon Notify: SensLogn . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\WlNotify.dll

O20 - Winlogon Notify: termsrv . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\wlnotify.dll

O20 - Winlogon Notify: wlballoon . (.Microsoft Corporation - DLL commune de réception des notifications.) -- C:\WINDOWS\system32\wlnotify.dll

~ Winlogon: Scanned in 00mn 00s

---\\ Liste des services NT non Microsoft et non désactivés (O23)

O23 - Service: Dedicarz Service (Dedicarz Service) . (.Pas de propriétaire - DedicarzService.) - C:\Program Files\Orange\Assistance Livebox\dedicarz\DedicarzService.exe

O23 - Service: TomTomHOMEService (TomTomHOMEService) . (.TomTom - Windows Service for TomTom HOME.) - C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe

~ Services: 15 Legitimates Filtered in 00mn 06s

---\\ Enumération Active Desktop & MHTML Editor (O24)

O24 - Desktop General: BackupWallPaper - .(...) - C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Microsoft\Wallpaper1.bmp

O24 - Desktop General: WallPaper - .(...) - C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Microsoft\Wallpaper1.bmp

~ Desktop Component: 4 Legitimates Filtered in 00mn 00s

---\\ Logiciels installés (O42)

O42 - Logiciel: About Font - (...) [HKLM] -- About Font

O42 - Logiciel: HSP56 World MicroModem Drivers - (...) [HKLM] -- Installing HSP56 MicroModem Drivers

O42 - Logiciel: MyDVD - (...) [HKLM] -- {5E835305-63BB-4E55-BBB7-EEBBE67774DB}

O42 - Logiciel: PhotoImpression - (...) [HKLM] -- {EFF8A42A-0814-4864-92D7-52EFB3048ABD}

O42 - Logiciel: S3Display - (...) [HKLM] -- S3Display

O42 - Logiciel: S3Gamma2 - (...) [HKLM] -- S3Gamma2

O42 - Logiciel: S3Info2 - (...) [HKLM] -- S3Info2

O42 - Logiciel: S3Overlay - (...) [HKLM] -- S3Overlay

O42 - Logiciel: Symbols (remove only) - (...) [HKLM] -- Symbols

~ Logic: 46 Legitimates Filtered in 00mn 01s

---\\ HKCU & HKLM Software Keys

[HKCU\Software\APN]

[HKCU\Software\AskPartnerNetwork]

[HKCU\Software\In Poculis]

[HKCU\Software\IncrediMail]

[HKCU\Software\Max2k]

[HKCU\Software\TraumaStudios]

[HKCU\Software\Vocabelum Inc]

[HKLM\Software\APN]

[HKLM\Software\Action]

[HKLM\Software\AskPartnerNetwork]

[HKLM\Software\IncrediMail]

[HKLM\Software\libiconv]

~ Key Software: 389 Legitimates Filtered in 00mn 01s

---\\ Contenu des dossiers Programs/ProgramFiles/ProgramData/AppData (O43)

O43 - CFD: 17/06/2010 - 17:40:45 - [2,625] ----D C:\Program Files\About Font

O43 - CFD: 07/02/2014 - 12:05:48 - [3,997] ----D C:\Program Files\AskPartnerNetwork

O43 - CFD: 01/01/2002 - 16:46:53 - [2,727] ----D C:\Program Files\DLA

O43 - CFD: 19/09/2009 - 19:10:59 - [0] ----D C:\Program Files\Elements Interactive

O43 - CFD: 16/09/2005 - 20:42:39 - [0,060] ----D C:\Program Files\fdjeux

O43 - CFD: 25/01/2005 - 20:00:56 - [0,452] ----D C:\Program Files\google toolbar =>Toolbar.Google

O43 - CFD: 01/01/2002 - 16:55:46 - [0] ----D C:\Program Files\Home Media Networks Limited

O43 - CFD: 31/08/2009 - 18:17:38 - [4,256] ----D C:\Program Files\incredimail

O43 - CFD: 05/05/2009 - 08:24:52 - [0,373] ----D C:\Program Files\Max2k

O43 - CFD: 29/01/2005 - 09:09:51 - [9,298] ----D C:\Program Files\real player

O43 - CFD: 21/09/2009 - 07:58:42 - [35,609] ----D C:\Program Files\TeachMe Version 4

O43 - CFD: 07/02/2014 - 12:03:48 - [0] ----D C:\Documents and Settings\All Users\Application Data\APN

O43 - CFD: 07/02/2014 - 12:05:48 - [1,179] ----D C:\Documents and Settings\All Users\Application Data\AskPartnerNetwork

O43 - CFD: 10/01/2014 - 19:16:09 - [0] ----D C:\Documents and Settings\All Users\Application Data\T1 Games

O43 - CFD: 07/02/2014 - 23:26:26 - [0] ----D C:\Documents and Settings\All Users\Application Data\Updater =>PUP.CrossRider

O43 - CFD: 17/07/2006 - 22:44:18 - [0] ----D C:\Documents and Settings\Propriétaire\Application Data\eConf

