Programmes Malveillants, etc..

Comment faire face ?

1. Programme

2. Quelques définitions

3. Comment prévenir ?

4. Comment guérir ?

5. Notes et référence

1. Programme

1.1 Cette rubrique à pour objectif de structurer ce document support

1.2 Présentation, faisons connaissance en quelques mots

1.3 Quelques définitions pour se familiariser avec le langage

1.4 Comment prévenir ? Phase préventive, soyez vigilent !

1.5 Comment guérir ? Phase curative, il faut agir !

1.6 Toutes les infos utiles

2. Quelques définitions

- **Malware, en français programme malveillant :**
- Programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté.
- **Adware, en français logiciel publicitaire :**
- Logiciel qui affiche de la publicité lors de son utilisation. Logiciels espions qui espionnent les habitudes de l'utilisateur pour lui envoyer de la publicité ciblée.
- **Ransomware, en français logiciel exigeant une rançon :**
- Logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.
- **Spyware, en français logiciel espion :**
- Logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

3.1 Quelques définitions (suite)

- **Trojan, en français cheval de Troie :**

- Type de logiciel malveillant, souvent confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une malveillance. Le rôle du cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur. Le cheval de Troie n'est rien d'autre que le véhicule, celui qui fait "entrer le loup dans la bergerie". Il n'est pas nuisible en lui-même car il n'exécute aucune action, si ce n'est celle de permettre l'installation du vrai parasite.

- **Rootkit, en français outil de dissimulation d'activité :**

- Ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible, à la différence d'autres logiciels malveillants. La plupart des rootkits servent à installer des logiciels malveillants sur les machines où l'accès est obtenu.

- **Virus :**

- Les virus sont capables de se répliquer, puis de se propager à d'autres ordinateurs en s'insérant dans d'autres programmes ou des documents légitimes appelés « hôtes ». Ils se répartissent ainsi : virus de secteur d'amorçage ; de fichier ; de macro ; et de script. Certains intègrent des rootkits. Les virus peuvent s'avérer particulièrement dangereux et endommager plus ou moins gravement les machines infectées

3.2 Quelques définitions (suite)

- PC :
- De l'anglais Personal Computer, traduisez Ordinateur Personnel

- Système d'exploitation, ou OS (Operating system)
- C'est l'environnement présent sur votre ordinateur, exemples :
- - Windows : XP, Vista, Windows 7, Windows 8 et 8.1, Windows 10 (il s'agit ici de versions)
- - Linux : Ubuntu, Debian, Fedora, Mandriva, etc (il s'agit ici de distribution)
- - Mac OS : Leopard, Snow Leopard, Lion, Mountain Lion, Mavericks, Yosemite

- Update = Mise à jour / Mettre à jour
- Download = Télécharger / Téléchargement
- Agree = Accepter
- Next = Suivant
- Cancel = Quitter / Annuler

3. Comment prévenir ?

- Comment prévenir ? Phase préventive, soyez vigilent !

3.1 Maintenir à jour son système d'exploitation

- Il est essentiel d'effectuer les mises à jour de votre version de Windows, Linux ou Mac OS . Malheureusement il arrive qu'une mise à jour ne soit pas totalement au point et rende instable votre système, voir même dans certains cas extrêmes planter votre ordinateur.
-
-

3.2 Maintenir à jour ses programmes

- Il est essentiel de toujours utiliser la dernière version de vos programmes préférés. Lorsqu'un programme vous invite à le mettre à jour allez-y ! Il s 'agit le plus souvent de correctifs ou mises à jour de sécurité. Toutefois méfiance aux imposteurs, il n'est pas rare qu'un malware se fasse passer pour une mise à jour d'un programme bien répandu, type « Adobe Flash Player » ou « Java » !!

3.3 Maintenir à jour ses programmes

- Utiliser un navigateur web alternatif à « Internet Explorer » (installé par défaut sous Windows) du type Google Chrome ou Mozilla Firefox, ils intègrent déjà « Adobe Flash Player » ce qui vous évite d'avoir à le mettre à jour indépendemment de votre navigateur. Autre chose, ils se mettent à jour indépendamment de votre système, de façon autonome. Encore un chose, des bloqueurs de pubs efficaces sont disponibles sous la forme d'extensions pour Google Chrome ou de modules complémentaires pour Mozilla Firefox

3.4 Vérifiez l'adresse exacte des sites web

- Toujours vérifier l'adresse exacte d'un site avant de cliquer sur un résultat de recherche Google
- Certaines extensions issues d'anti-virus vous indiquent si les sites sont fiables ou non. Cette fonction dépend toutefois de la version de l'anti-virus que vous utilisez
- Quelques exemples :
- - Avast !
- - Kaspersky
- - Bitdefender

3.5 Préférez utiliser le moteur de recherche Google

- Tout est dans le titre ! Le référencement du moteur de recherche « Google » est nettement plus clair et plus précis que la plupart des autres moteur de recherche.
- Quelques exemples à éviter:
- - Yahoo
- - Bing
- - Orange

3.6 Évitez de télécharger via des sites plates-formes

- Évitez de télécharger des programmes via des sites plates-formes. Préférez toujours le **site officiel de l'éditeur**.
- Quelques exemples à éviter:
- - 01net.com
- - clubic.com
- - commentcamarche.net

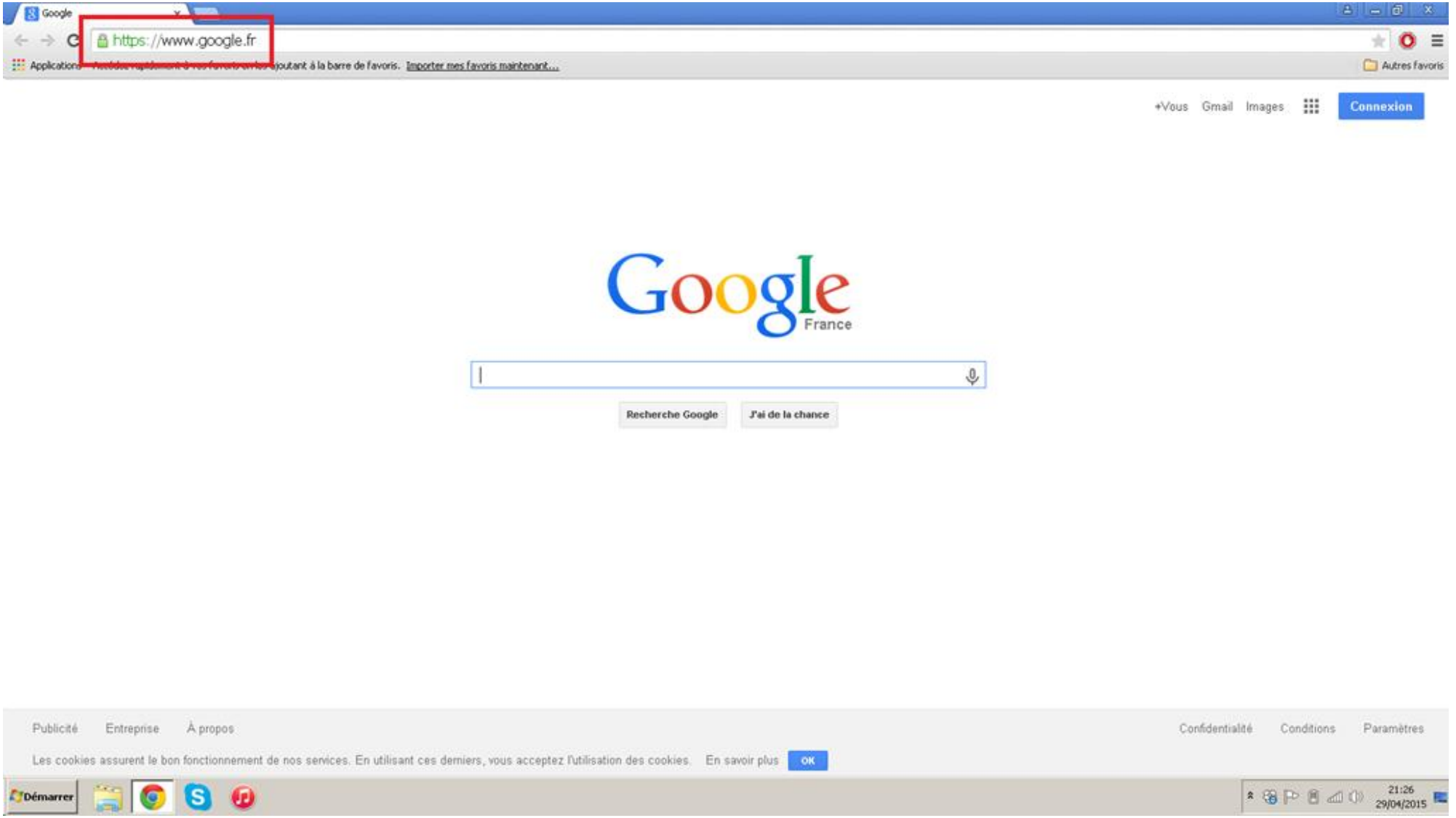
3.7 Prenez le temps de lire

- Lorsque vous téléchargez ou installez un programme dont vous avez vérifié l'éditeur, méfiez vous lors de l'installation à ne pas cliquer sur « suivant » ou « j'accepte » trop vite, prenez le temps de lire chaque étape, il est courant que lors de l'installation principale on vous propose d'installer un programme partenaire de l'éditeur.
- La suite en image

3.8 Prenons un exemple

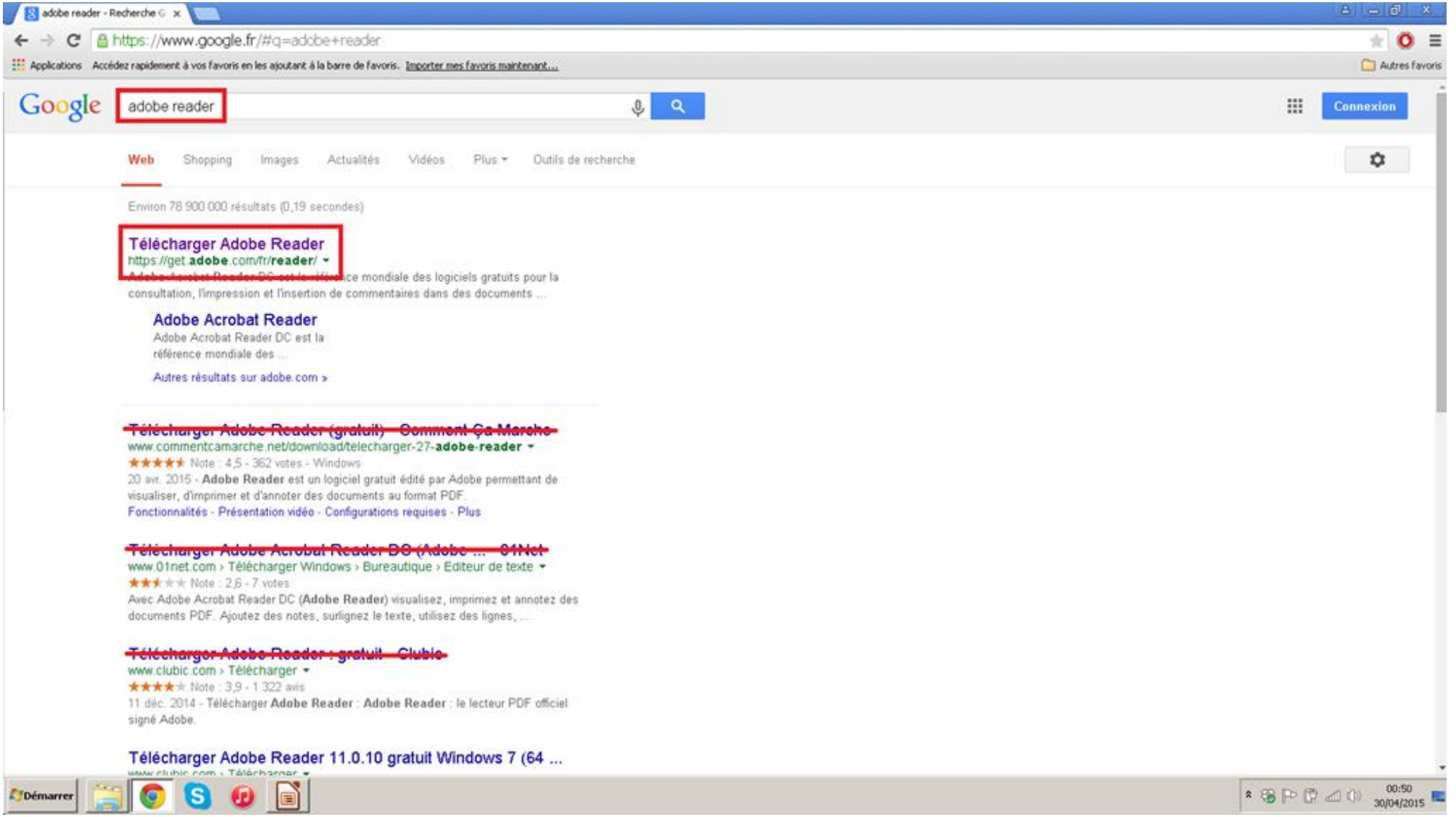
- Pour exemple, j'ai choisi Adobe Reader, célèbre programme gratuit permettant de lire les fichiers PDF

3.8.1 Rendez-vous sur Google

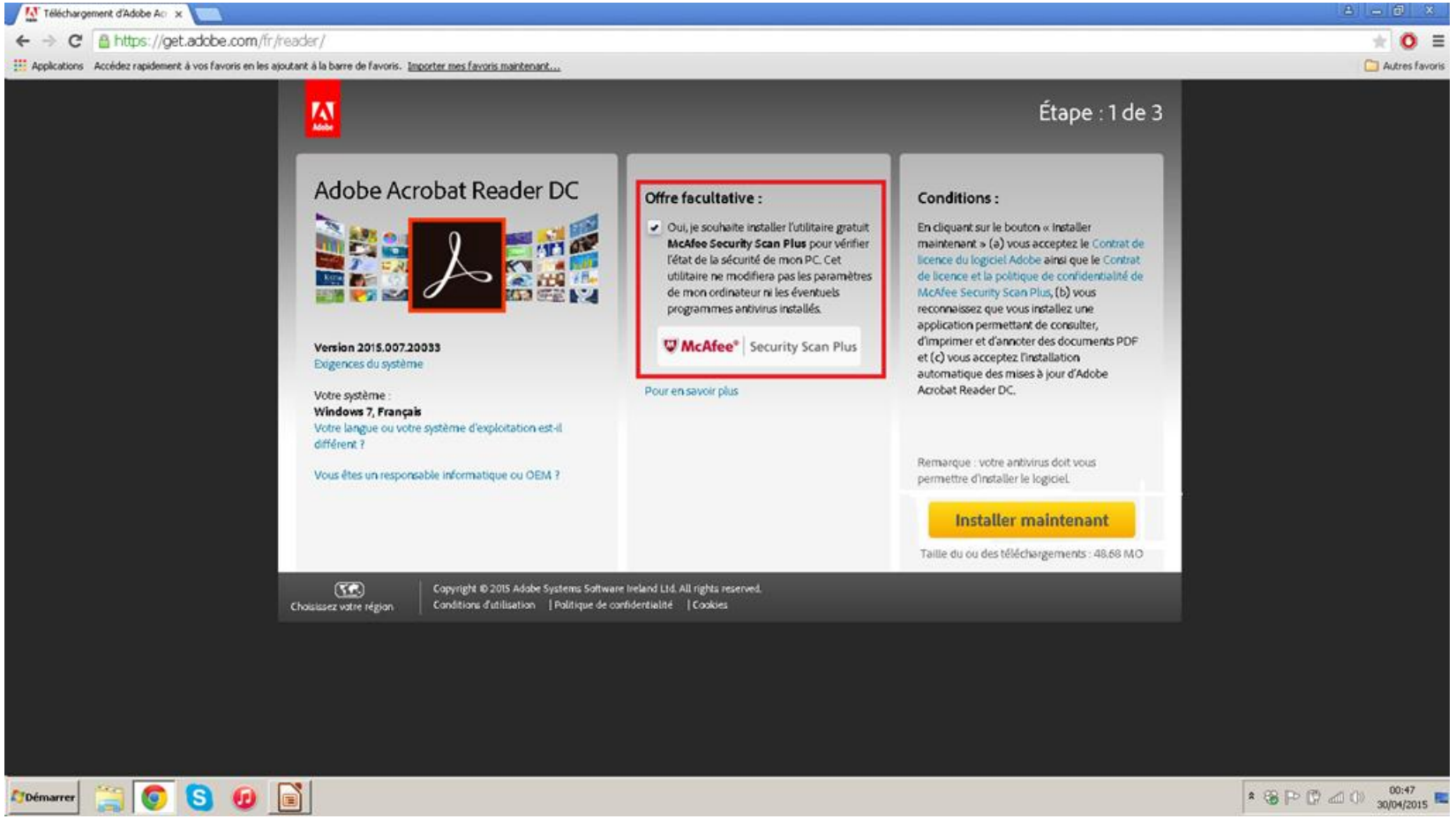


3.8.2 Tapez votre recherche

puis cliquez sur le lien

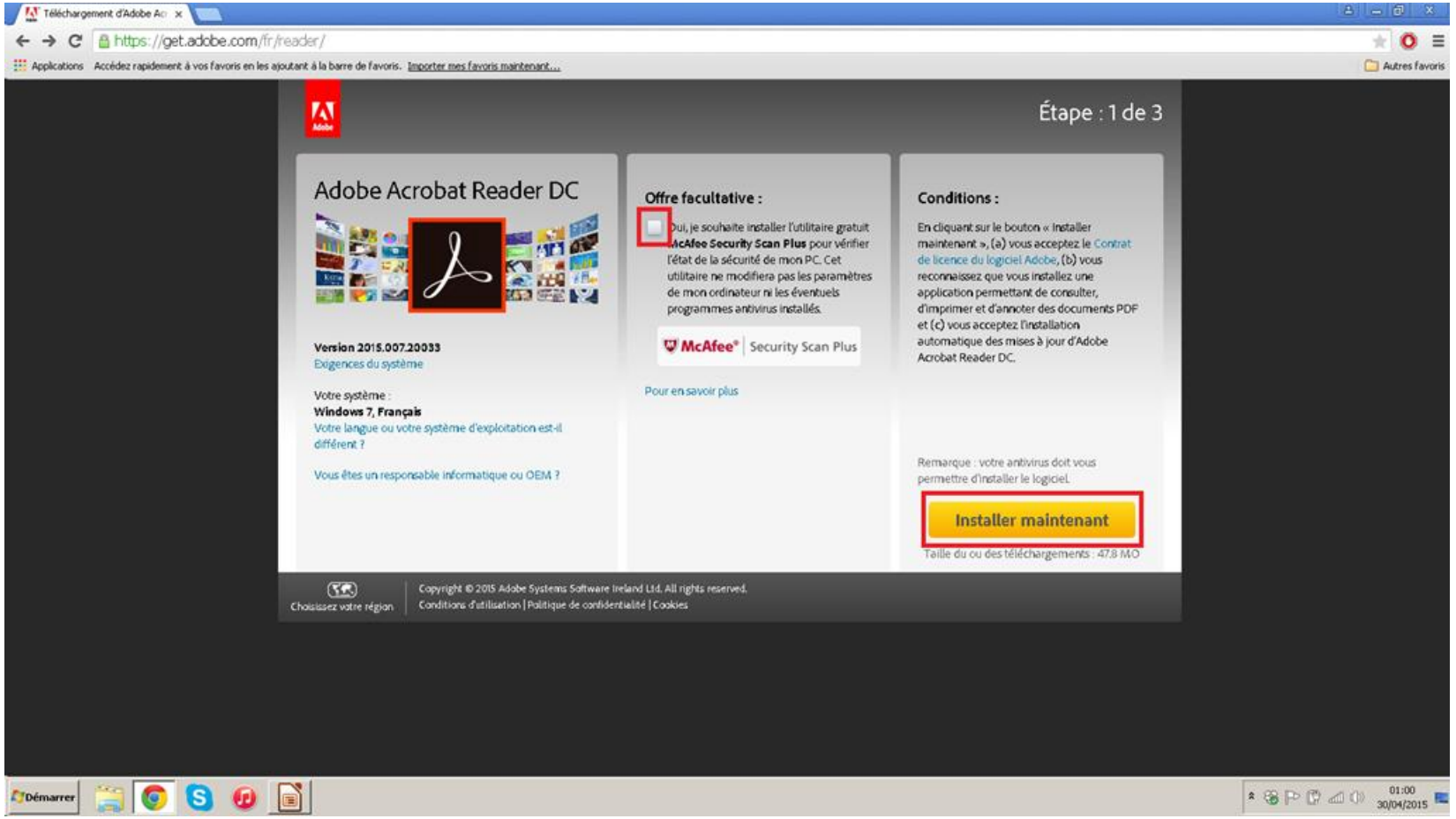


3.8.3 Attention ! Décochez la case « Offre facultative »

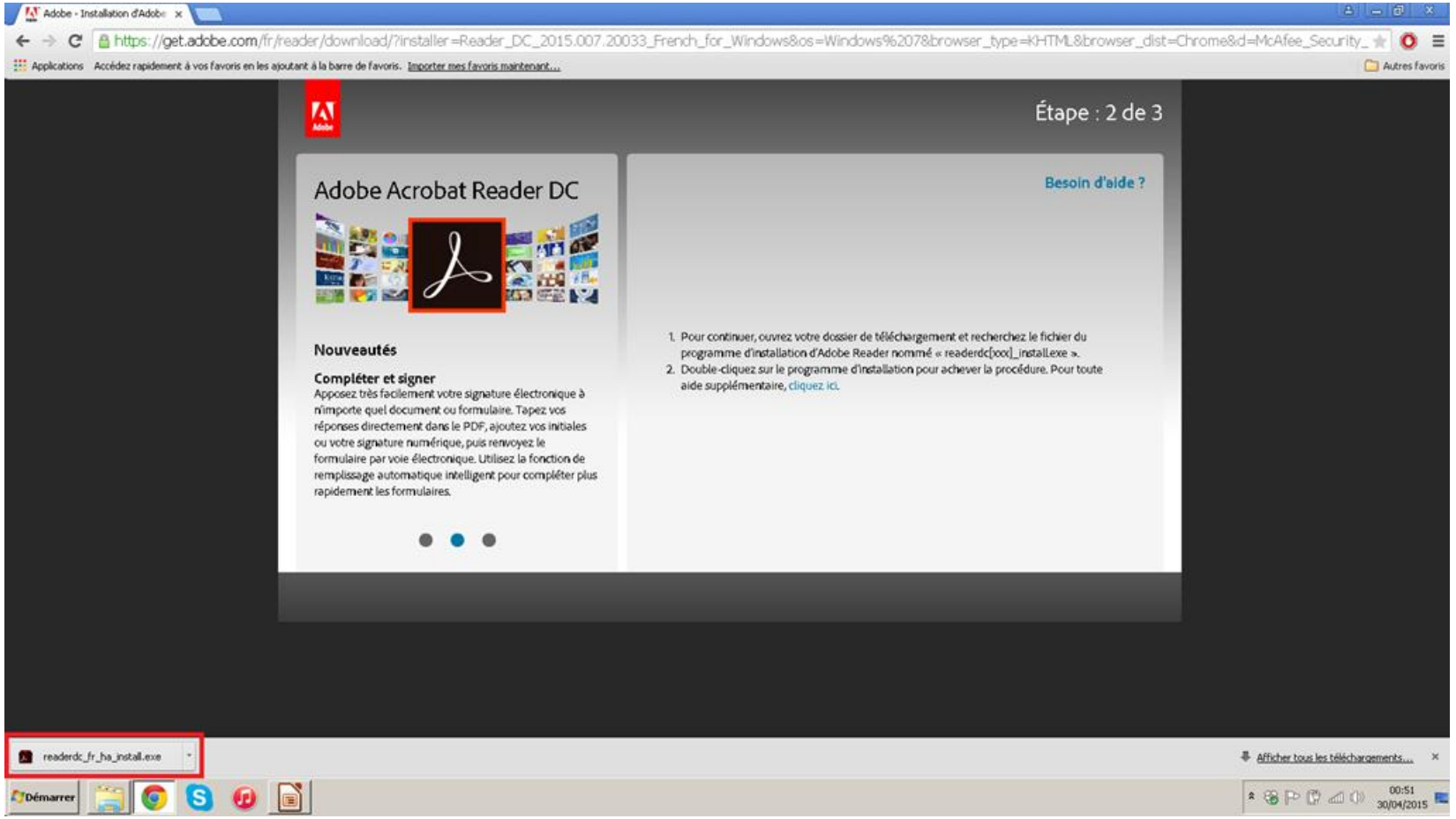


3.8.4 Maintenant, cliquez sur

« Installer maintenant »



3.8.5 Votre programme est téléchargé, exécutez le !



4. Comment guérir ?

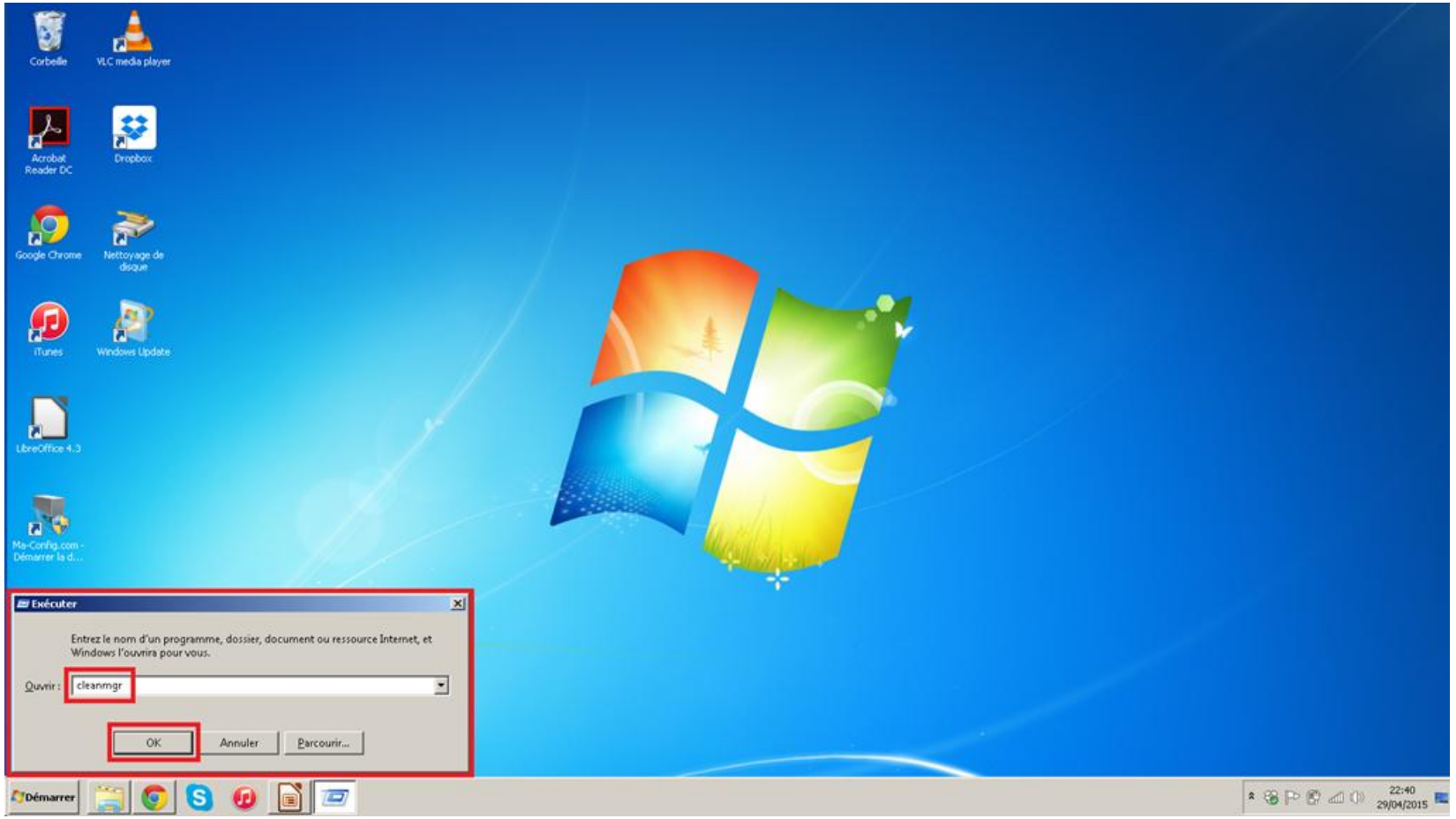
- Comment guérir ? Phase curative, il faut agir !

4.1 Nettoyage de disque

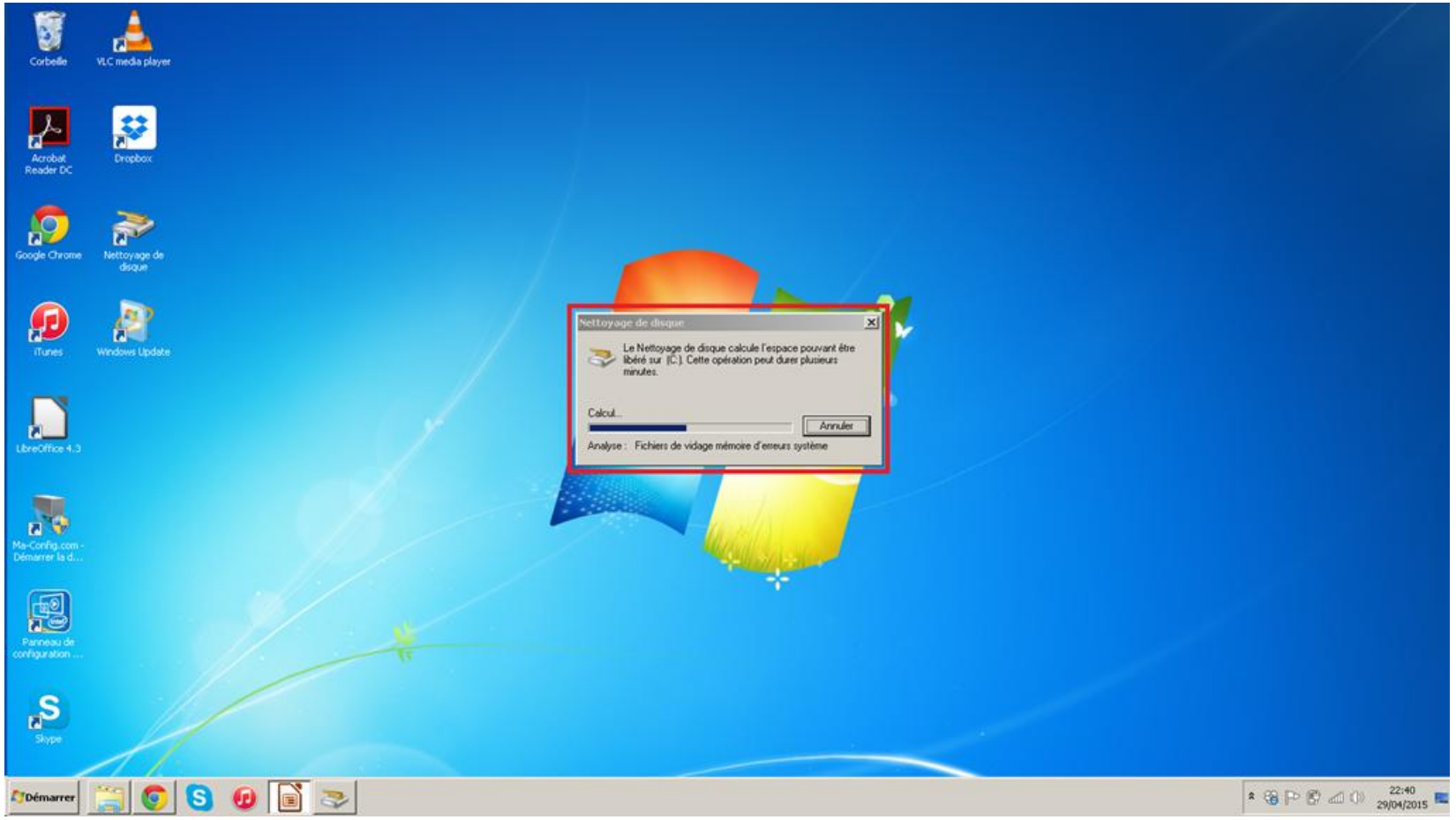
- Cet outil très pratique est déjà présent sous Windows, pour l'exécuter rien de plus simple !
- 1. Maintenez la touche « Windows » de votre clavier enfoncée
- 2. Faites une impulsion sur la « R » de votre clavier jusqu'à ce que la fenêtre « Exécuter » vous invite à entrer le nom d'un programme
- 3. La suite en image !!

1. Tapez « cleanmgr »

2. Cliquez sur « OK »

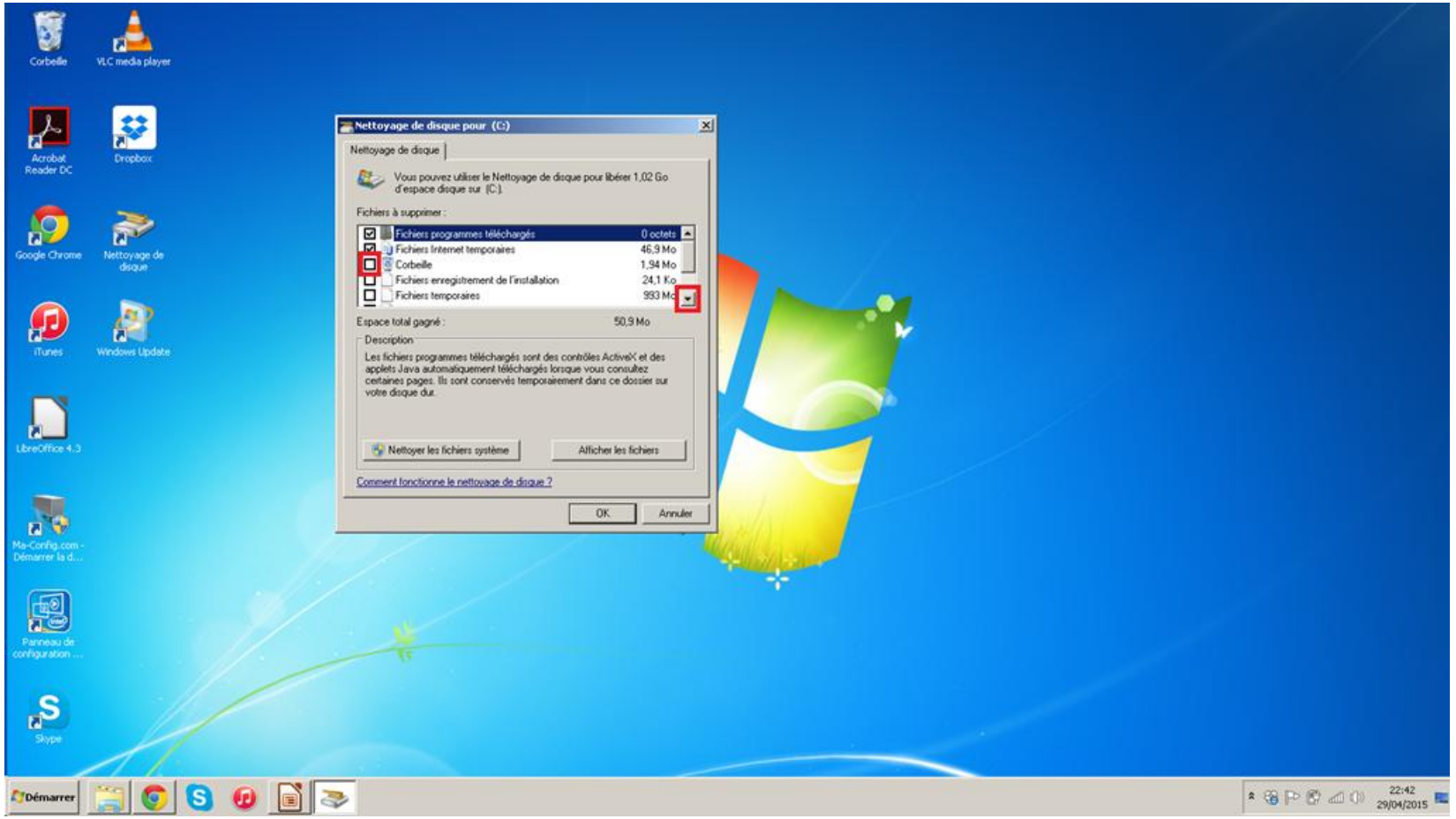


Patientez ⟶ phase de calcul de l'espace pouvant être libéré

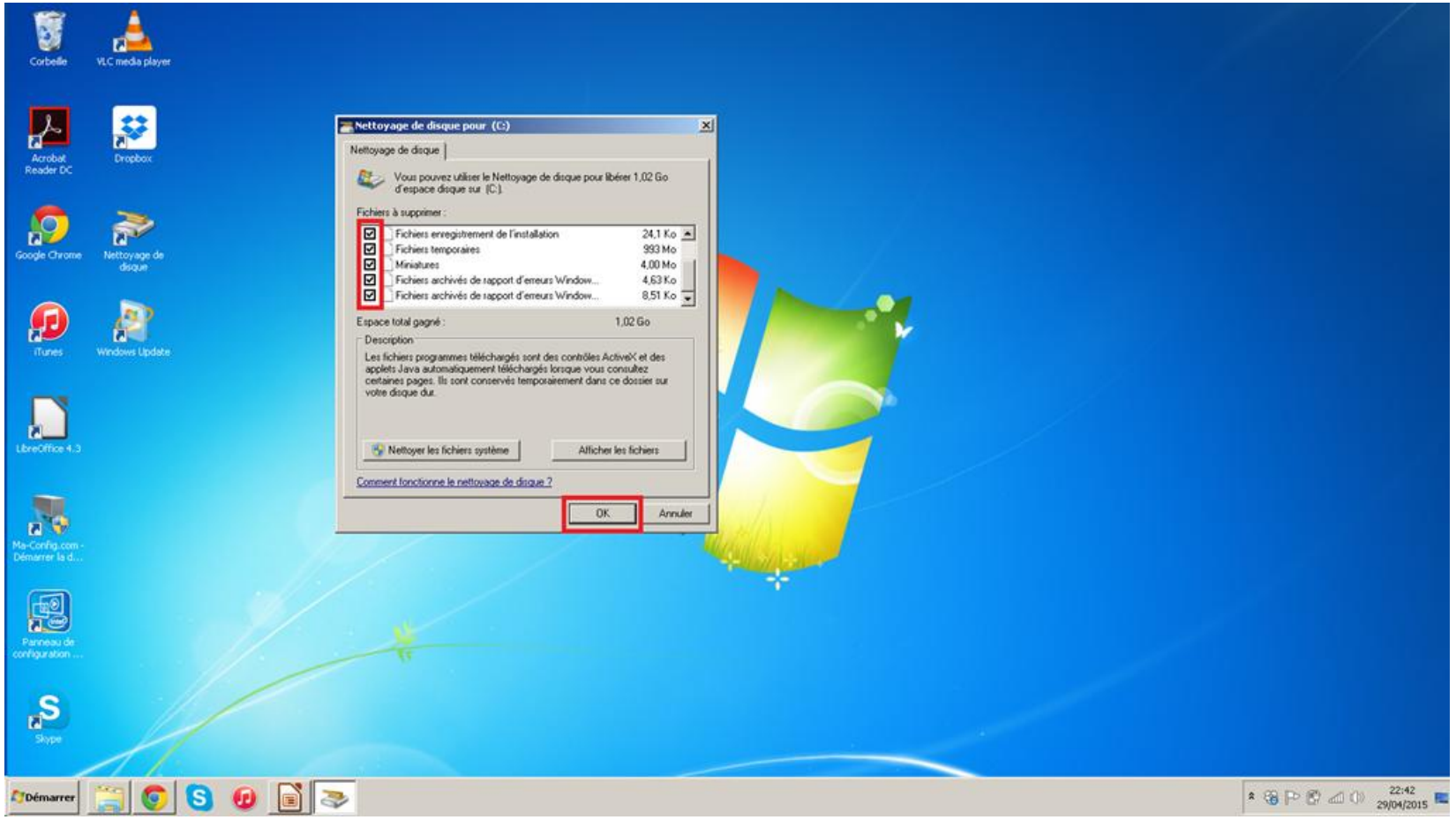


1. Cochez toutes les petites cases

2. Faites dérouler le menu

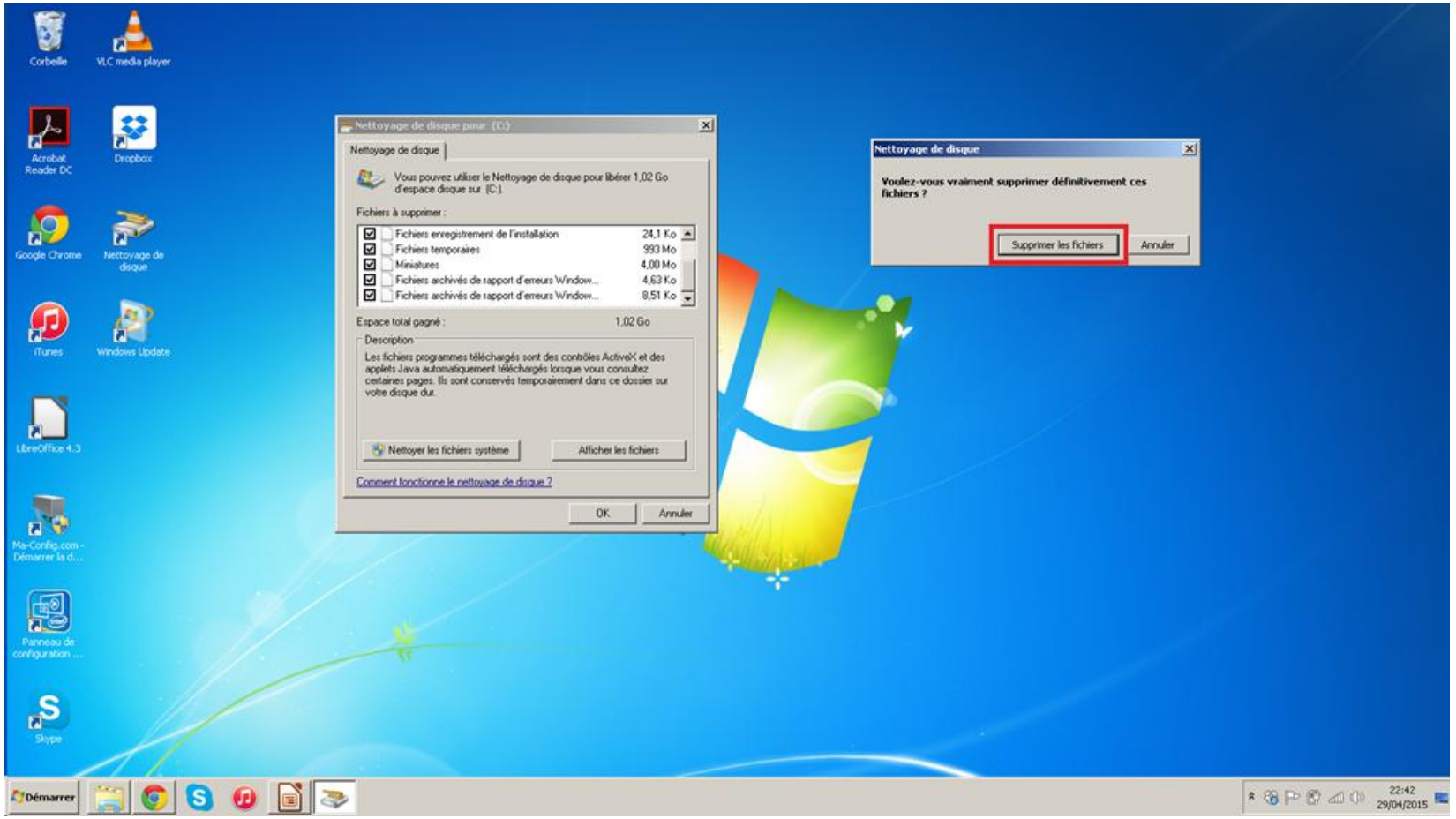


Une fois toutes les petites cases cochées, cliquez sur « OK »