O43 - CFD: 18/01/2012 - 18:51:53 - [0,003] ----D C:\Documents and Settings\Propriétaire\Application Data\JQ

O43 - CFD: 10/01/2014 - 19:16:09 - [0,004] ----D C:\Documents and Settings\Propriétaire\Application Data\T1 Games

O43 - CFD: 16/02/2005 - 20:58:06 - [122,381] ----D C:\Documents and Settings\Propriétaire\Local Settings\Application Data\IM

O43 - CFD: 05/05/2009 - 07:53:58 - [0,001] ----D C:\Documents and Settings\Propriétaire\Menu Démarrer\Programmes\About Font

O43 - CFD: 05/05/2009 - 08:24:52 - [0,006] ----D C:\Documents and Settings\Propriétaire\Menu Démarrer\Programmes\Symbols

~ Program Folder: 269 Legitimates Filtered in 00mn 59s

---\\ Derniers fichiers modifiés ou crées sous Windows et System32 (O44)

O44 - LFC:[MD5.C17B50CE5F20D7A23761F5501AAAD039] - 13/02/2014 - 21:00:11 ---A- . (...) -- C:\WINDOWS\imsins.BAK [1374]

O44 - LFC:[MD5.858DFC11C9B915926EE0BB6892281F27] - 13/02/2014 - 21:14:49 ---A- . (...) -- C:\WINDOWS\updspapi.log [3669]

O44 - LFC:[MD5.A443F4C066EF203D31BE0CF633AC5ED4] - 13/02/2014 - 21:14:51 ---A- . (...) -- C:\WINDOWS\FaxSetup.log [18476]

O44 - LFC:[MD5.599869CFFA320AD5FAAE75940FA90EF2] - 13/02/2014 - 21:14:51 ---A- . (...) -- C:\WINDOWS\msgsocm.log [927]

O44 - LFC:[MD5.0B7ADFF169707DA105CEB0ED8E7B8188] - 13/02/2014 - 21:14:51 ---A- . (...) -- C:\WINDOWS\ocgen.log [8868]

O44 - LFC:[MD5.39152F969D6A5AE47AB82B5289218740] - 13/02/2014 - 21:14:52 ---A- . (...) -- C:\WINDOWS\comsetup.log [6130]

O44 - LFC:[MD5.5DCC6269472073F9337777ECB581EEA0] - 13/02/2014 - 21:14:52 ---A- . (...) -- C:\WINDOWS\iis6.log [2952]

O44 - LFC:[MD5.B32E37834942C9167E8F0D23CD264BFB] - 13/02/2014 - 21:14:52 ---A- . (...) -- C:\WINDOWS\imsins.log [1374]

O44 - LFC:[MD5.51A1567E43E46F26DFFC5775A762123A] - 13/02/2014 - 21:14:52 ---A- . (...) -- C:\WINDOWS\ntdtcsetup.log [3723]

O44 - LFC:[MD5.28FF64679160F4D363D392607B9A79A1] - 13/02/2014 - 21:14:52 ---A- . (...) -- C:\WINDOWS\ocmsn.log [1026]

O44 - LFC:[MD5.82F171847974085243EBC8EBBB24ADE5] - 13/02/2014 - 21:14:52 ---A- . (...) -- C:\WINDOWS\tsoc.log [7077]

O44 - LFC:[MD5.F69408CEFE70C14C05C5B3001DDCFB7D] - 19/02/2014 - 11:35:26 ---A- . (...) -- C:\WINDOWS\wiaservc.log [50]

O44 - LFC:[MD5.AD800F90A445019C182C4E96BCE7847B] - 19/02/2014 - 11:35:42 ---A- . (...) -- C:\WINDOWS\ModemLog_HSP56 World MicroModem.txt [4958]

O44 - LFC:[MD5.33D1091FCC4904A3CBE005A62FD200EB] - 19/02/2014 - 11:36:04 ---A- . (...) -- C:\WINDOWS\wiadebug.log [159]

~ Files: 58 Legitimates Filtered in 00mn 11s

---\\ Derniers fichiers créés dans Windows Prefetcher (O45)

O45 - LFCP:[MD5.9DE7CAD1F1C41C144FFC5938B596DBF7] - 13/02/2014 - 20:33:22 ---A- - C:\WINDOWS\Prefetch\ATLANTIS.EXE-17C403D3.pf

O45 - LFCP:[MD5.AC545B0AA40893AB4A057692579E9E6D] - 16/02/2014 - 09:02:47 ---A- - C:\WINDOWS\Prefetch\NSF.TMP-398E6167.pf

~ Prefetcher: 83 Legitimates Filtered in 00mn 00s

---\\ Opérations et fonctions au démarrage de Windows Explorer (O46)

O46 - SEH:ShellExecuteHooks - URL Exec Hook - {AEB6717E-7E19-11d0-97EE-00C04FD91972} - shell32.dll

~ ShellExecuteHooks: Scanned in 00mn 00s

---\\ Export de clé d'application autorisée (O47)