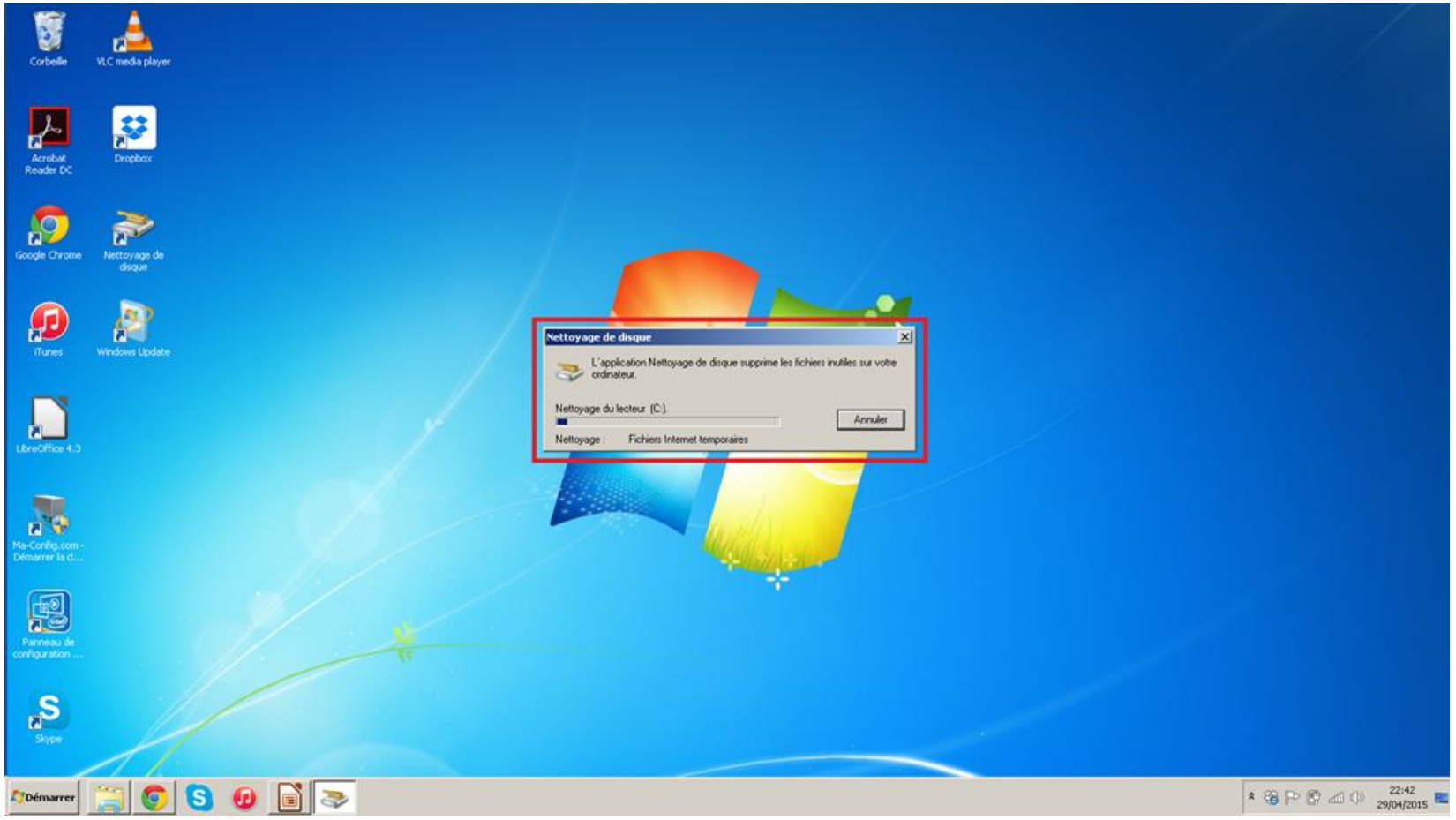


Cliquez sur

« Supprimer les fichiers »

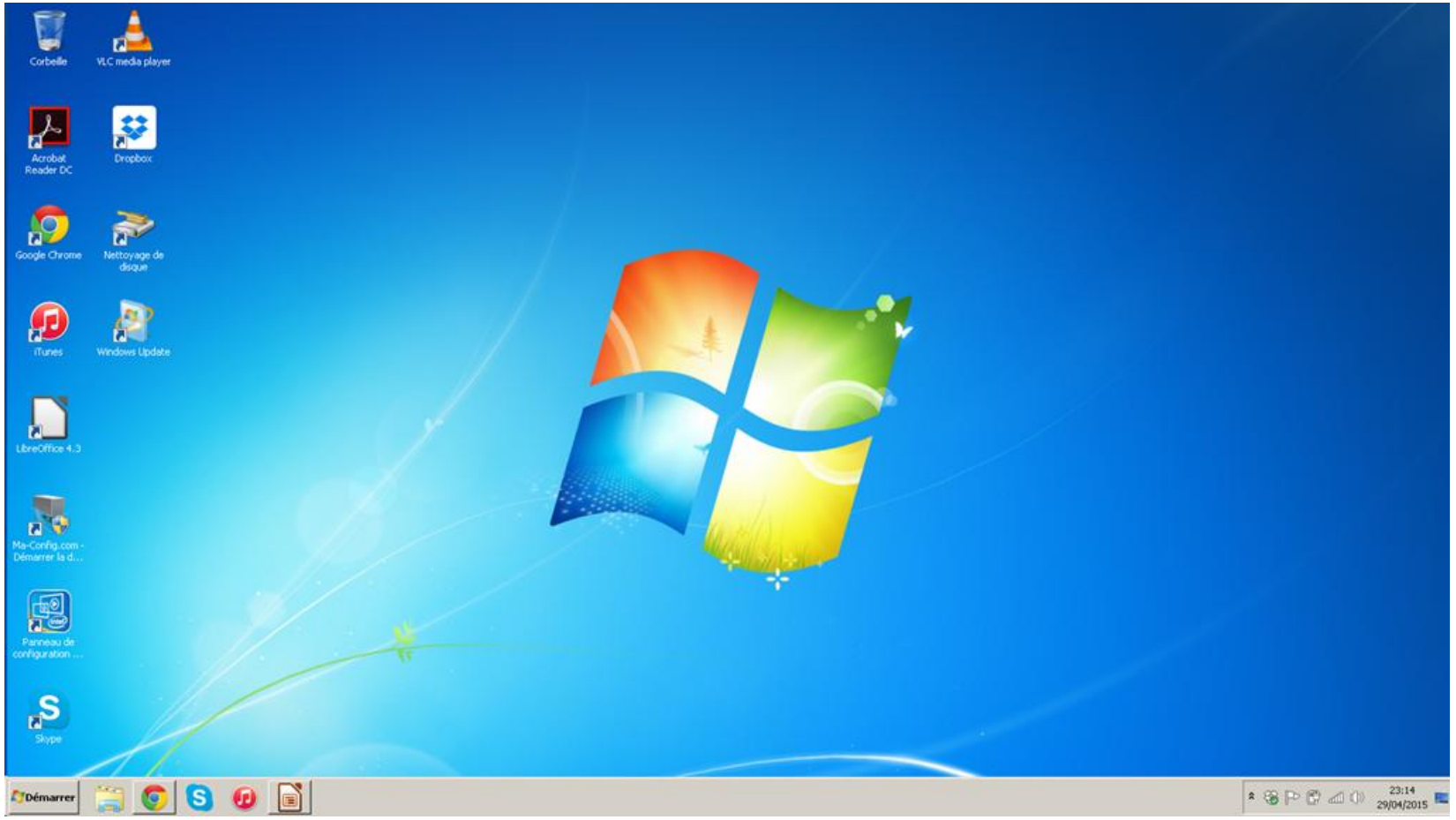


Patientez ⟶ phase de nettoyage des fichiers superflus



Une fois terminé,

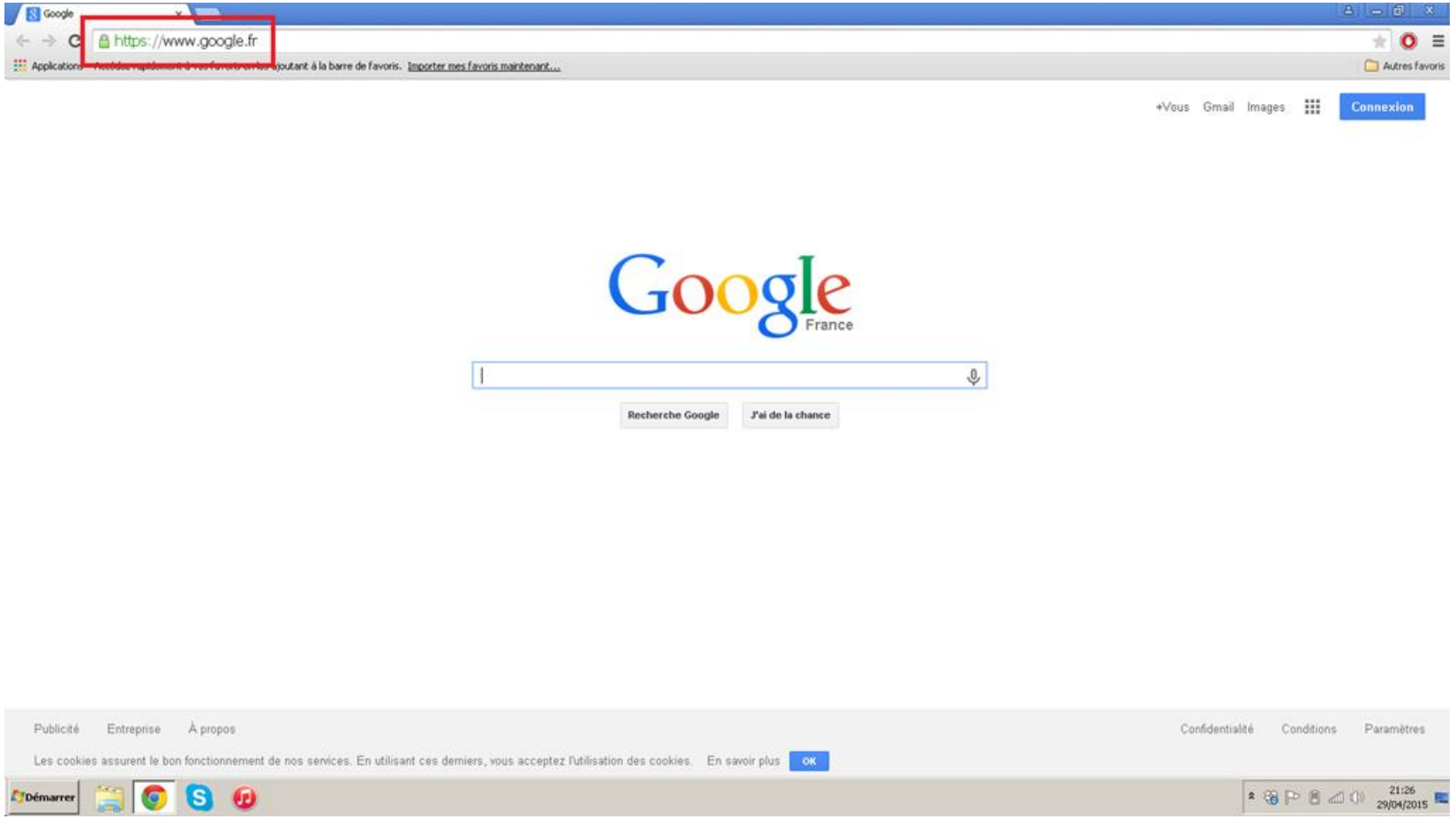
la fenêtre se ferme



4.2 Malwarebytes anti-malware

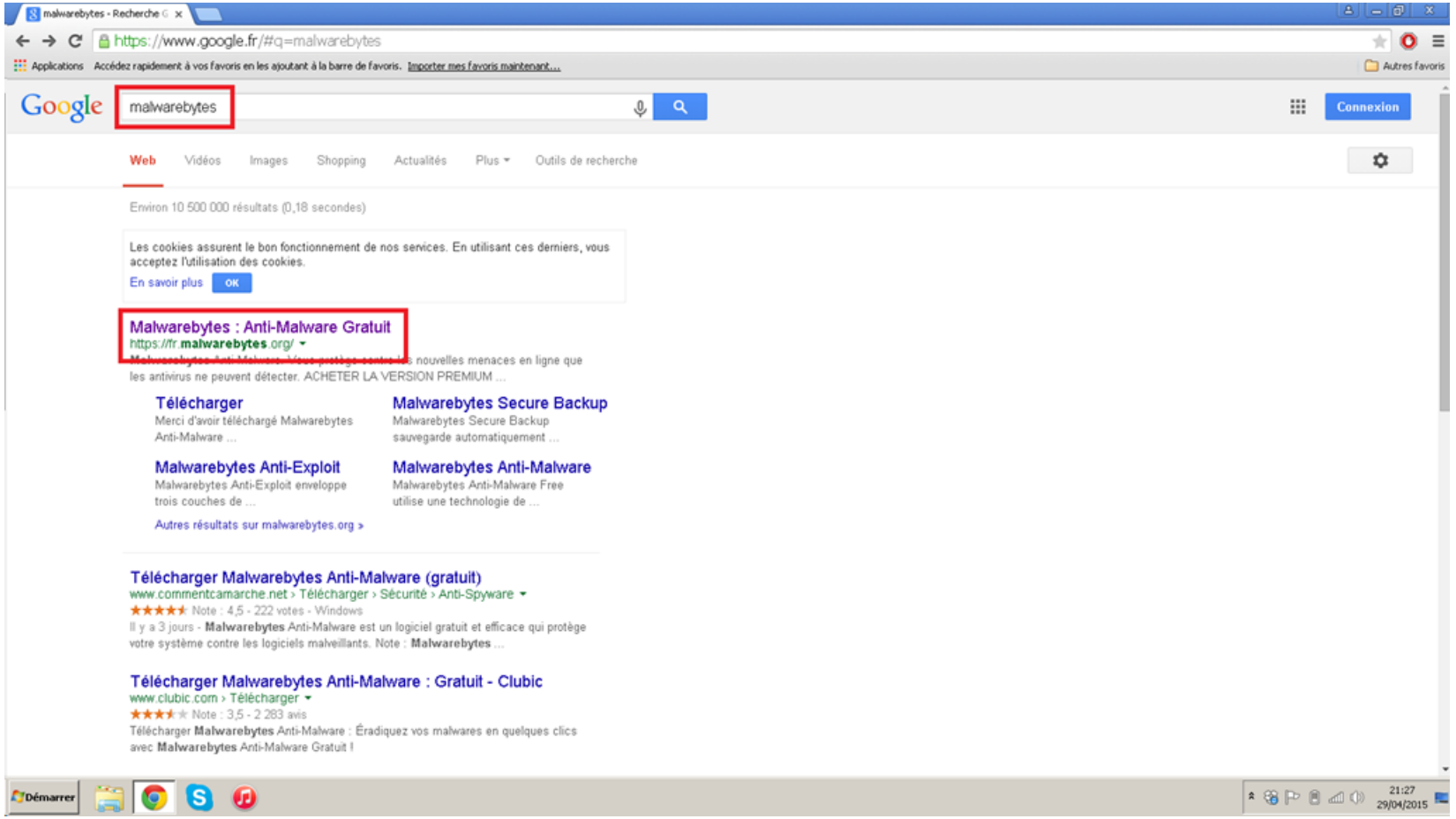
- Installez et exécutez le programme « Malwarebytes anti-malware », gratuit dans sa version de base disponible sur le site « malwarebytes.org »

Rendez-vous sur Google



1. Tapez votre recherche

2.Cliquez sur le lien

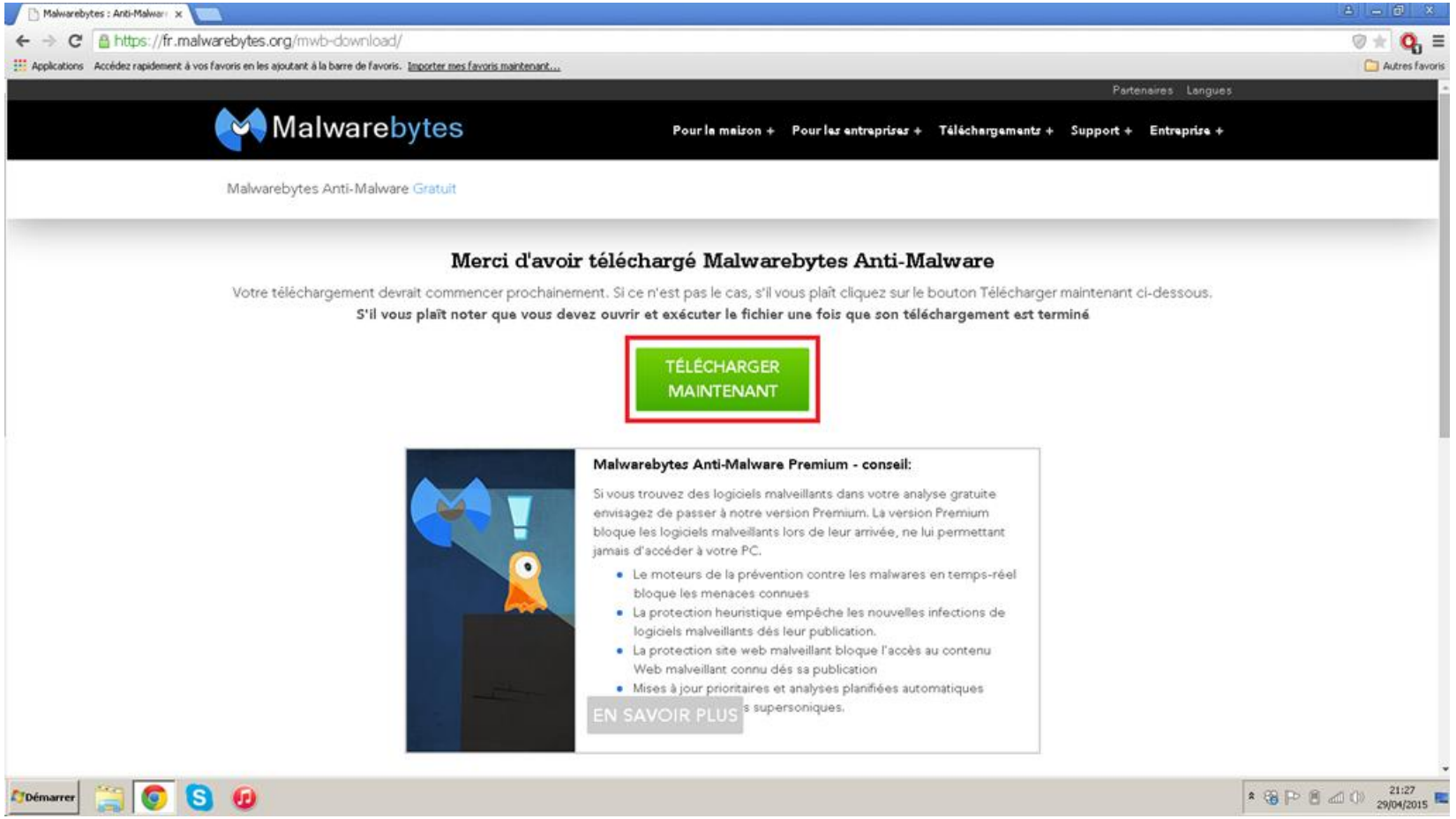


Cliquez sur

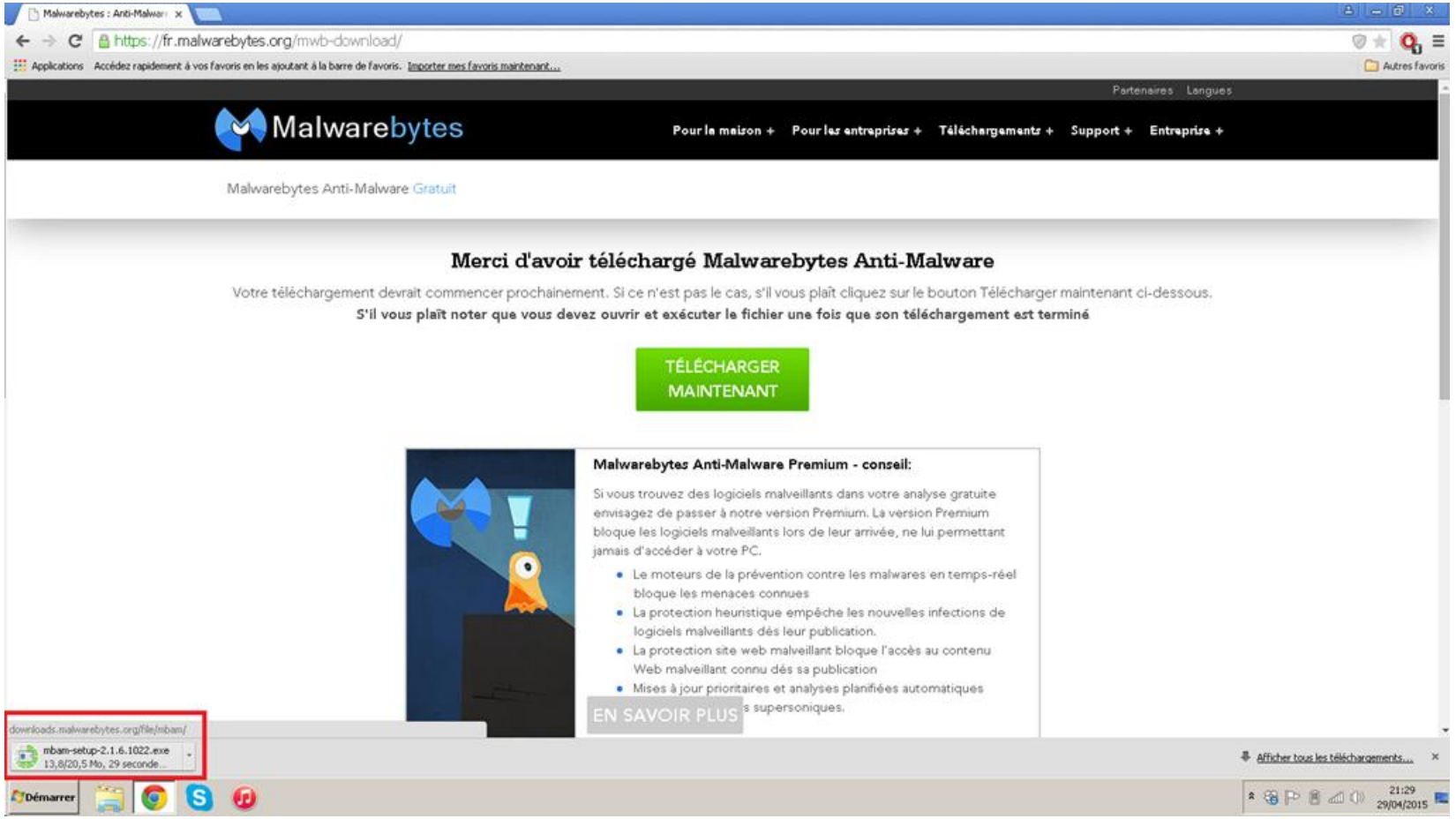
« téléchargez la version gratuite »

Cliquez sur

« télécharger maintenant »

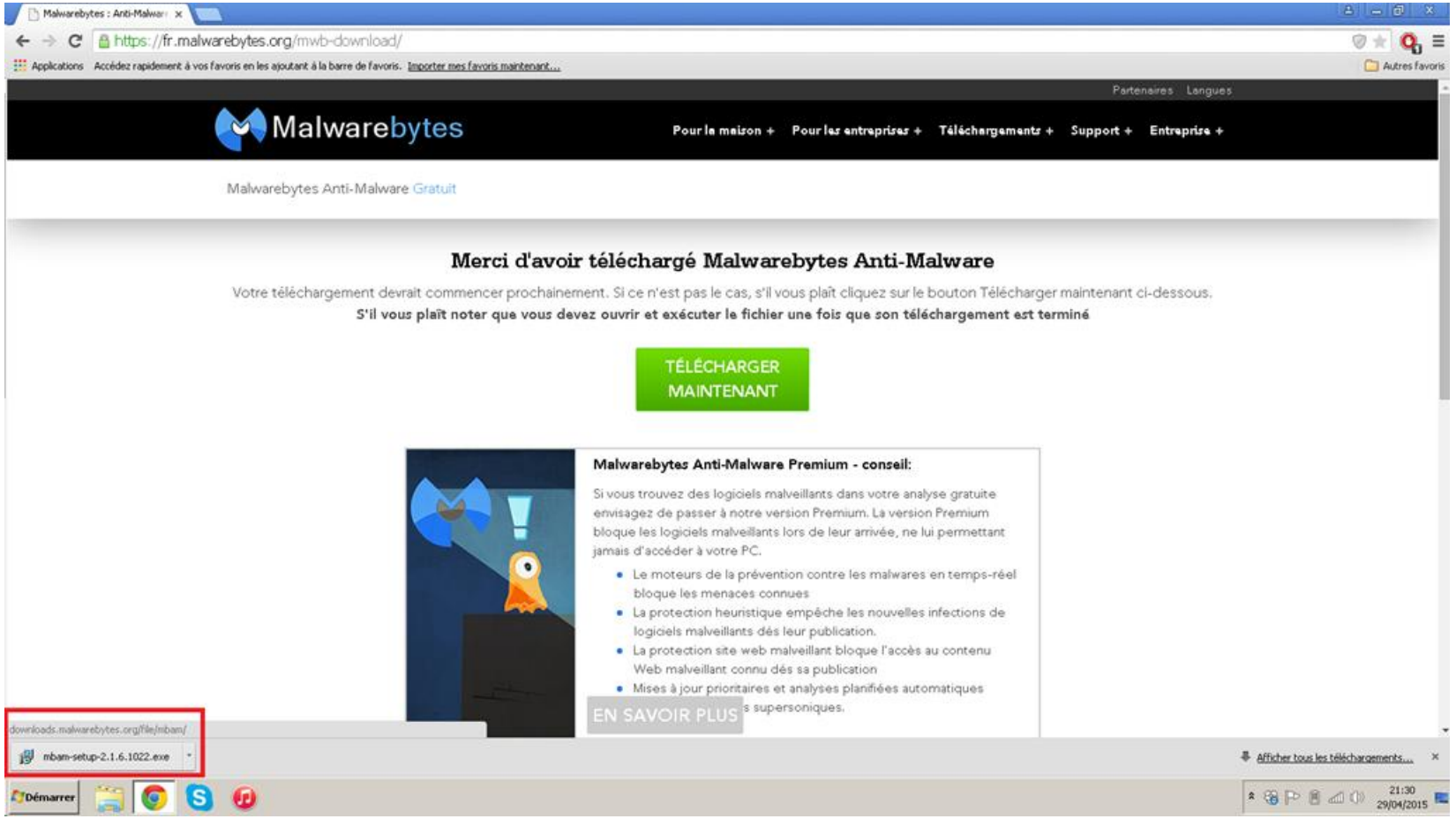


Le fichier est en cours de téléchargement

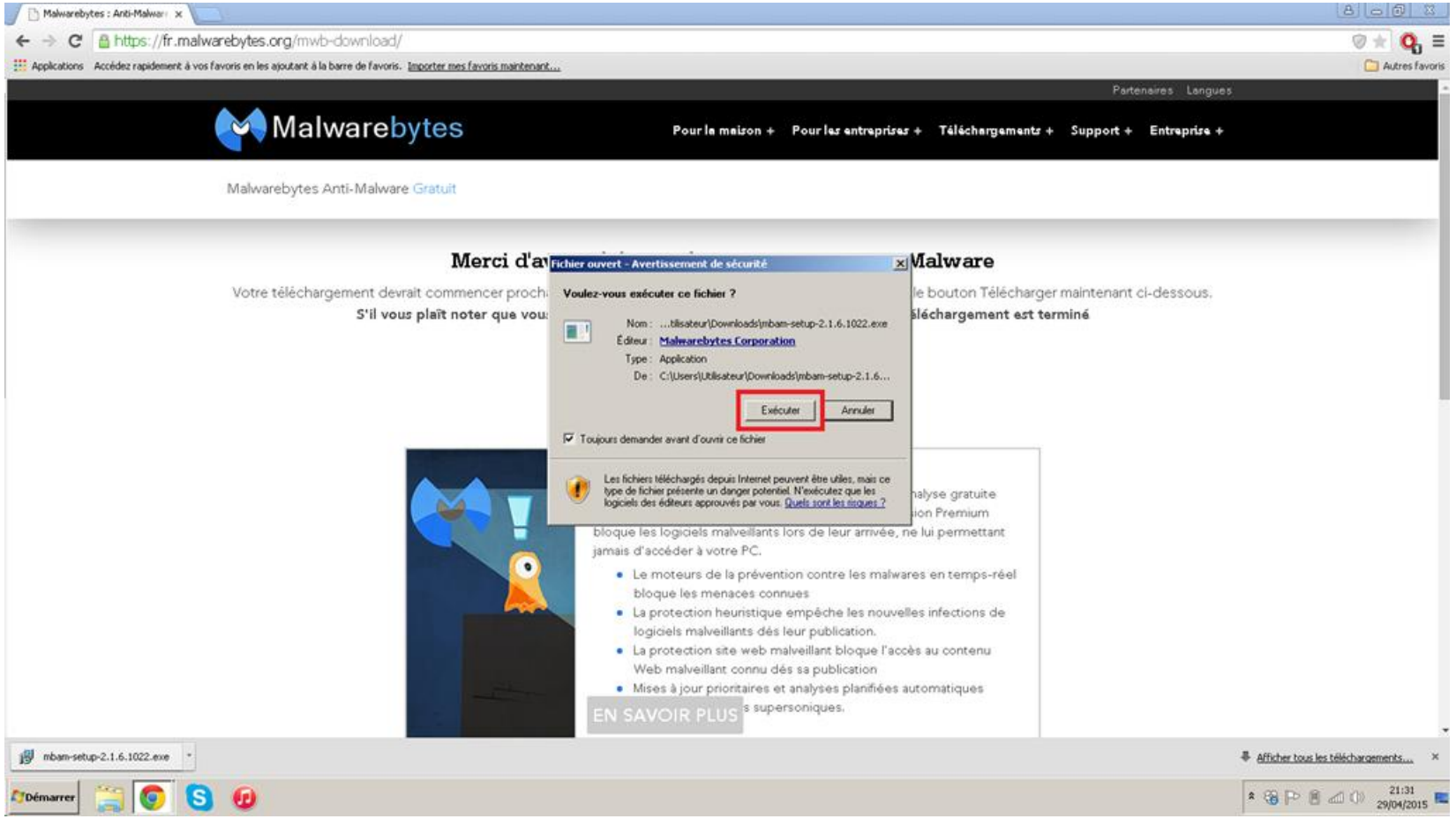


Le fichier est téléchargé,

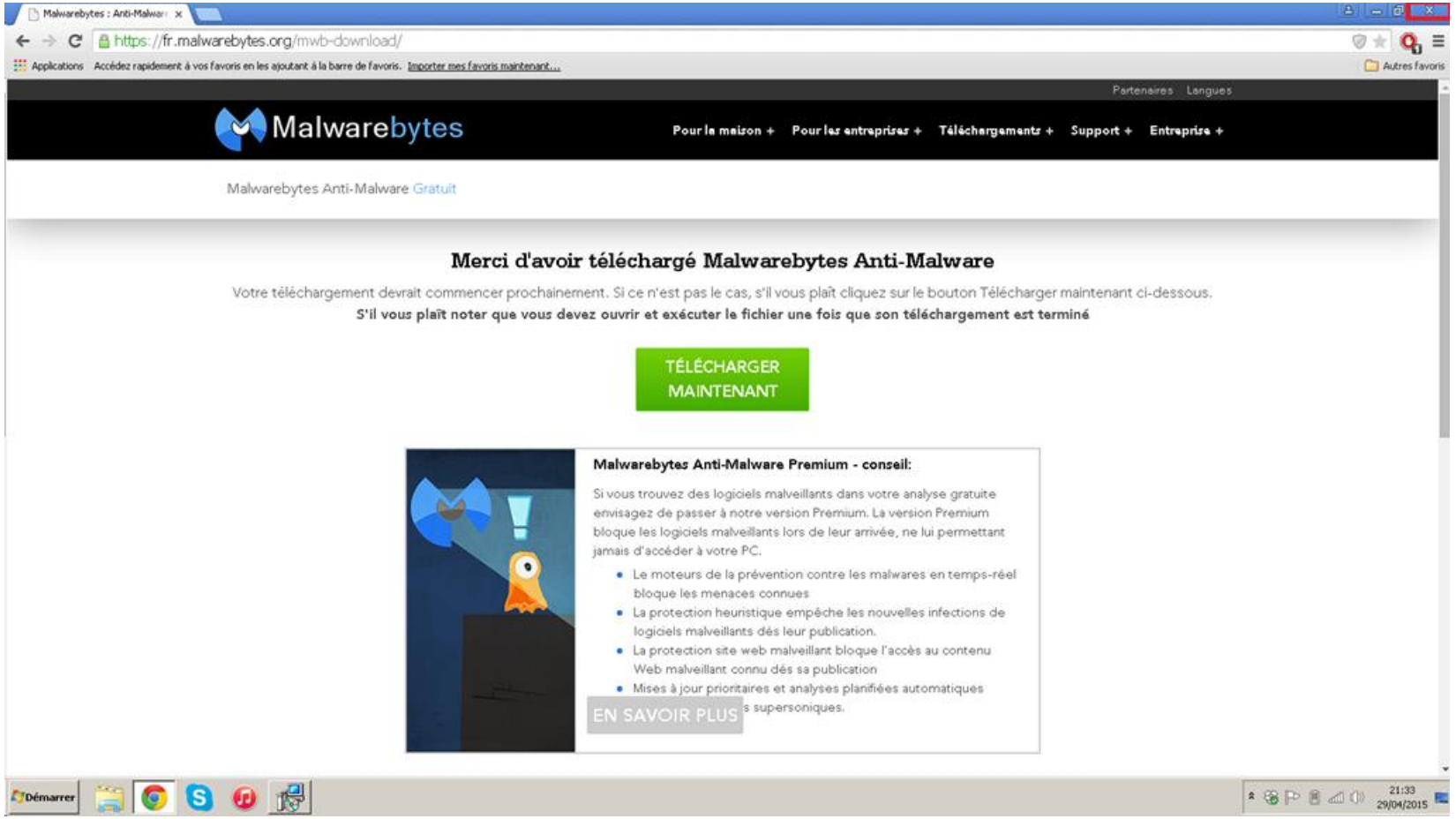
cliquez dessus



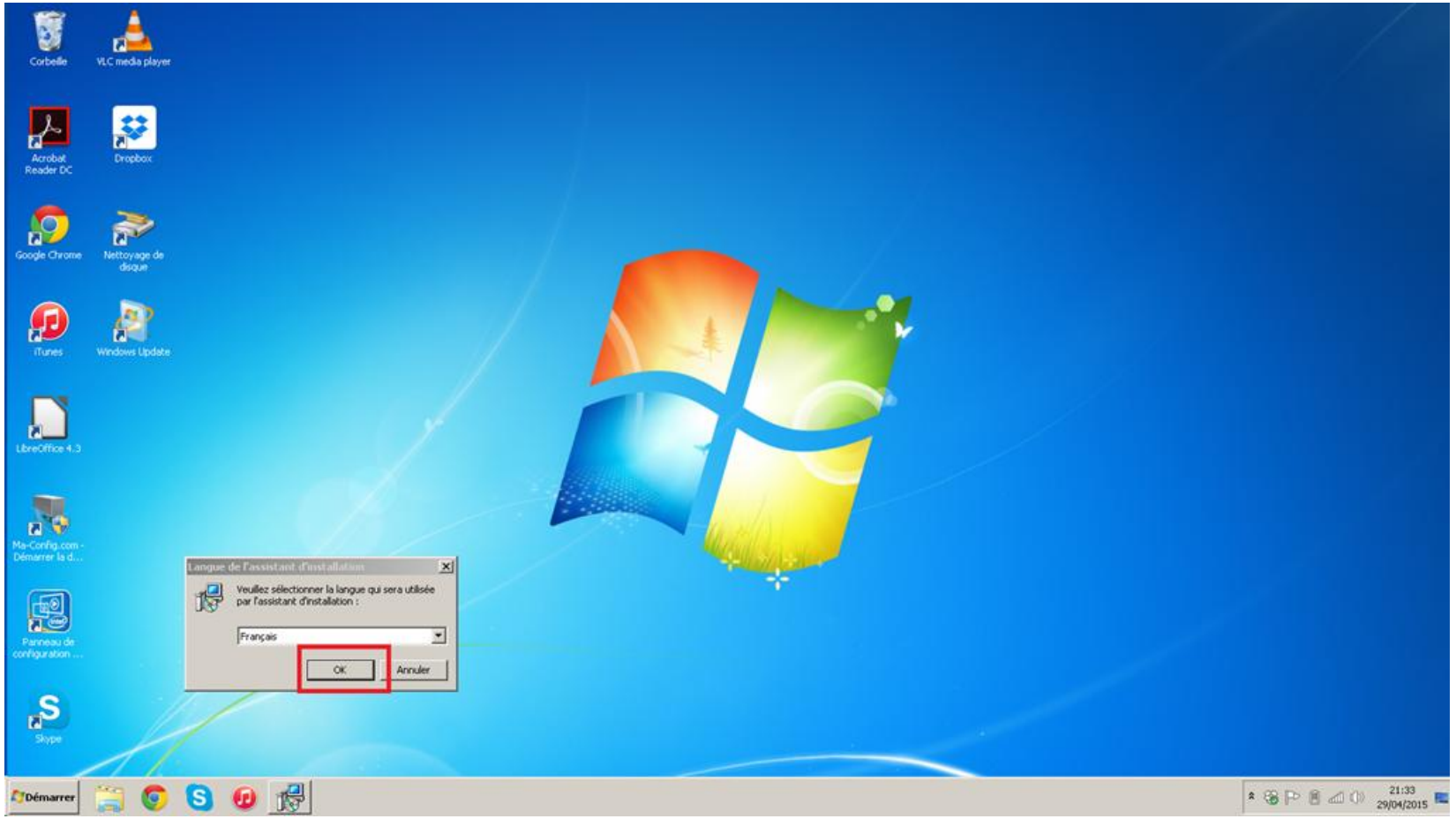
Cliquez sur « Exécuter »



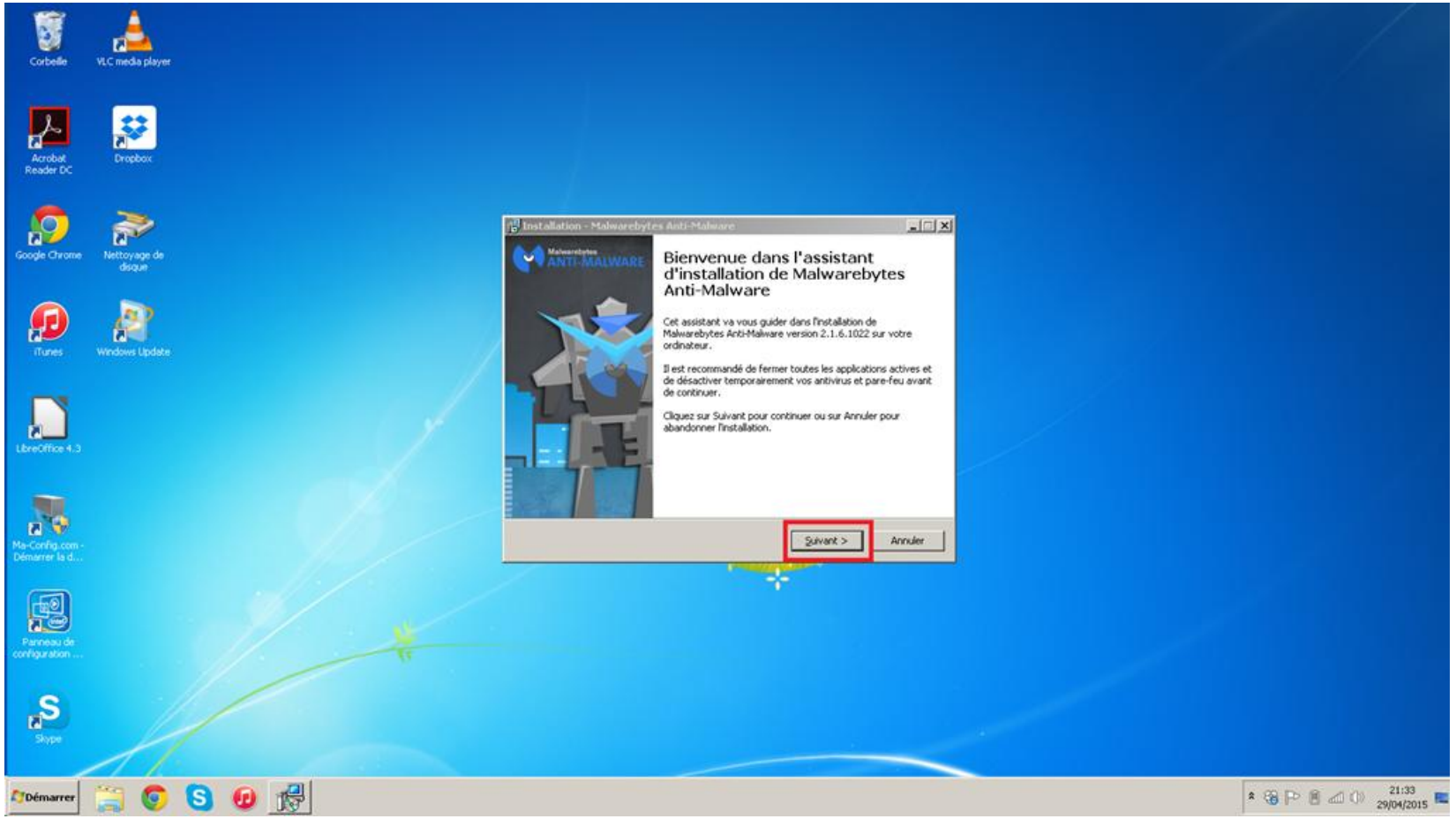
Vous pouvez refermer votre navigateur Internet