O47 - AAKE:Key Export SP - "C:\Program Files\incredimail\bin\IMApp.exe" [Enabled] .(...) -- C:\Program Files\incredimail\bin\IMApp.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\Program Files\incredimail\bin\IncMail.exe" [Enabled] .(...) -- C:\Program Files\incredimail\bin\IncMail.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\Program Files\incredimail\bin\ImpCnt.exe" [Enabled] .(...) -- C:\Program Files\incredimail\bin\ImpCnt.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\Program Files\JVTorrent\btdownloadgui.exe" [Enabled] .(...) -- C:\Program Files\JVTorrent\btdownloadgui.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\Sierra\Empire Earth\Empire Earth.exe" [Disabled] .(...) -- C:\Sierra\Empire Earth\Empire Earth.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\Program Files\Orange Link\Application\Exe\Orange Link.exe" [Enabled] .(...) -- C:\Program Files\Orange Link\Application\exe\Orange Link.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\Program Files\Orange Link\Application\eConfv4\olinkp.exe" [Enabled] .(...) -- C:\Program Files\Orange Link\Application\eConfv4\olinkp.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\Program Files\hp center\137903\Program\BackWeb-137903.exe" [Enabled] .(...) -- C:\Program Files\hp center\137903\Program\BackWeb-137903.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\WINDOWS\system32\dmwu.exe" [Enabled] .(...) -- C:\WINDOWS\system32\dmwu.exe (.not file.)

O47 - AAKE:Key Export SP - "C:\Program Files\orange\Assistance Livebox\dedicarz\DedicarzService.exe" [Enabled] .(..) -- C:\Program Files\orange\Assistance Livebox\dedicarz\DedicarzService.exe

O47 - AAKE:Key Export SP - "C:\Program Files\orange\Assistance Livebox\dedicarz\LiveboxManager.exe" [Enabled] .(.Pas de propriétaire.) -- C:\Program Files\orange\Assistance Livebox\dedicarz\LiveboxManager.exe

O47 - AAKE:Key Export SP - "C:\Program Files\orange\Assistance Livebox\dedicarz\PluginLivebox.exe" [Enabled] .(.Pas de propriétaire.) -- C:\Program Files\orange\Assistance Livebox\dedicarz\PluginLivebox.exe

~ Keys Export: 31 Legitimates Filtered in 00mn 00s

---\\ Image File Execution Options (IFEO) (O50)

O50 - IFEO:Image File Execution Options - Your Image File Name Here without a path - ntsd -d

~ IFEO: Scanned in 00mn 00s

---\\ Clé de registre Shell MountPoints2 (MPKS) (O51)

O51 - MPSK:{4eb0d569-d809-11dd-acdb-0040ca3b2ec8}\AutoRun\command. (...) -- H:\InstallTomTomHOME.exe (.not file.)

O51 - MPSK:{76e60fbf-37c2-11e3-b4a9-0040ca3b2ec8}\AutoRun\command. (...) -- I:\AutoRun.exe (.not file.)

~ Keys: Scanned in 00mn 00s

---\\ Liste des pilotes du système (SDL) (O58)

O58 - SDL:[MD5.8058DAA7CAEF5499FC2909F3F2B2EFBF] - 22/05/2002 - 19:44:14 ---A- . (...) -- C:\WINDOWS\system32\Drivers\a312.sys [9785]

O58 - SDL:[MD5.627909FDC8ED535E903FBB2F889DBC16] - 22/06/2002 - 02:29:30 ---A- . (.Avance Logic, Inc. - Avance AC'97 Audio Driver (WDM).) -- C:\WINDOWS\system32\Drivers\ALCXWDM.SYS [656172]

O58 - SDL:[MD5.C9B25AE9B8ABD983C5AD3F8CBFAB0F9C] - 28/08/2001 - 20:00:00 ---A- . (.RAVISENT Technologies Inc. - Pilote principal CineMaster C 1.2 WDM.) -- C:\WINDOWS\system32\Drivers\cinemst2.sys [262528]

O58 - SDL:[MD5.3CE6611C4F87FCE85EB9569B2CBB0945] - 17/08/2001 - 20:19:30 ---A- . (.Crystal Semiconductor Corp. - Crystal WDM OS Driver.) -- C:\WINDOWS\system32\Drivers\cwcos.sys [3584]

O58 - SDL:[MD5.798DDEC7FC30464F8CB6521122BEAD05] - 17/08/2001 - 20:19:36 ---A- . (.Crystal Semiconductor Corp. - Crystal PCI WDM Audio Driver.) -- C:\WINDOWS\system32\Drivers\cwcspud.sys [111872]

O58 - SDL:[MD5.A53A331CDA2434A9CB421C3D1717A8D2] - 18/12/2002 - 12:22:26 ---A- . (.Crystal Semiconductor Corp. - Crystal PCI WDM Audio Driver.) -- C:\WINDOWS\system32\Drivers\cwcwdm.sys [94976]