Cliquez sur OK

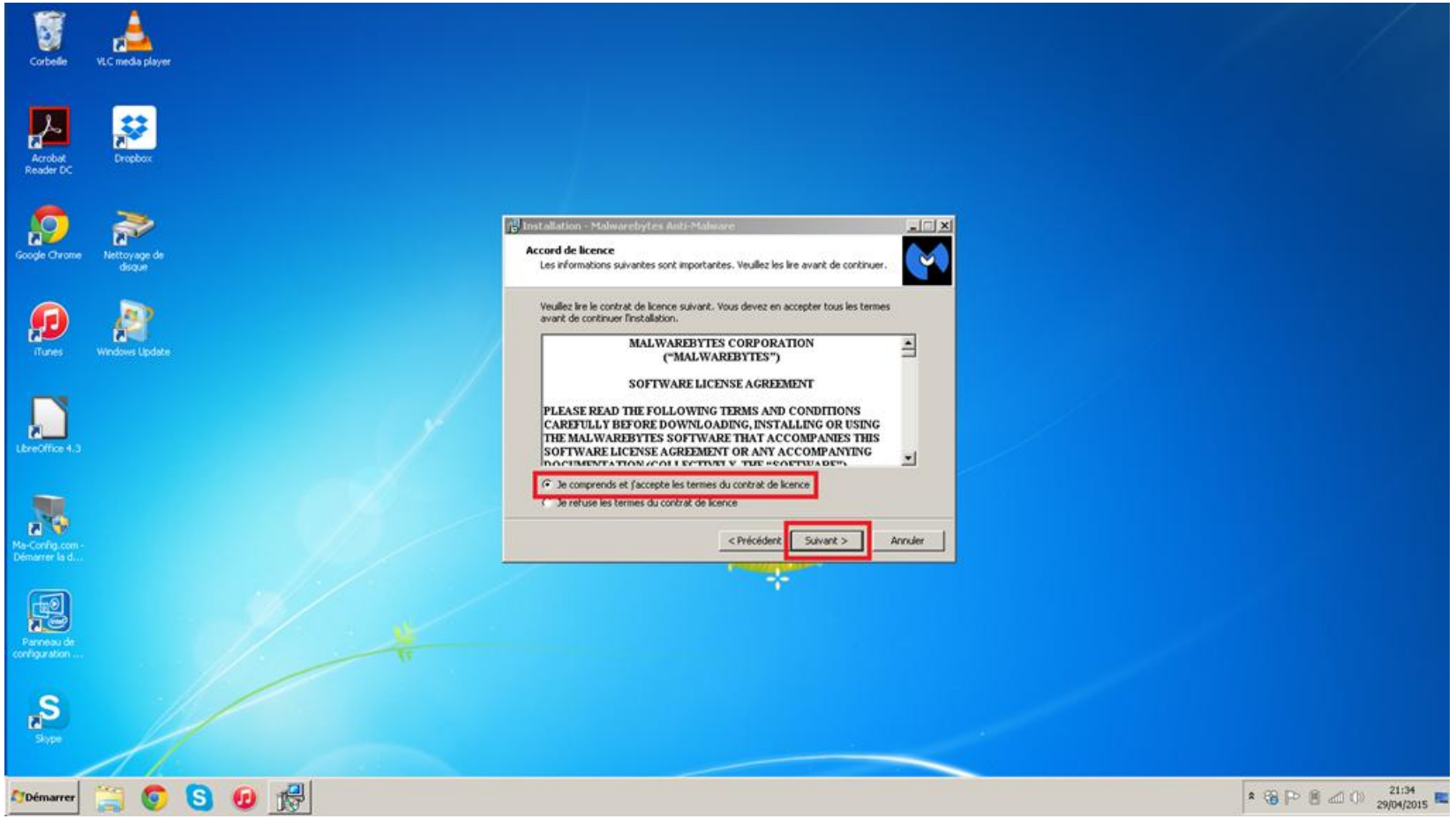


Cliquez sur « Suivant »

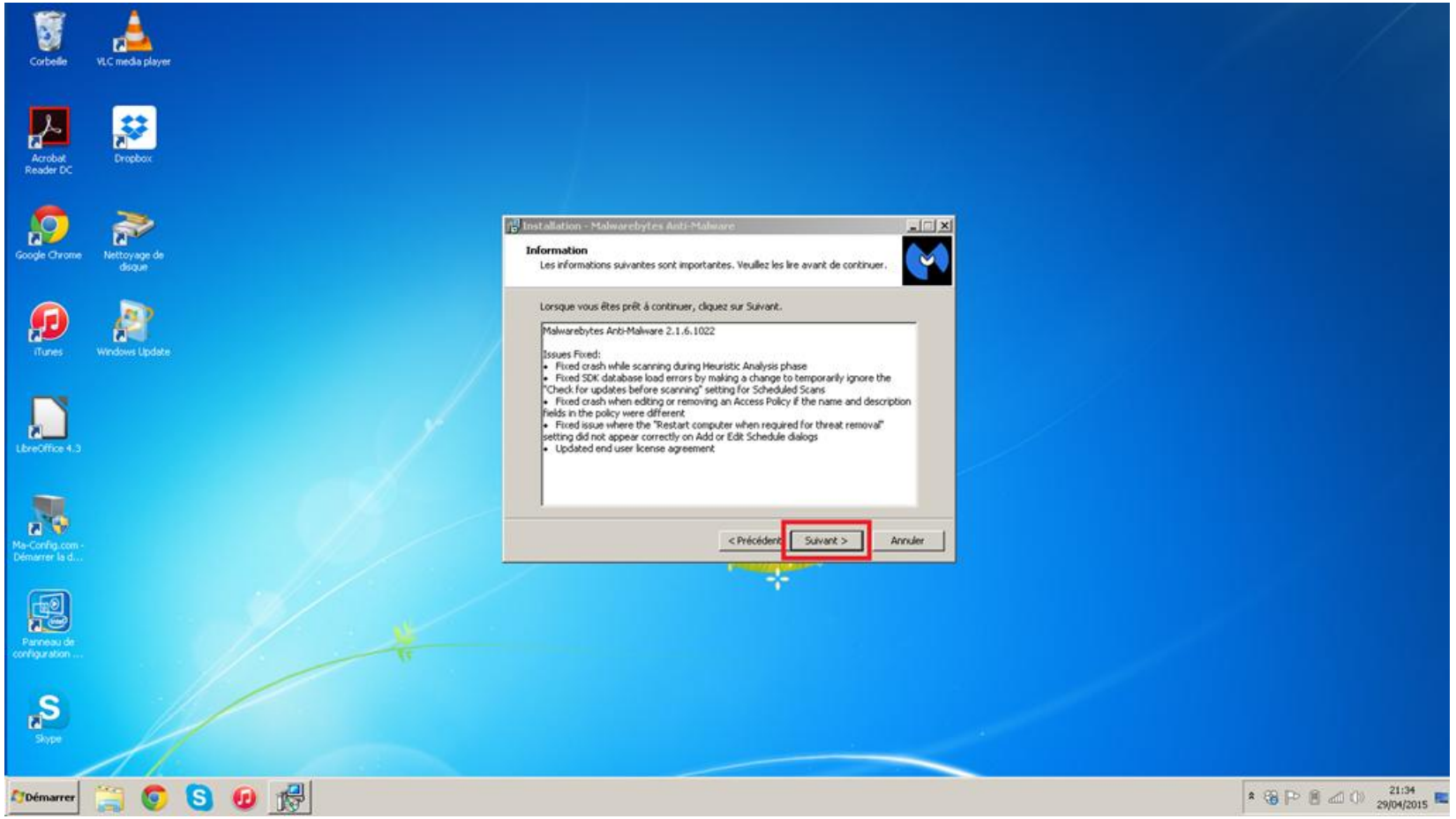


1. Cochez la case

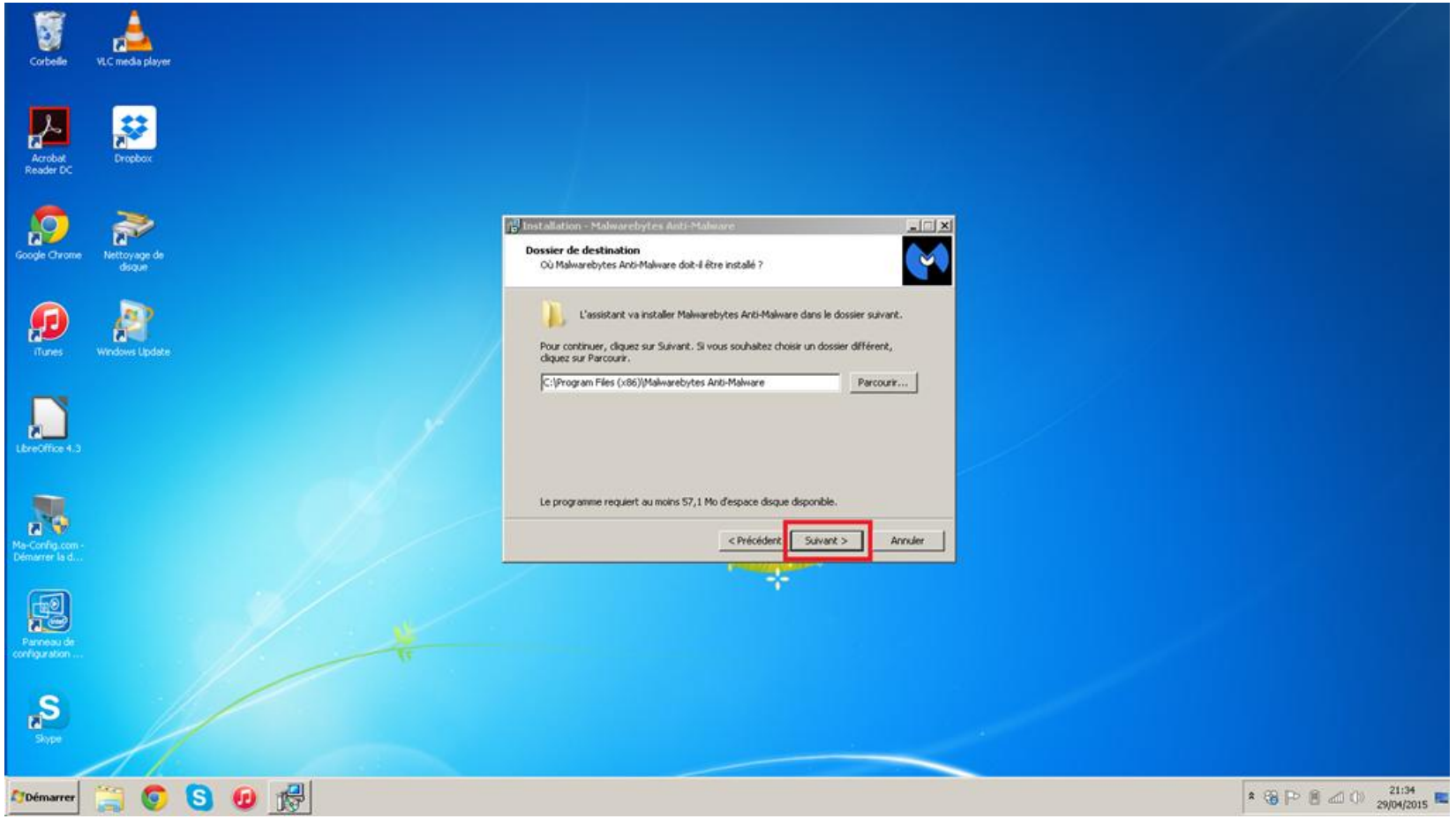
2. Cliquez sur « Suivant »



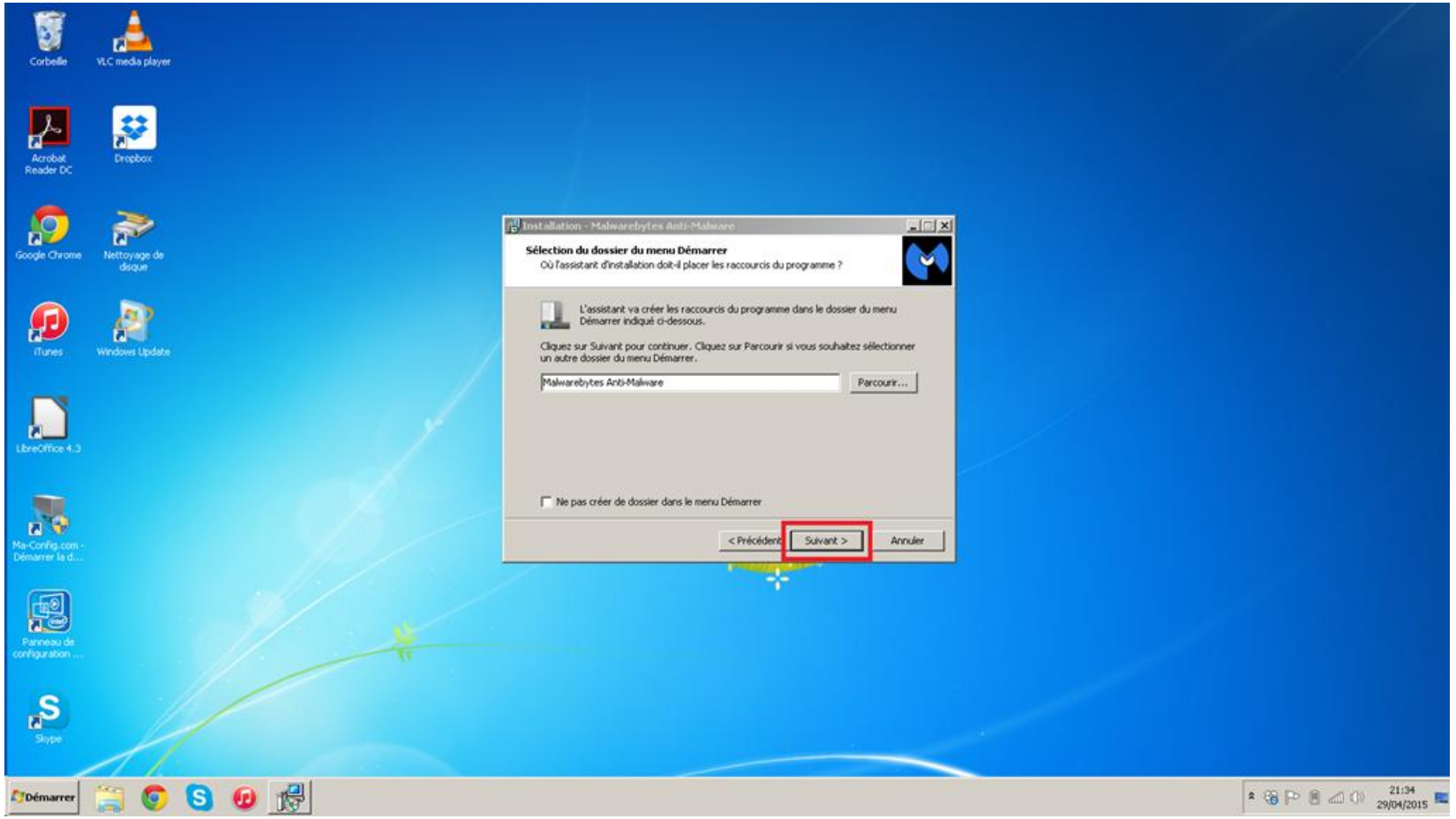
Cliquez sur « Suivant »



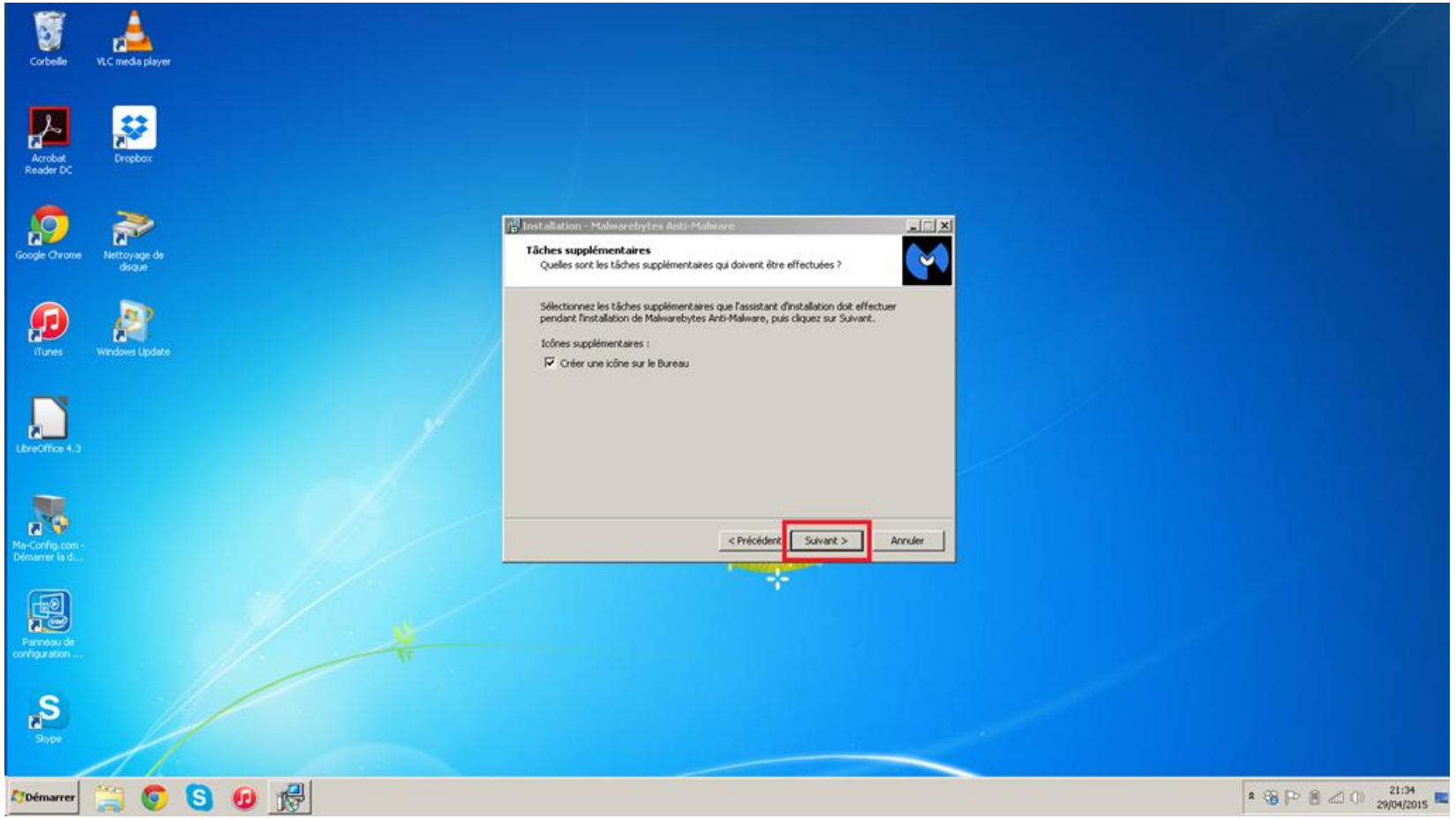
Cliquez sur « Suivant »



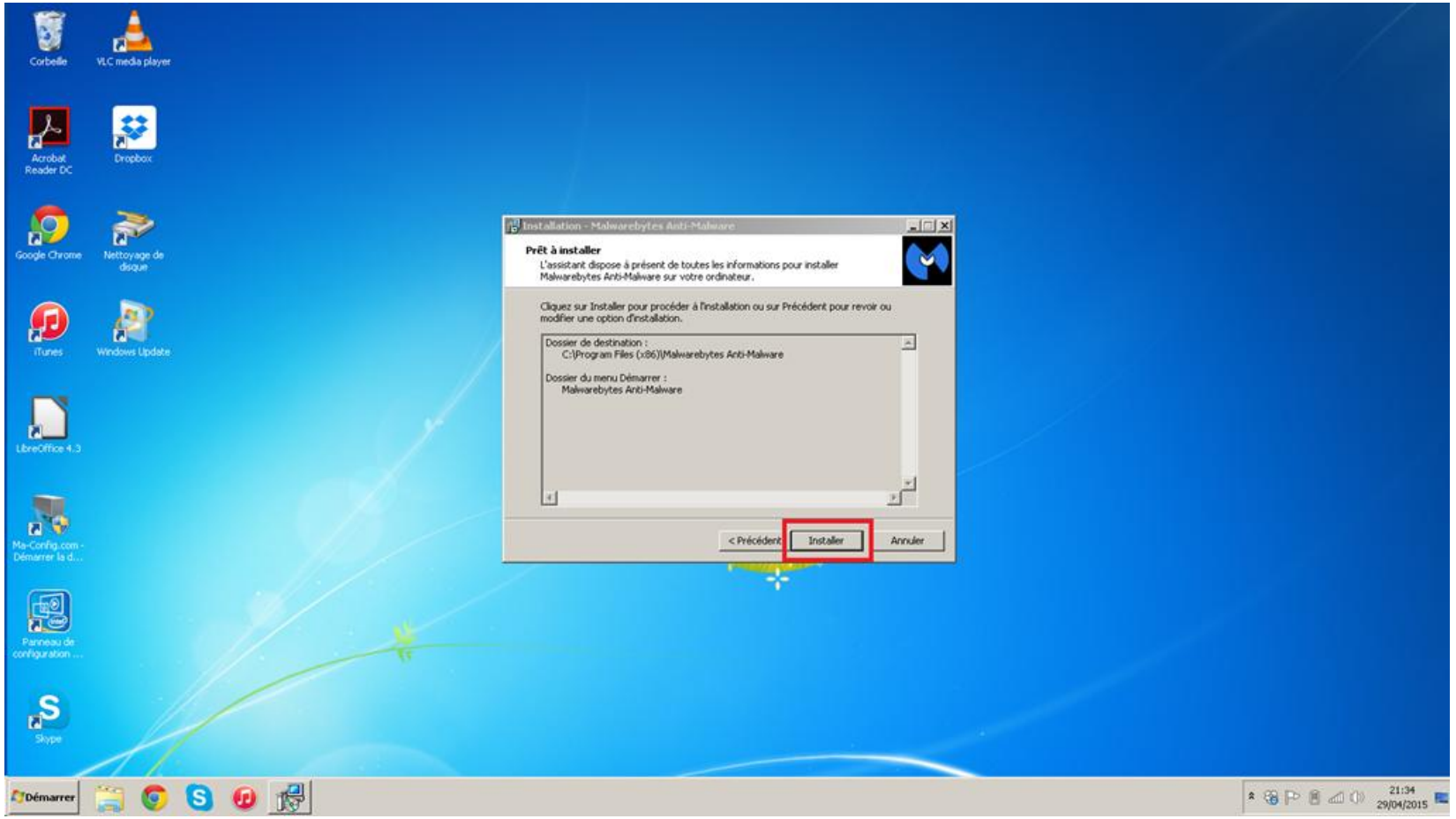
Cliquez sur « Suivant »



Cliquez sur « Suivant »

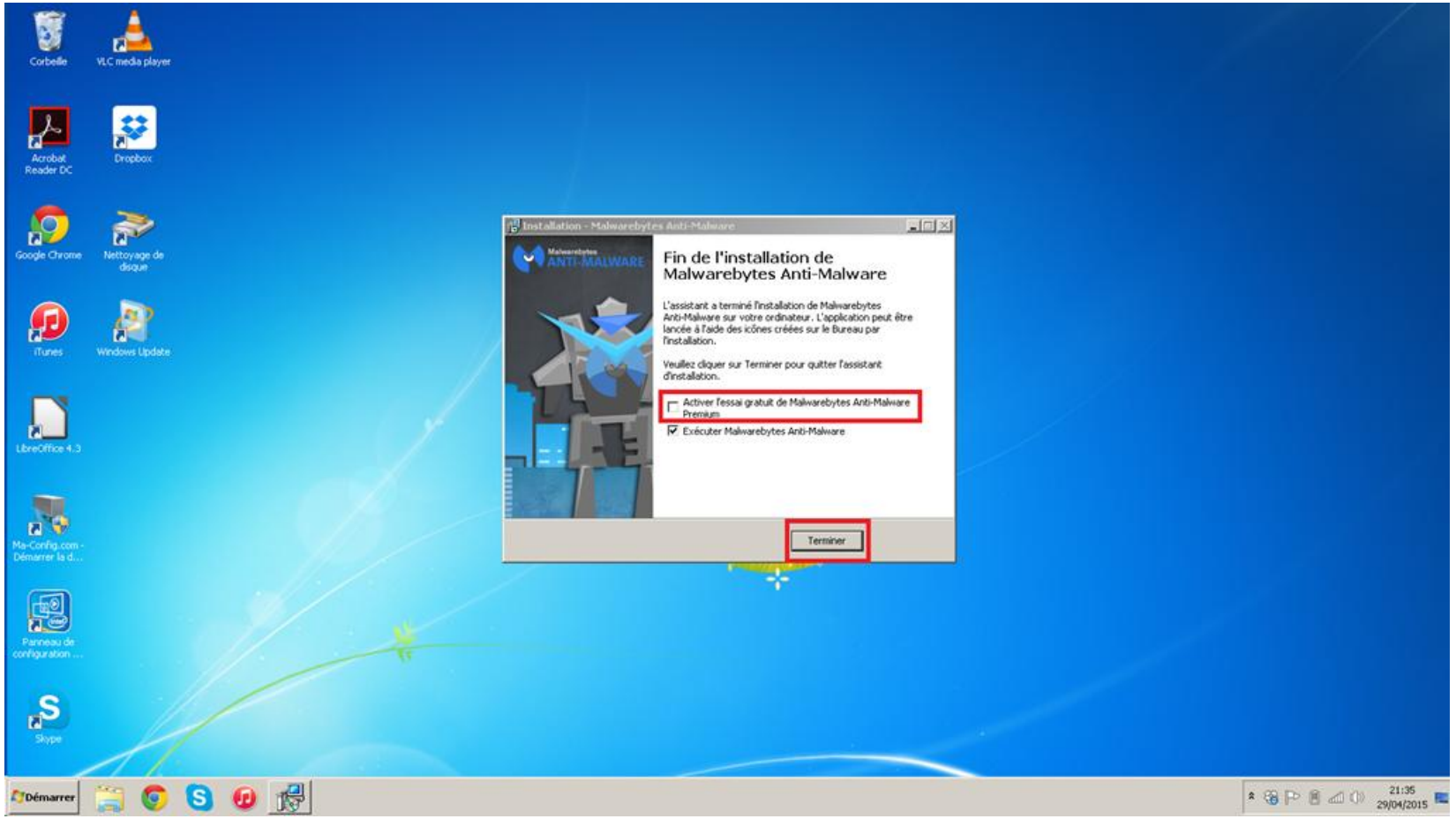


Cliquez sur « Installer »

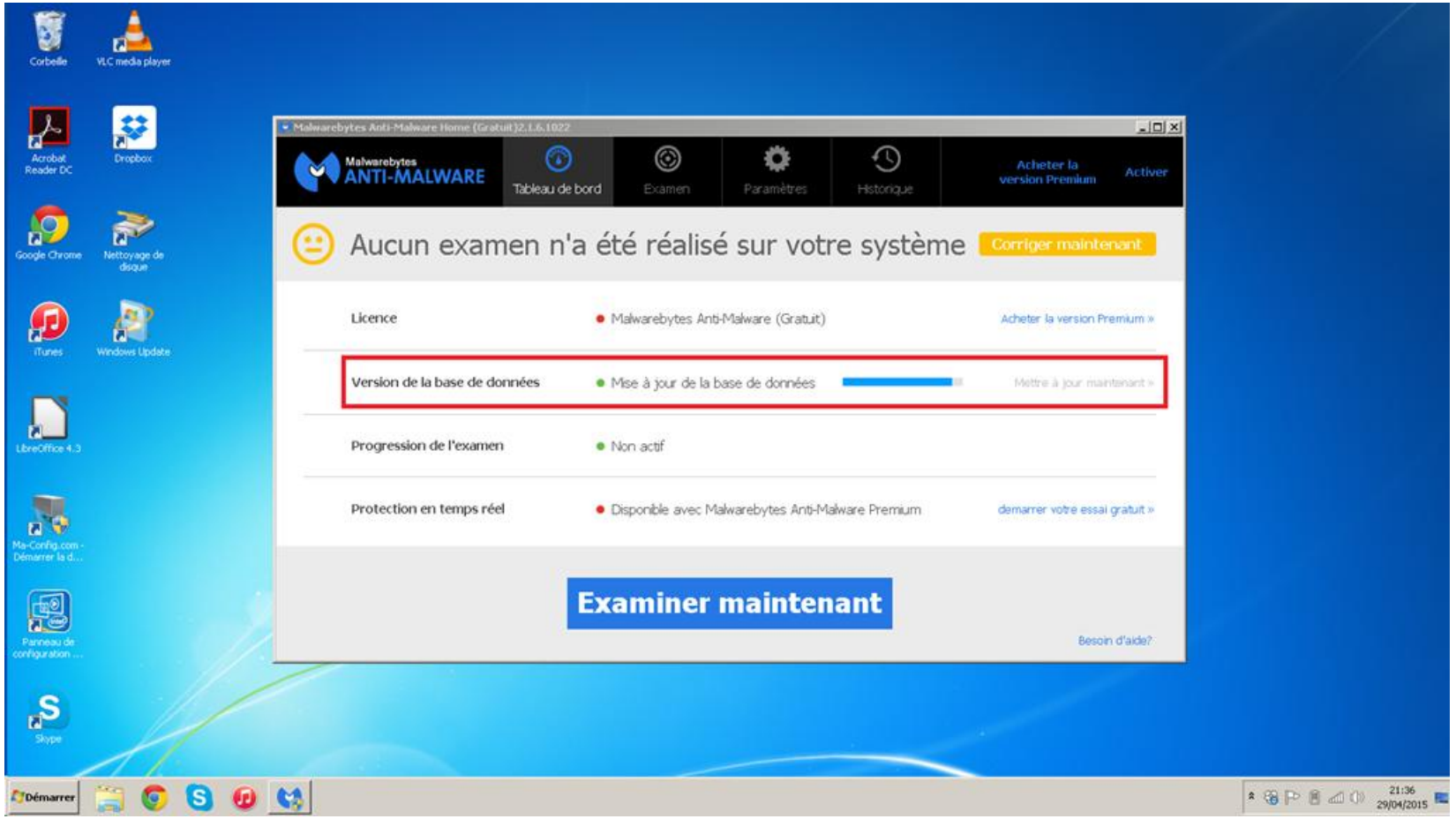


1. Décochez la case

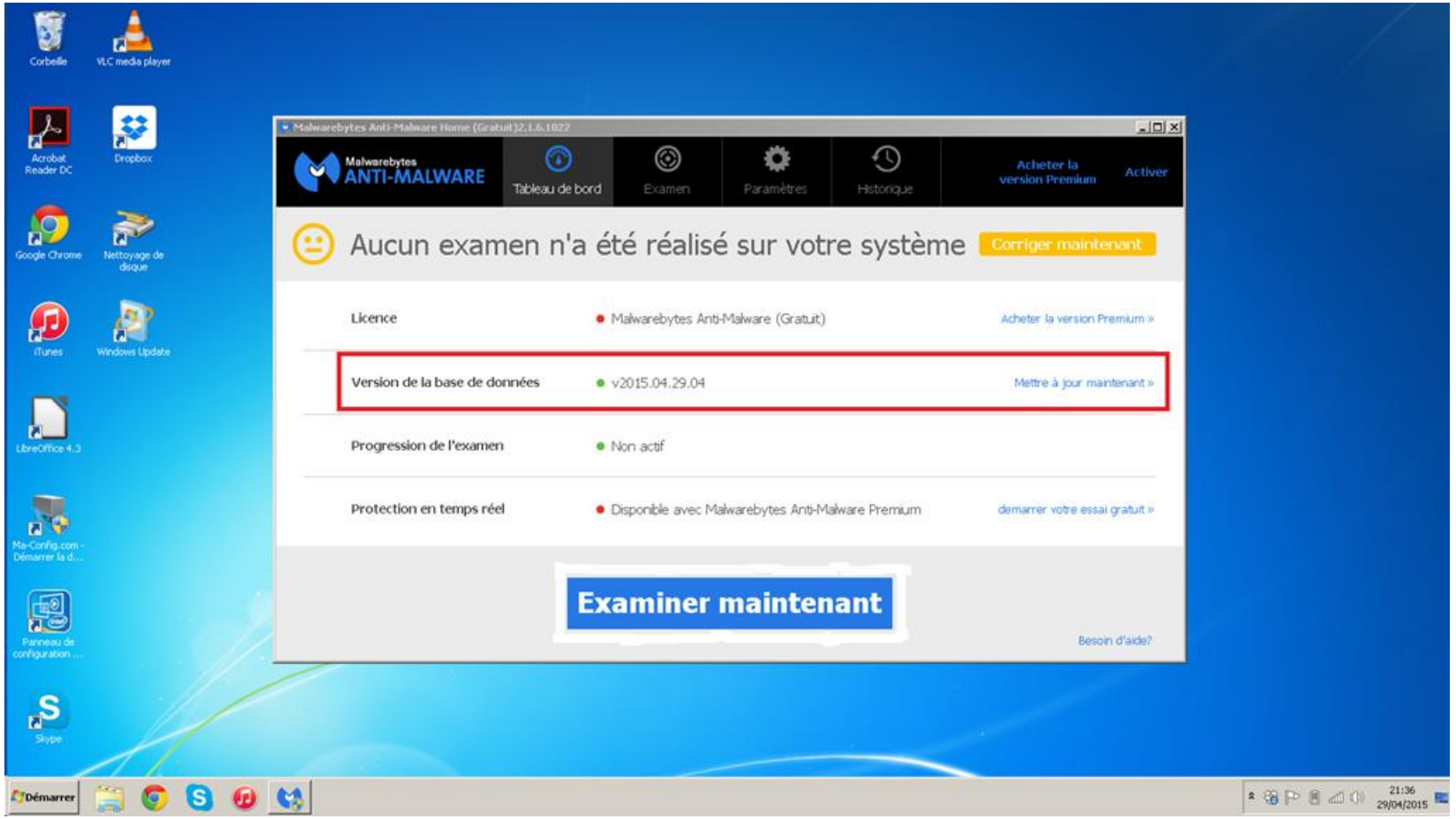
2. Cliquez sur « Terminer »



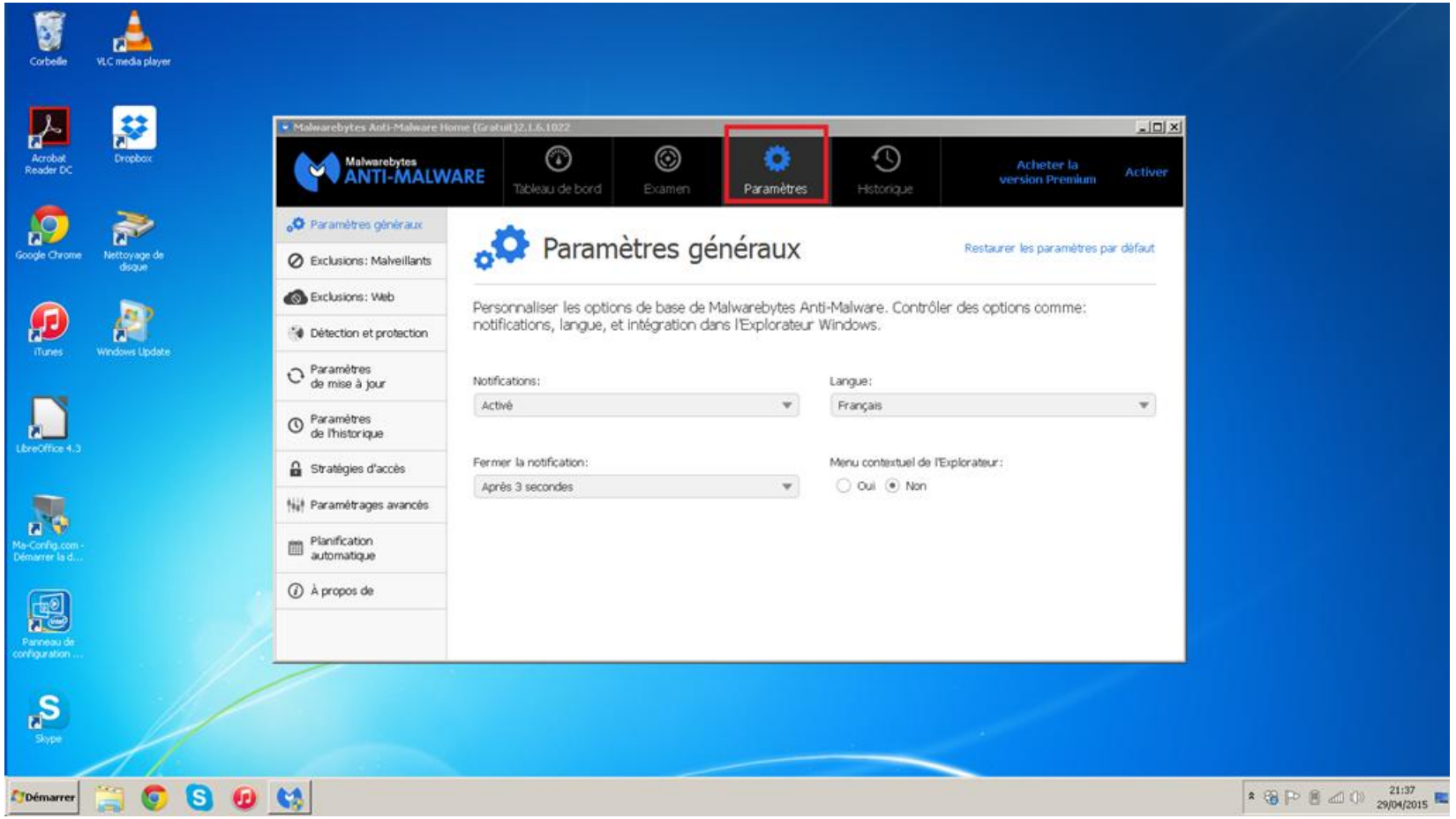
La base de données se met automatique à jour, patientez



La base de données est maintenant à jour



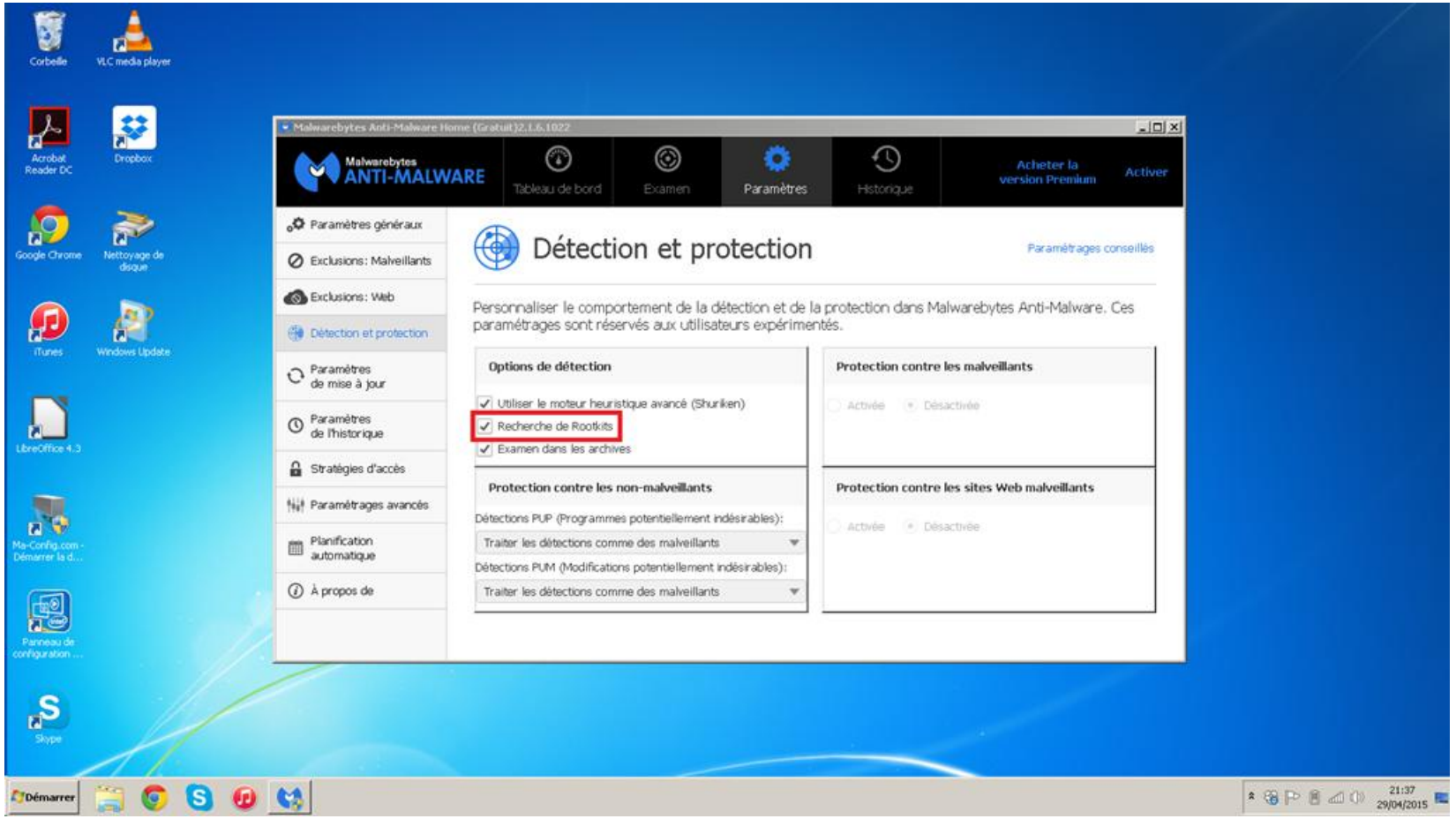
Cliquez sur « paramètres »