O58 - SDL:[MD5.573C7D0A32852B48F3058CFD8026F511] - 13/04/2008 - 17:36:05 ----- . (.Windows (R) Server 2003 DDK provider - High Definition Audio Bus Driver v1.0a.) -- C:\WINDOWS\system32\Drivers\hdaudbus.sys [144384]

O58 - SDL:[MD5.C4AA89518E8A2934EAF503C9587FF157] - 08/03/2002 - 21:40:10 ---A- . (.Padus, Inc. - Padus(R) ASPI Shell.) -- C:\WINDOWS\system32\Drivers\pfc.sys [13780]

O58 - SDL:[MD5.80D317BD1C3DBC5D4FE7B1678C60CADD] - 28/08/2001 - 13:00:00 ---A- . (.Parallel Technologies, Inc. - Parallel Technologies DirectParallel IO Library.) -- C:\WINDOWS\system32\Drivers\ptilink.sys [17792]

O58 - SDL:[MD5.327498102BB919DE86E53CA45630DA4A] - 05/06/2002 - 04:38:14 ---A- . (.PCTEL, INC. - HSP Modem Serial Device Driver for NT 5.0.) -- C:\WINDOWS\system32\Drivers\ptserial.sys [138160]

O58 - SDL:[MD5.A36EE93698802CD899F98BFD553D8185] - 13/12/2013 - 15:03:37 ---A- . (.Avira GmbH - AVIRA SnapShot Driver.) -- C:\WINDOWS\system32\Drivers\ssmdrv.sys [28520]

O58 - SDL:[MD5.F92254B0BCFCD10CAAC7BCCC7CB7F467] - 12/11/2009 - 13:48:56 ---A- . (...) -- C:\WINDOWS\system32\Drivers\StarOpen.sys [7168]

O58 - SDL:[MD5.55E01061C74A8CEFFF58DC36114A8D3F] - 28/08/2001 - 20:00:00 ---A- . (.RAVISENT Technologies Inc. - CineMaster C WDM DVD Minidriver.) -- C:\WINDOWS\system32\Drivers\vdmindvd.sys [58112]

O58 - SDL:[MD5.2AC2225577904F690AAEBDA696906395] - 05/06/2002 - 04:37:18 ---A- . (.PCTEL, INC. - HSP Modem Modem Device Driver.) -- C:\WINDOWS\system32\Drivers\vmodem.sys [633533]

O58 - SDL:[MD5.67C8234D1B08E67B0D285D00C3B953DE] - 05/06/2002 - 04:56:38 ---A- . (.PCTEL, INC. - HSP Modem Controller Device Driver.) -- C:\WINDOWS\system32\Drivers\vpctcom.sys [396458]

O58 - SDL:[MD5.2EA58AFCEA43FA85169C291E886296BF] - 05/06/2002 - 04:37:44 ---A- . (.PCtel, Inc. - HSP Modem device driver.) -- C:\WINDOWS\system32\Drivers\vvoice.sys [65342]

O58 - SDL:[MD5.6D3ADA4CE95CECA7BCE527A08C4C474E] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\ansi.sys [9037]

O58 - SDL:[MD5.0FE9F16075C9ACB941C957B7C649176E] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\country.sys [27097]

O58 - SDL:[MD5.C6D29F29DE7427B1B0775E53E577B623] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\himem.sys [4912]

O58 - SDL:[MD5.582BCDD47CF4B68B5CB528F18E3CB808] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\key01.sys [42809]

O58 - SDL:[MD5.FBBCFEC1379C5C02D88A361993EDF1B8] - 04/08/2004 - 06:46:54 ---A- . (...) -- C:\WINDOWS\system32\keyboard.sys [42537]

O58 - SDL:[MD5.7D30A74B5FB9FE3B245A6CE5FBCD71D5] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\ntdos.sys [27916]

O58 - SDL:[MD5.CF9ED169FF86D935E47999E82359E898] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\ntdos404.sys [29146]

O58 - SDL:[MD5.03B945AC0481CD8BB161C3569D8ED1C3] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\ntdos411.sys [29370]

O58 - SDL:[MD5.BBC957DC18C17CC027EB80B7C77F2AEA] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\ntdos412.sys [29274]

O58 - SDL:[MD5.3CFFAEFFF23B0D208214A6D3061A5B1B] - 28/08/2001 - 13:00:00 ---A- . (...) -- C:\WINDOWS\system32\ntdos804.sys [29146]

O58 - SDL:[MD5.CAAA108FD7BF71989946B39704323455] - 17/05/2004 - 23:43:15 ---A- . (...) -- C:\WINDOWS\system32\ntio.sys [34000]

O58 - SDL:[MD5.6F73F50162DEF60C84B725C18CD9140F] - 17/05/2004 - 23:43:07 ---A- . (...) -- C:\WINDOWS\system32\ntio404.sys [34560]

O58 - SDL:[MD5.0FDD5E69C1FF3B58043D44F2CC743D45] - 17/05/2004 - 23:43:04 ---A- . (...) -- C:\WINDOWS\system32\ntio411.sys [35648]