Cliquez sur

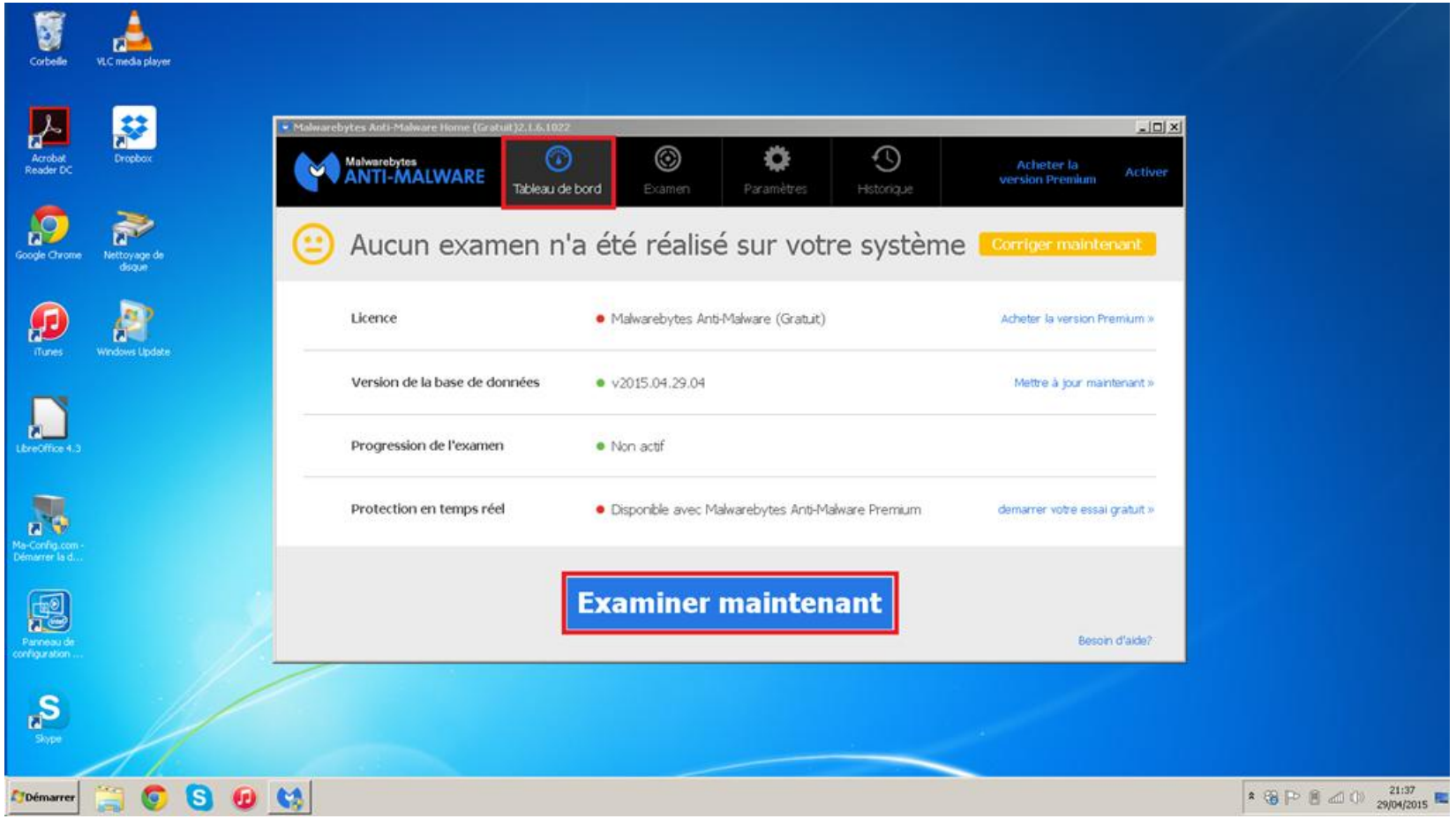
« détection et protection »

Cochez la case

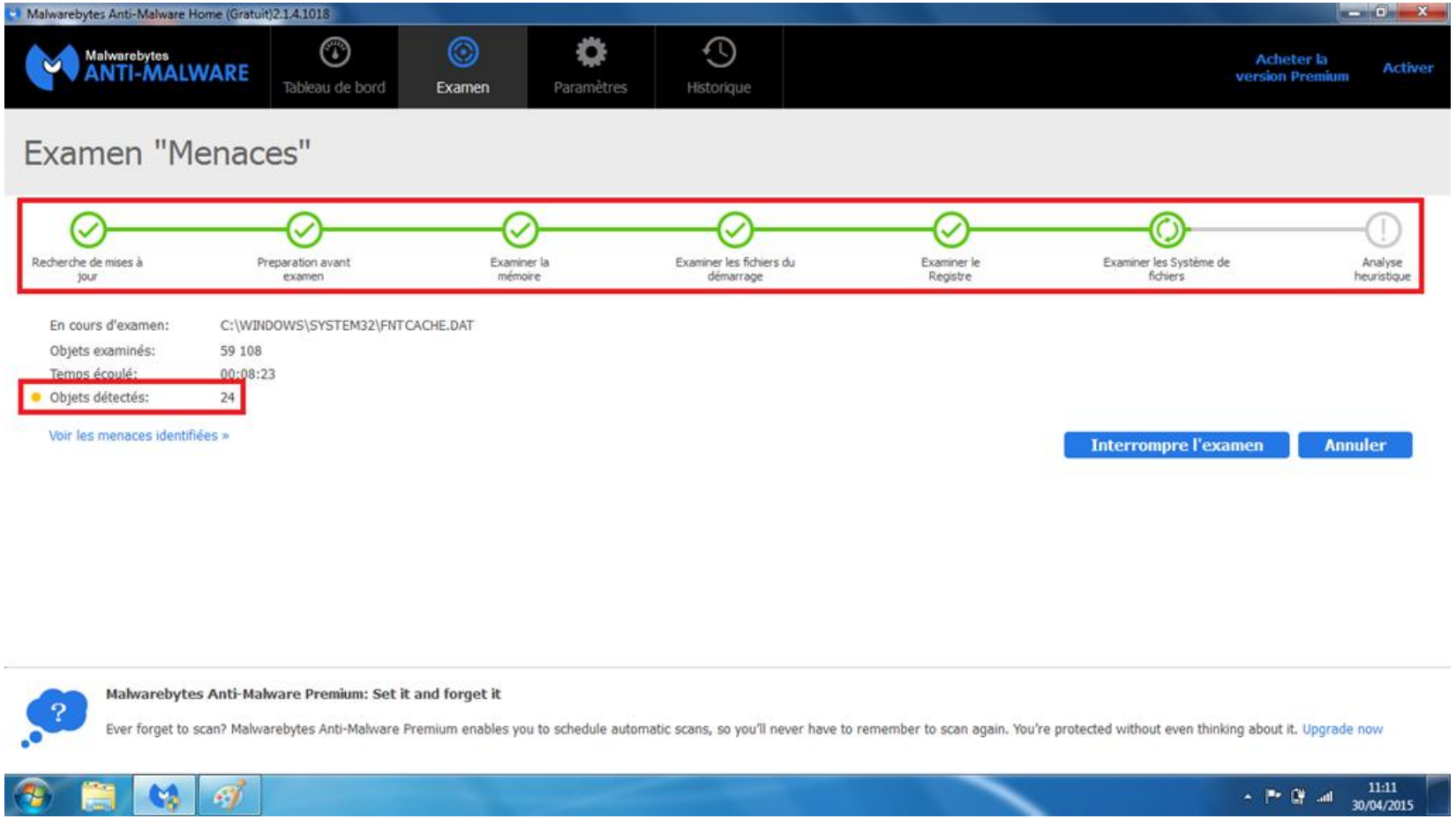


1. Cliquez sur « tableau de bord »

2. Puis sur « Examiner maintenant »

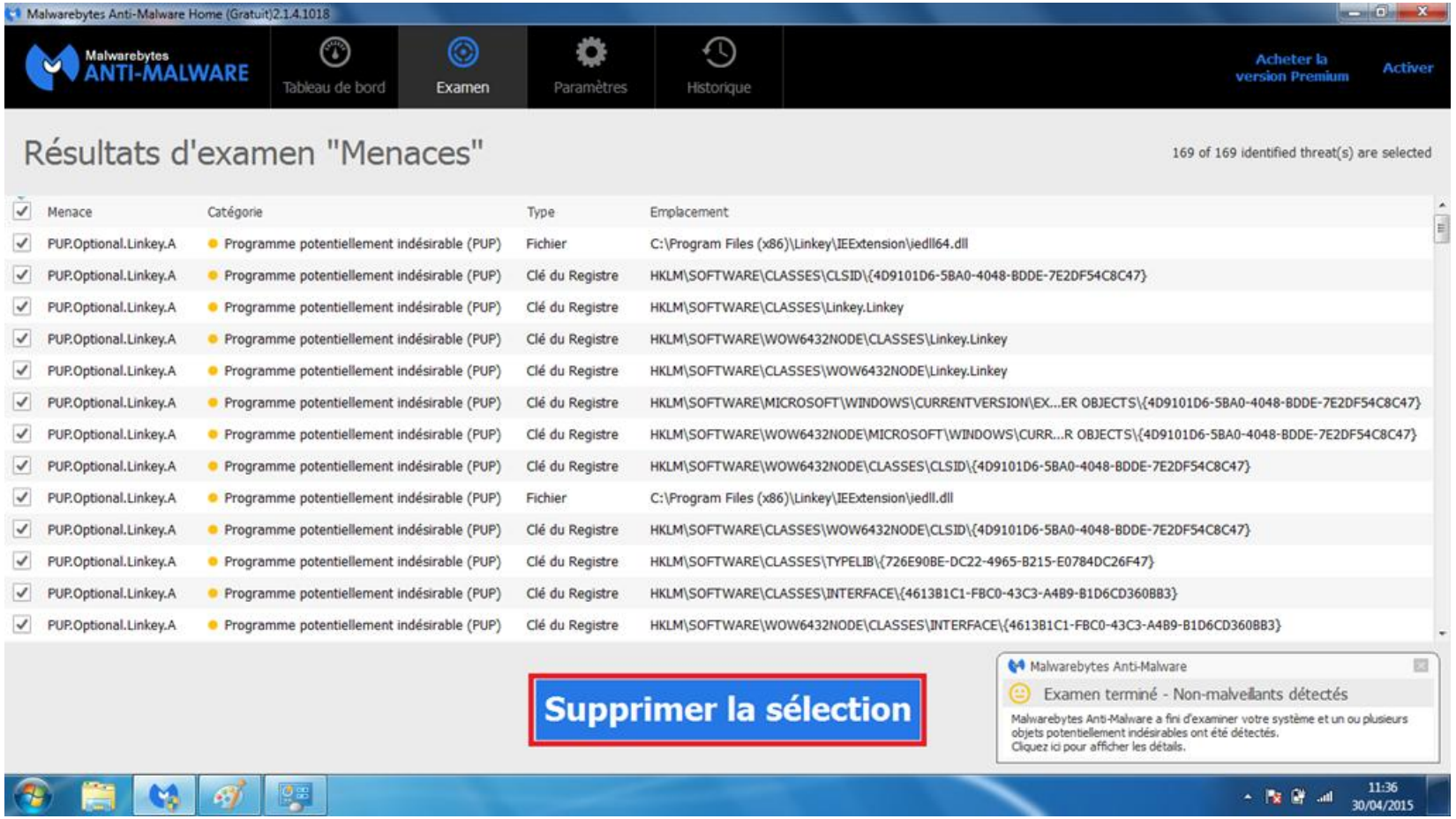


Durant l'examen, des menaces sont détectées

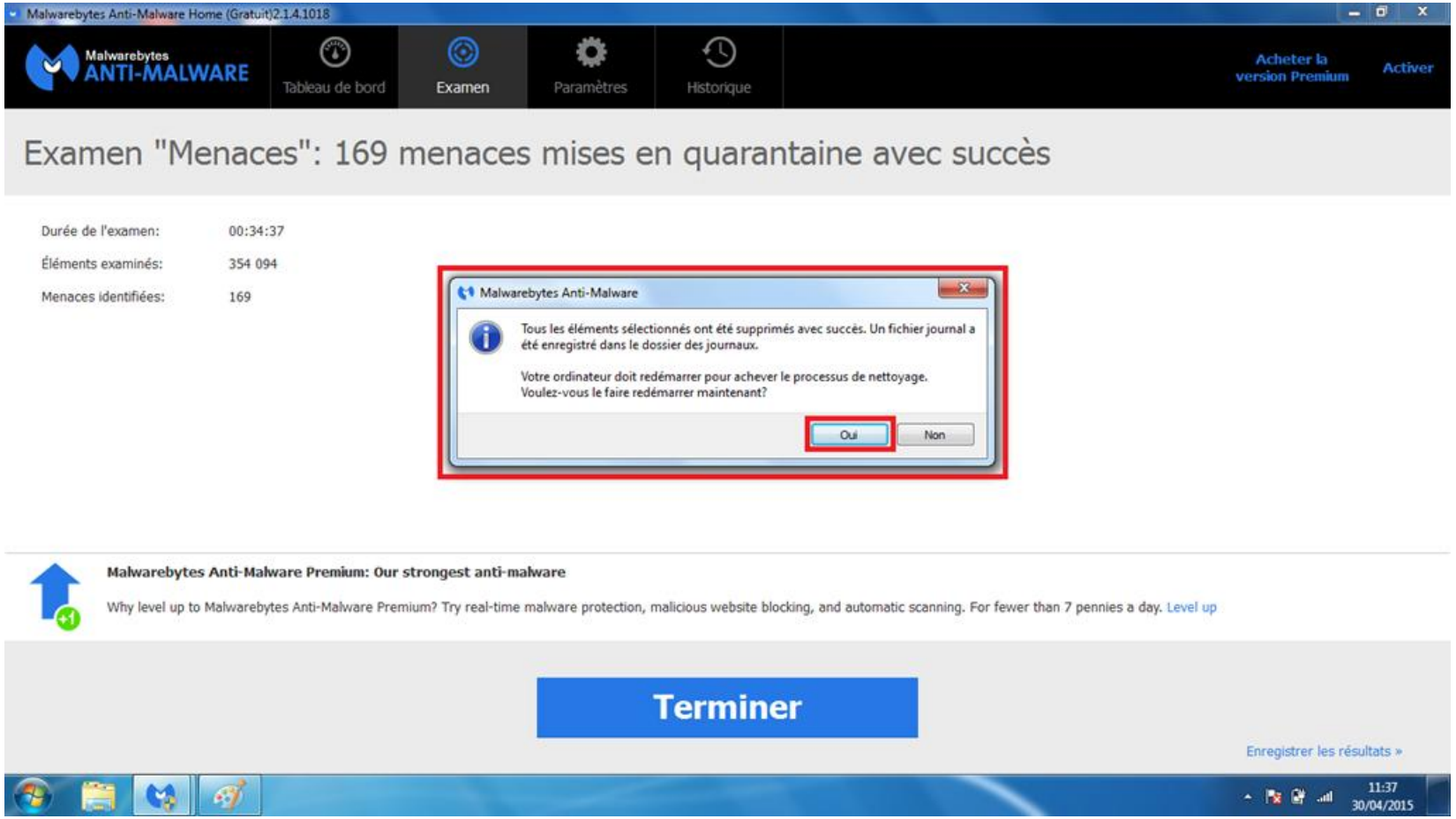


L'examen se termine, cliquez sur

« Supprimer la sélection »



Patientez que la fenêtre apparaisse, puis cliquez sur « Oui »



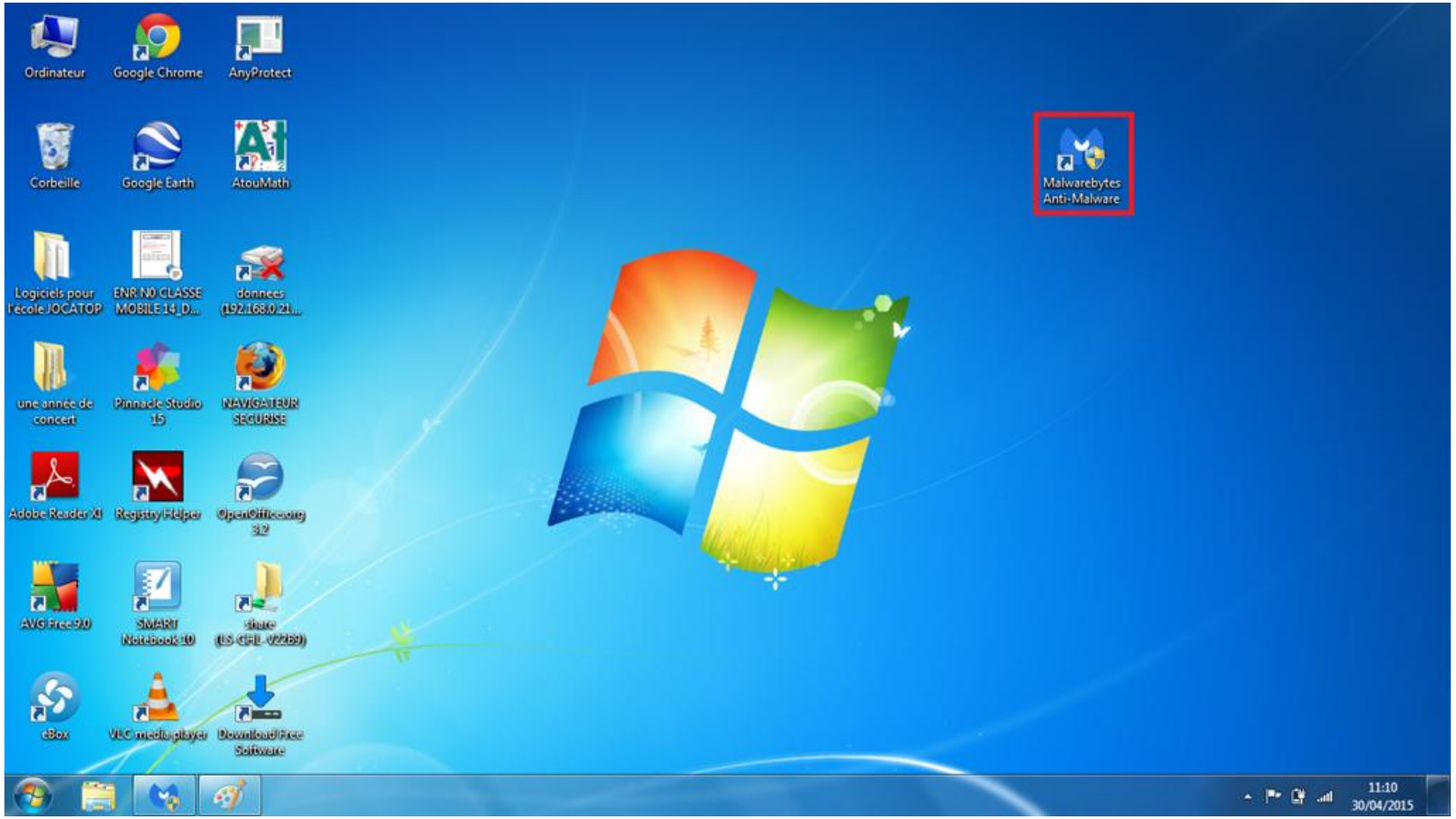
L'ordinateur redémarre, vous avez terminé !