O58 - SDL:[MD5.8842837C4D8311BF8E72BEE8CCC42217] - 17/05/2004 - 23:43:09 ---A- . (...) -- C:\WINDOWS\system32\ntio412.sys [35424]

O58 - SDL:[MD5.6B56CEB3C6F9D5CD7293DBD9FE23B311] - 17/05/2004 - 23:43:06 ---A- . (...) -- C:\WINDOWS\system32\ntio804.sys [34560]

~ Drivers: 5 Legitimates Filtered in 00mn 05s

---\\ Derniers fichiers modifiés ou crées (Utilisateur) (O61)

O61 - LFC: 16/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Crash Reports\InstallTime20140212131424 [10]

O61 - LFC: 16/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\bookmarkbackups\bookmarks-2014-02-16_190.json [91496]

O61 - LFC: 16/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\search.json [19816]

O61 - LFC: 16/02/2014 - 12:20:51 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Mozilla\Firefox\Mozilla Firefox\active-update.xml [57]

O61 - LFC: 16/02/2014 - 12:20:51 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Mozilla\Firefox\Mozilla Firefox\updates.xml [14851]

O61 - LFC: 16/02/2014 - 12:20:52 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Recent\Mamie Rectif.lnk [1051]

O61 - LFC: 16/02/2014 - 12:20:52 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Recent\Photos prises par Chloé.lnk [714]

O61 - LFC: 17/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\bookmarkbackups\bookmarks-2014-02-17_190.json [91496]

O61 - LFC: 17/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\content-prefs.sqlite [15360]

O61 - LFC: 17/02/2014 - 12:20:52 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Recent\Facture Anne JACOLOT - Mois de Fev 2014 (2).lnk [533]

O61 - LFC: 17/02/2014 - 12:20:52 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Recent\Facture Anne JACOLOT - Mois de Fev 2014.lnk [536]

O61 - LFC: 17/02/2014 - 12:20:52 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Recent\Factures Février 2014.lnk [301]

O61 - LFC: 18/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\addons.json [12310]

O61 - LFC: 18/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\blocklist.xml [112813]

O61 - LFC: 18/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\bookmarkbackups\bookmarks-2014-02-18_190.json [91496]

O61 - LFC: 18/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\healthreport.sqlite [1146880]

O61 - LFC: 18/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\local_2.db [79]

O61 - LFC: 18/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\sessionstart.sl [30]

O61 - LFC: 18/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\signons.sqlite [45056]

O61 - LFC: 19/02/2014 - 12:20:40 -SHA- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Microsoft\Credentials\S-1-5-21-1300003180-1421531899-4282951562-1003\Credentials [1292]

O61 - LFC: 19/02/2014 - 12:20:42 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Microsoft\Templates\Normal.dotm [737569]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\bookmarkbackups\bookmarks-2014-02-19_190.json [91496]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\cert8.db [376832]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\cookies.sqlite [524288]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\cookies.sqlite-shm [32768]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\cookies.sqlite-wal [590288]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\extensions.json [43055]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\formhistory.sqlite [273408]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\healthreport.sqlite-shm [32768]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\healthreport.sqlite-wal [0]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\key3.db [16384]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\localstore.rdf [15286]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\permissions.sqlite [40960]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\places.sqlite [20971520]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\places.sqlite-shm [32768]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\places.sqlite-wal [296672]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\prefs.js [145508]

O61 - LFC: 19/02/2014 - 12:20:43 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\sessionstore.bak [85177]

O61 - LFC: 19/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\sessionstore.js [6375]

O61 - LFC: 19/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\storage\persistent\chrome\idb\2948351385b3d0l4acncr0e0t-nbic.sqlite [524288]

O61 - LFC: 19/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\urlclassifierkey3.txt [154]

O61 - LFC: 19/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\webapps\webapps.json [2]

O61 - LFC: 19/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\webappsstore.sqlite [1459200]

O61 - LFC: 19/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\webappsstore.sqlite-shm [32768]

O61 - LFC: 19/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\webappsstore.sqlite-wal [19944]

O61 - LFC: 19/02/2014 - 12:20:44 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\win_2.db [48]

O61 - LFC: 19/02/2014 - 12:20:45 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\ZHP\Log.txt [21898] =>.Nicolas Coolman

O61 - LFC: 19/02/2014 - 12:20:45 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Application Data\ZHP\TestsZHPDiag.txt [3469] =>.Nicolas Coolman

O61 - LFC: 19/02/2014 - 12:20:45 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Bureau\ZHPDiag.lnk [1534] =>.Nicolas Coolman

O61 - LFC: 19/02/2014 - 12:20:45 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Bureau\ZHPFix.lnk [1639] =>.Nicolas Coolman

O61 - LFC: 19/02/2014 - 12:20:46 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Google\Chrome\User Data\default\preferences [55]

O61 - LFC: 19/02/2014 - 12:20:46 -SHA- . (...) -- C:\Documents and Settings\Propriétaire\IETldCache\index.dat [262144]

O61 - LFC: 19/02/2014 - 12:20:48 -SHA- . (...) -- C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Microsoft\Credentials\S-1-5-21-1300003180-1421531899-4282951562-1003\Credentials [5226]

O61 - LFC: 19/02/2014 - 12:20:51 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default_CACHE_CLEAN_ [1]

O61 - LFC: 19/02/2014 - 12:20:51 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Local Settings\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\startupCache\startupCache.4.little [78698]

O61 - LFC: 19/02/2014 - 12:20:52 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Mes documents\Téléchargements\adwcleaner.exe [1241834]

O61 - LFC: 19/02/2014 - 12:20:52 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Recent\Normal.lnk [1112]

O61 - LFC: 19/02/2014 - 12:20:52 ---A- . (...) -- C:\Documents and Settings\Propriétaire\Recent\Templates.lnk [850]

~ 6 Fichiers temporaires (Temporary files)

~ 2 Fichiers cookies (Cookies files)

~ Files: 125 Legitimates Filtered in 00mn 12s

---\\ Liste des outils de désinfection (LATC) (O63)

O63 - Logiciel: ZHPDiag 2014 - (.Nicolas Coolman.) [HKLM] -- ZHPDiag_is1 =>.Nicolas Coolman

~ ADS: Scanned in 00mn 00s

---\\ Liste les services legacy du registre (LALS) (O64)

O64 - Services: CurCS - 17/09/2013 - C:\Program Files\Orange\Assistance Livebox\dedicarz\DedicarzService.exe (Dedicarz Service) .(.Pas de propriétaire - DedicarzService.) - LEGACY_DEDICARZ_SERVICE

O64 - Services: CurCS - 05/06/2002 - C:\WINDOWS\system32\DRIVERS\vmodem.sys (Vmodem) .(.PCTEL, INC. - HSP Modem Modem Device Driver.) - LEGACY_VMODEM

O64 - Services: CurCS - 05/06/2002 - C:\WINDOWS\system32\DRIVERS\vpctcom.sys (Vpctcom) .(.PCTEL, INC. - HSP Modem Controller Device Driver.) - LEGACY_VPCTCOM

O64 - Services: CurCS - 05/06/2002 - C:\WINDOWS\system32\DRIVERS\vvoice.sys (Vvoice) .(.PCtel, Inc. - HSP Modem device driver.) - LEGACY_VVOICE

~ Legacy: 194 Legitimates Filtered in 00mn 00s

---\\ Menu de démarrage Internet (SMI) (O68)

O68 - StartMenuInternet: <FIREFOX.EXE> <Mozilla Firefox>[HKLM\..\Shell\open\Command] (.Mozilla Corporation - Firefox.) -- C:\Program Files\Mozilla Firefox\firefox.exe

O68 - StartMenuInternet: <IEXPLORE.EXE> <Internet Explorer>[HKLM\..\Shell\open\Command] (.Microsoft Corporation - Internet Explorer.) -- C:\Program Files\Internet Explorer\iexplore.exe

O68 - StartMenuInternet: <Launcher.exe> <>[HKLM\..\Shell\open\Command] (.Not Key.)

O68 - StartMenuInternet: <MSN Explorer> <>[HKLM\..\Shell\open\Command] (.Microsoft Corporation - msn.) -- C:\Program Files\MSN\MSNCoreFiles\MSN6.exe

O68 - StartMenuInternet: <WOOBrowser.exe> <>[HKLM\..\Shell\open\Command] (...) -- C:\Program Files\Wanadoo\WOOBrowser\WOOBrowser.exe (.not file.)

~ Keys: Scanned in 00mn 00s

---\\ Recherche d'infection sur les navigateurs internet (SBI) (O69)

O69 - SBI: SearchScopes [HKCU] ${searchCLSID} - (@ieframe.dll,-12512) - http://search.live.com

O69 - SBI: SearchScopes [HKCU] {0633EE93-D776-472f-A0FF-E1416B8B2E3A} - (Bing) - http://www.bing.com

O69 - SBI: SearchScopes [HKCU] {0F63006E-D173-437C-B143-83CB56AF6FA2} - (Google) - http://www.google.com

O69 - SBI: SearchScopes [HKCU] {423AF60D-24CA-4BAD-B501-40FE1B0B9FCE} - (Ask Search) - http://websearch.ask.com =>Toolbar.Ask

O69 - SBI: SearchScopes [HKCU] {814C76CB-2623-43F4-AAD0-58A0E5190A20} - (Orange) - http://r.orange.fr

O69 - SBI: SearchScopes [HKCU] {B2EB4093-DE29-44B5-96D1-D906B6FAE0DE} - (Search By ZoneAlarm) - http://search.zonealarm.com

O69 - SBI: SearchScopes [HKUS\.DEFAULT] {F955CDA0-20C4-477F-AEC9-4398AABBA672} - (Ask Search) - http://websearch.ask.com =>Toolbar.Ask

O69 - SBI: SearchScopes [HKUS\S-1-5-18] {F955CDA0-20C4-477F-AEC9-4398AABBA672} - (Ask Search) - http://websearch.ask.com =>Toolbar.Ask

~ Keys: Scanned in 00mn 00s

---\\ Recherche particulière à la racine du système (SPRF) (O84)

[MD5.54DB2B8C60F04C5ADE6D711D47EABA75] [SPRF][07/02/2014] (...) -- C:\Documents and Settings\Propriétaire\Bureau\adwcleaner.exe   [1166132]

[MD5.DEA1BE9A2652D883AECC4F5E9266C3E8] [SPRF][13/03/2012] (.Agence JURIS - Pas de description.) -- C:\Documents and Settings\Propriétaire\Bureau\amortissements.exe   [69632]

[MD5.E42FBFE616264106AEAAEC502033FBE0] [SPRF][11/02/2014] (...) -- C:\Documents and Settings\Propriétaire\Bureau\free-mahjong-game-in-poculis.exe   [15925528]

[MD5.E42FBFE616264106AEAAEC502033FBE0] [SPRF][11/02/2014] (...) -- C:\Documents and Settings\Propriétaire\Bureau\free-mahjong-game-in-poculis[1].exe   [15925528]

[MD5.389E4A5A670B1080F236068D71E08784] [SPRF][28/03/2010] (...) -- C:\Documents and Settings\Propriétaire\Bureau\photofiltre_photofiltre_6.4.0_francais_10731.exe   [1804644]

[MD5.18075B2C9F0F300BEE209744A8BEC353] [SPRF][07/12/2004] (...) -- C:\WINDOWS\Downloaded Program Files\bdcore.dll   [32]

[MD5.298068536300DA6DC163E394797A7C50] [SPRF][25/05/2006] (...) -- C:\WINDOWS\Downloaded Program Files\bdupd.dll   [118784]

[MD5.1CAB87DE6638846FBF51F32B5D95E482] [SPRF][25/05/2006] (...) -- C:\WINDOWS\Downloaded Program Files\ipsupd.dll   [53248]

[MD5.18075B2C9F0F300BEE209744A8BEC353] [SPRF][07/12/2004] (...) -- C:\WINDOWS\Downloaded Program Files\libfn.dll   [32]

~ Files: 16 Legitimates Filtered in 00mn 08s

---\\ Enumère les codes produits des logiciels (PUC) (O90)

O90 - PUC: "25946514D214736534007A857BC0A000" . (.Avira SearchFree Toolbar.) -- C:\WINDOWS\Installer\{41564952-412D-5637-4300-A758B70C0A00}\ToolbarIcon.exe =>Toolbar.Avira

~ Update Products: 70 Legitimates Filtered in 00mn 00s

---\\ Etat général des services non Microsoft (EGS) (SR=Running, SS=Stopped)

SS - | Demand 07/02/2014 257928 | (AdobeFlashPlayerUpdateSvc) . (.Adobe Systems Incorporated.) - C:\WINDOWS\system32\Macromed\Flash\FlashPlayerUpdateService.exe

SS - | Demand 14/04/2008 225280 | (dmadmin) . (.Microsoft Corp., Veritas Software.) - C:\WINDOWS\system32\dmadmin.exe

SS - | Auto 29/07/2010 136176 | (gupdate) . (.Google Inc..) - C:\Program Files\Google\Update\GoogleUpdate.exe

SS - | Demand 29/07/2010 136176 | (gupdatem) . (.Google Inc..) - C:\Program Files\Google\Update\GoogleUpdate.exe

SS - | Auto 20/09/2011 194104 | (gusvc) . (.Google.) - C:\Program Files\Google\Common\Google Updater\GoogleUpdaterService.exe

SS - | Demand 04/04/2005 69632 | (IDriverT) . (.Macrovision Corporation.) - C:\Program Files\Fichiers communs\InstallShield\Driver\11\Intel 32\IDriverT.exe

SS - | Demand 15/02/2014 118896 | (MozillaMaintenance) . (.Mozilla Foundation.) - C:\Program Files\Mozilla Maintenance Service\maintenanceservice.exe

SS - | Demand 04/03/2010 71096 | (NMSAccess) . (...) - C:\Program Files\CDBurnerXP\NMSAccessU.exe

SS - | Auto 25/03/2002 61440 | (NVSvc) . (.NVIDIA Corporation.) - C:\WINDOWS\system32\nvsvc32.exe

SS - | Auto 29/08/2013 1073160 | (Orange update Core Service) . (.Orange SA.) - C:\Program Files\Orange\OrangeUpdate\Service\OUCore.exe

SR - | Auto 13/12/2013 440376 | (AntiVirSchedulerService) . (.Avira Operations GmbH & Co. KG.) - C:\Program Files\Avira\AntiVir Desktop\sched.exe

SR - | Auto 13/12/2013 440376 | (AntiVirService) . (.Avira Operations GmbH & Co. KG.) - C:\Program Files\Avira\AntiVir Desktop\avguard.exe

SR - | Auto 13/12/2013 1011768 | (AntiVirWebService) . (.Avira Operations GmbH & Co. KG.) - C:\Program Files\Avira\AntiVir Desktop\AVWEBGRD.exe

SR - | Auto 21/02/2006 405504 | (Ati HotKey Poller) . (.ATI Technologies Inc..) - C:\WINDOWS\system32\Ati2evxx.exe

SR - | Auto 30/08/2011 390504 | (Bonjour Service) . (.Apple Inc..) - C:\Program Files\Bonjour\mDNSResponder.exe

SR - | Auto 17/09/2013 1966960 | (Dedicarz Service) . (...) - C:\Program Files\Orange\Assistance Livebox\dedicarz\DedicarzService.exe

SR - | Auto 17/12/2007 143872 | (EPSON_EB_RPCV4_01) . (.SEIKO EPSON CORPORATION.) - C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40ST7.exe

SR - | Auto 11/01/2007 113664 | (EPSON_PM_RPCV4_01) . (.SEIKO EPSON CORPORATION.) - C:\Documents and Settings\All Users\Application Data\EPSON\EPW!3 SSRP\E_S40RP7.exe

SR - | Auto 11/12/2007 65536 | C:\Program Files\FICHIE~1\France Telecom\Shared Modules\FTRTSVC\0\FTRTSVC.exe (FTRTSVC) . (.France Telecom SA.) - C:\Program Files\Fichiers communs\France Telecom\Shared Modules\FTRTSVC\0\FTRTSVC.exe

SR - | Auto 08/10/2013 182696 | (JavaQuickStarterService) . (.Oracle Corporation.) - C:\Program Files\Java\jre7\bin\jqs.exe

SR - | Auto 05/12/2012 92632 | (TomTomHOMEService) . (.TomTom.) - C:\Program Files\TomTom HOME 2\TomTomHOMEService.exe

~ Services: Scanned in 00mn 20s

---\\ Recherche d'infection sur le Master Boot Record (MBR)(O80)

Stealth MBR rootkit/Mebroot/Sinowal/TDL4 detector 0.4.2 by Gmer, http://www.gmer.net

Run by Propriétaire at 19/02/2014 12:22:40

device: opened successfully

user: MBR read successfully

Disk trace:

called modules: ntoskrnl.exe CLASSPNP.SYS disk.sys ACPI.sys hal.dll atapi.sys pciide.sys

1 nt!IofCallDriver[0x804E3735] >> \Device\Harddisk0\DR0[0x86F71AB8]

kernel: MBR read successfully

user & kernel MBR OK

~ MBR: 13 Legitimates Filtered in 00mn 02s

---\\ Recherche d'infection sur le Master Boot Record (MBRCheck)(O80)

Written by ad13, http://ad13.geekstog

Run by Propriétaire at 19/02/2014 12:22:48

********* Dump file Name *********

C:\PhysicalDisk0_MBR.bin

~ MBR: Scanned in 00mn 10s

---\\ Scan Additionnel (O88)

Database Version : 13031 - (17/02/2014)

Clés trouvées (Keys found) : 5

Valeurs trouvées (Values found) : 1

Dossiers trouvés (Folders found) : 6

Fichiers trouvés (Files found) : 0

[HKCU\Software\APN] =>Toolbar.Ask

[HKLM\Software\APN] =>Toolbar.Ask

[HKCU\Software\AskPartnerNetwork] =>Toolbar.Ask

[HKLM\Software\AskPartnerNetwork] =>Toolbar.Ask

[HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Ext\PreApproved\{11111111-1111-1111-1111-110411901182}] =>PUP.CrossRider

[HKLM\Software\Microsoft\Internet Explorer\Toolbar]:{41564952-412D-5637-4300-7A786E7484D7} =>Toolbar.Avira^

C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\extensions\5304cc00-bc6d-40d1-8c6b-457716a1eafc@874ed2aa-e67a-4dd0-9a61-a24d421de244.com =>Adware.PlusHD^

C:\Documents and Settings\Propriétaire\Application Data\Mozilla\Firefox\Profiles\cio0qjxf.default\extensions\support@websteroidsapp.com =>PUP.TubeDimmer^

C:\Program Files\google toolbar =>Toolbar.Google^

C:\Documents and Settings\All Users\Application Data\Updater =>PUP.CrossRider^

C:\Program Files\AskPartnerNetwork =>Toolbar.Ask

C:\Documents and Settings\All Users\Application Data\AskPartnerNetwork =>Toolbar.Ask

~ Additionnel Scan: 246524 Items scanned in 00mn 58s

---\\ Récapitulatif des détections trouvées sur votre station

~ http://nicolascoolman.webs.com/apps/blog/show/28138048-adware-plushd =>Adware.PlusHD

~ http://nicolascoolman.webs.com/apps/blog/show/37242682-pup-tubedimmer =>PUP.TubeDimmer

~ http://nicolascoolman.webs.com/apps/blog/show/27583526-pup-crossrider =>PUP.CrossRider

~ http://nicolascoolman.webs.com/apps/blog/show/28927746-toolbar-ask =>Toolbar.Ask

~ MSI: 4 link(s) detected in 00mn 58s

~ 1492 Legitimates filtered by white list

End of the scan (699 lines in 05mn 02s)(0)