5.2.1 Malwarebytes,

Nouvelle analyse

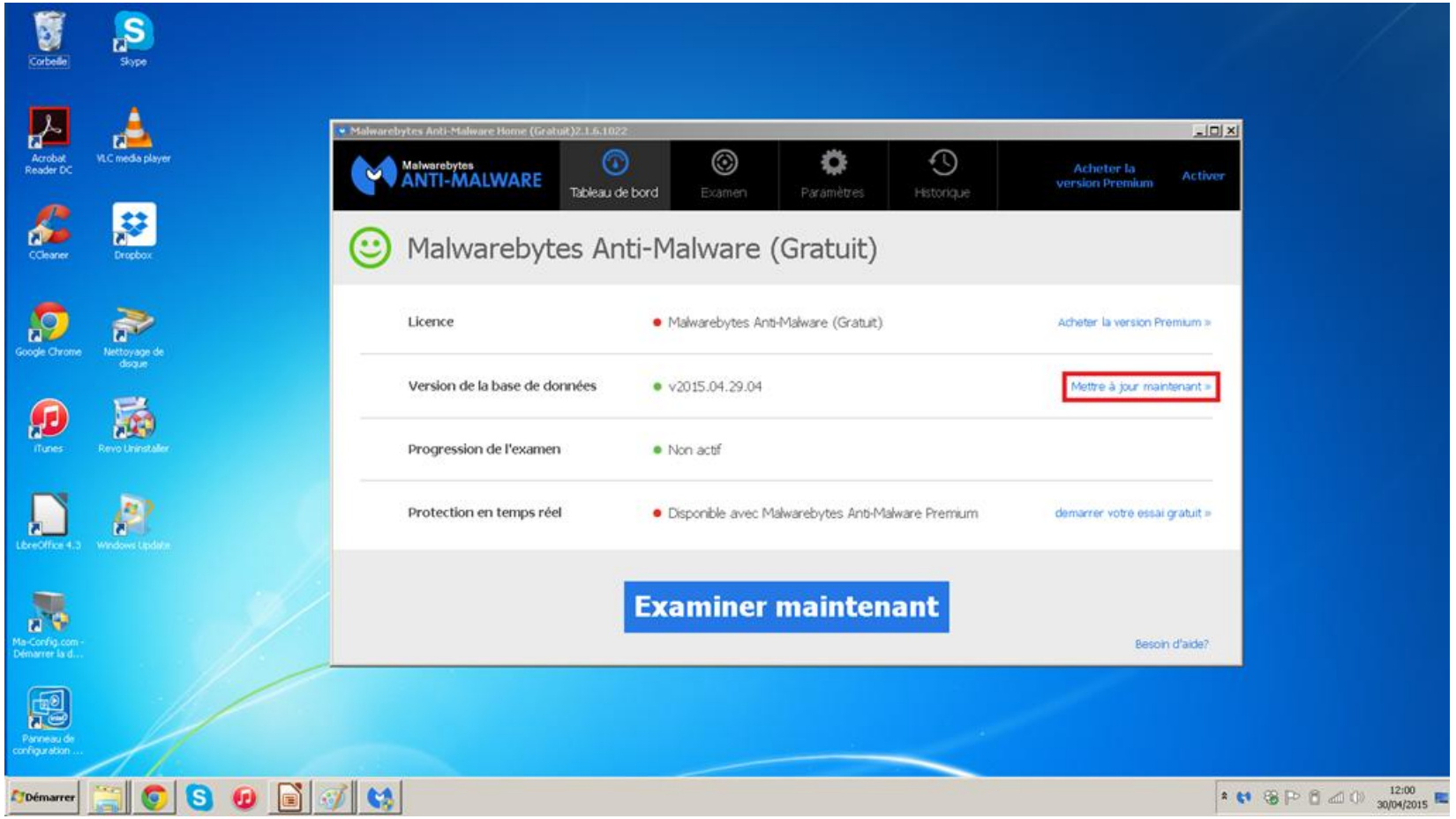
- Vous pouvez effectuer une contre analyse tout de suite après la première, ou de façon régulière et préventive.
- Pour se faire, la suite en image..

Cliquez sur l'icône du bureau



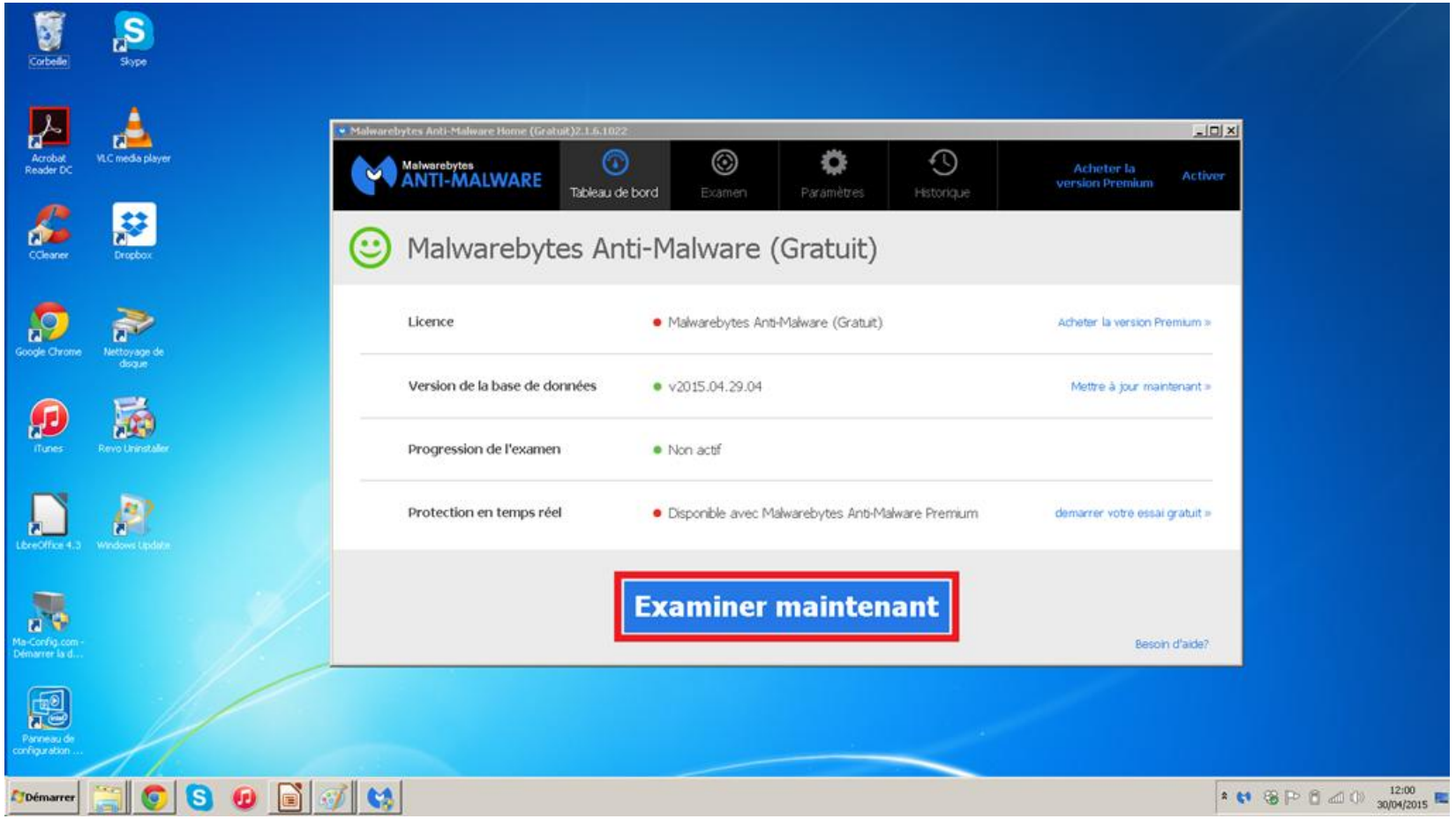
Le programme se lance, cliquez sur

« Mettre à jour maintenant »

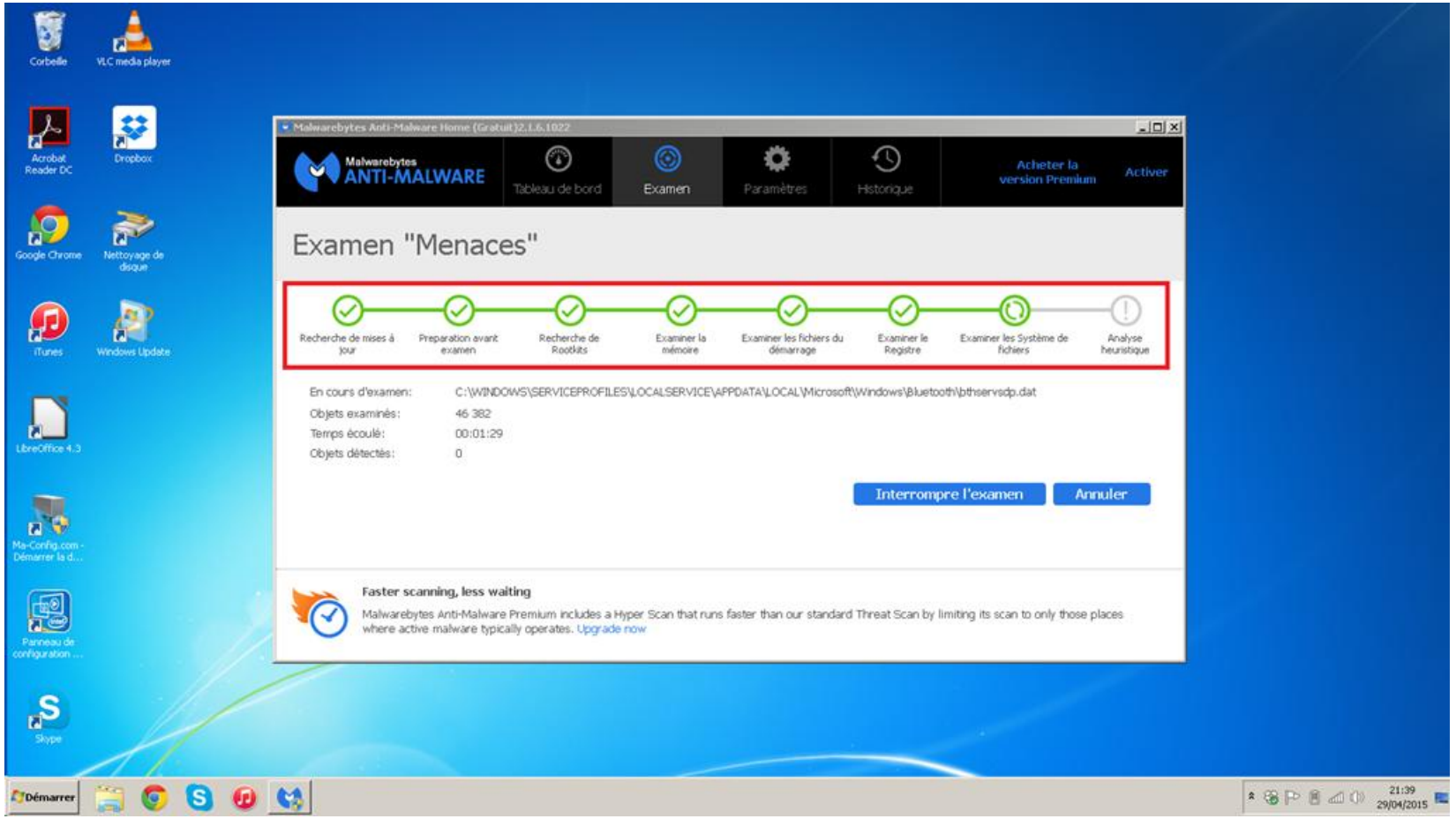


Une fois le programme assurément à jour, cliquez sur

« Examiner »

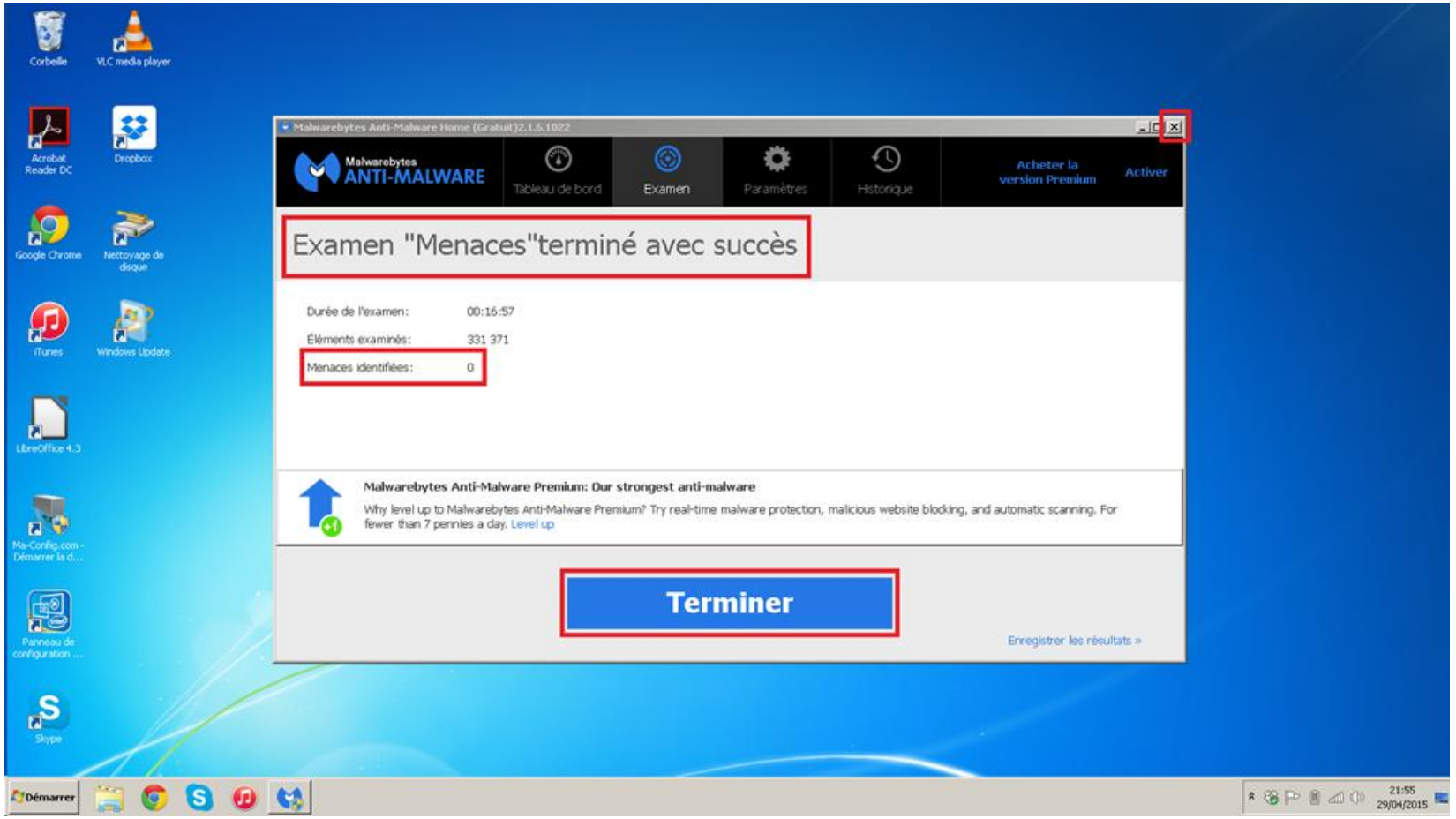


Patientez pendant l'analyse



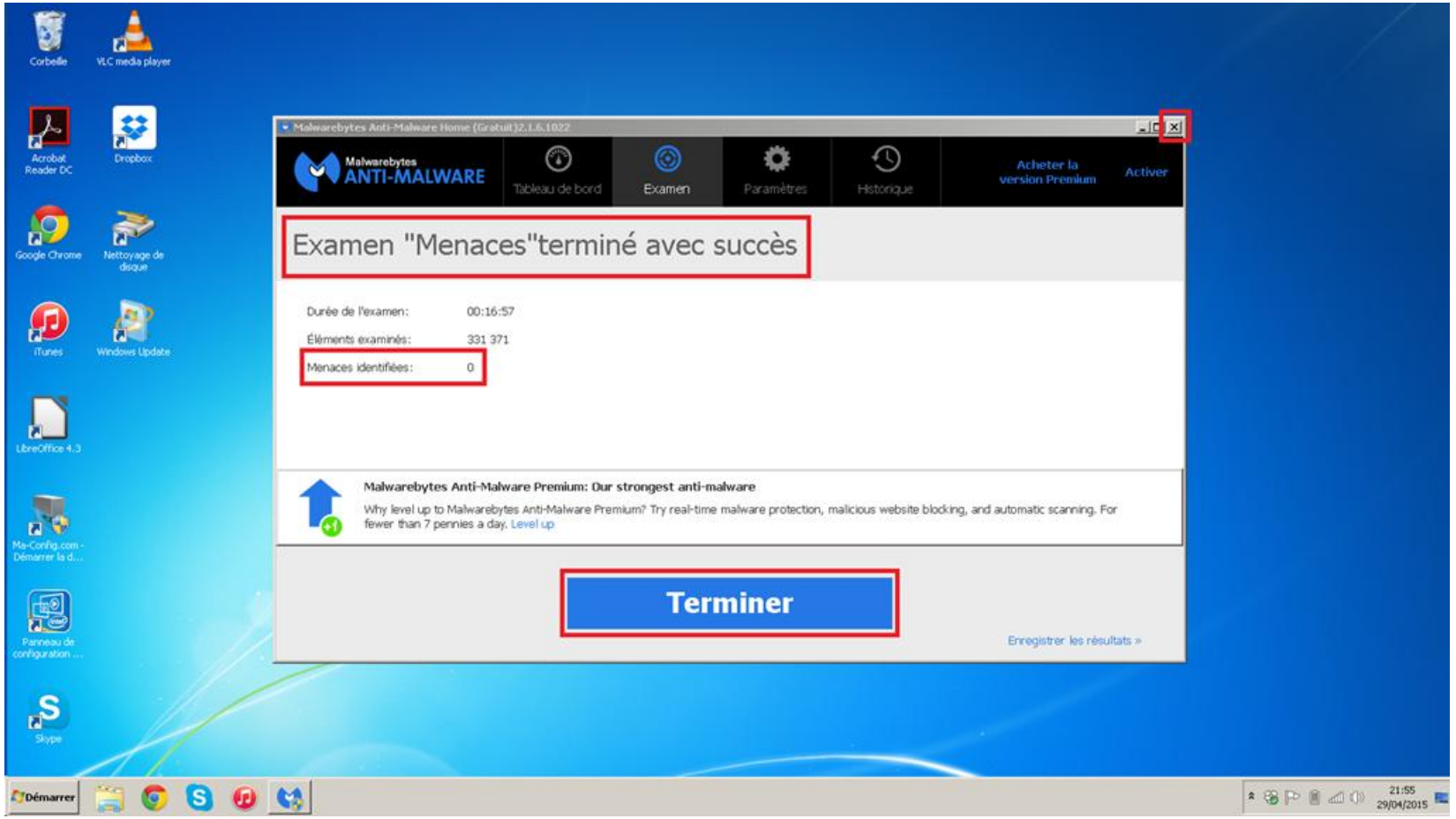
L'examen est terminé,

aucune menace n'a été détectée



1. Cliquez sur « Terminer »

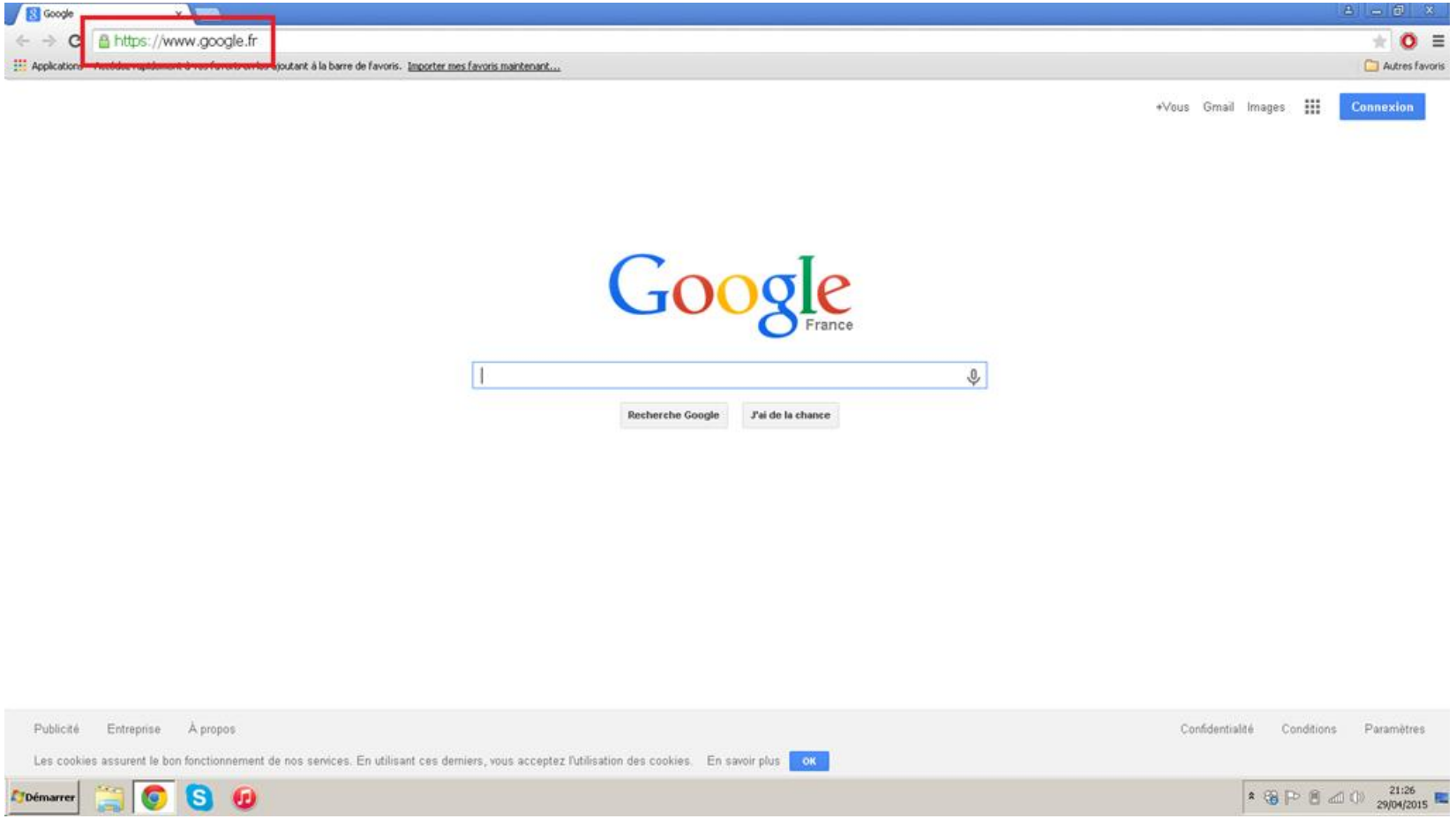
2. Fermez en cliquant sur la croix »



5.3 ADWCleaner

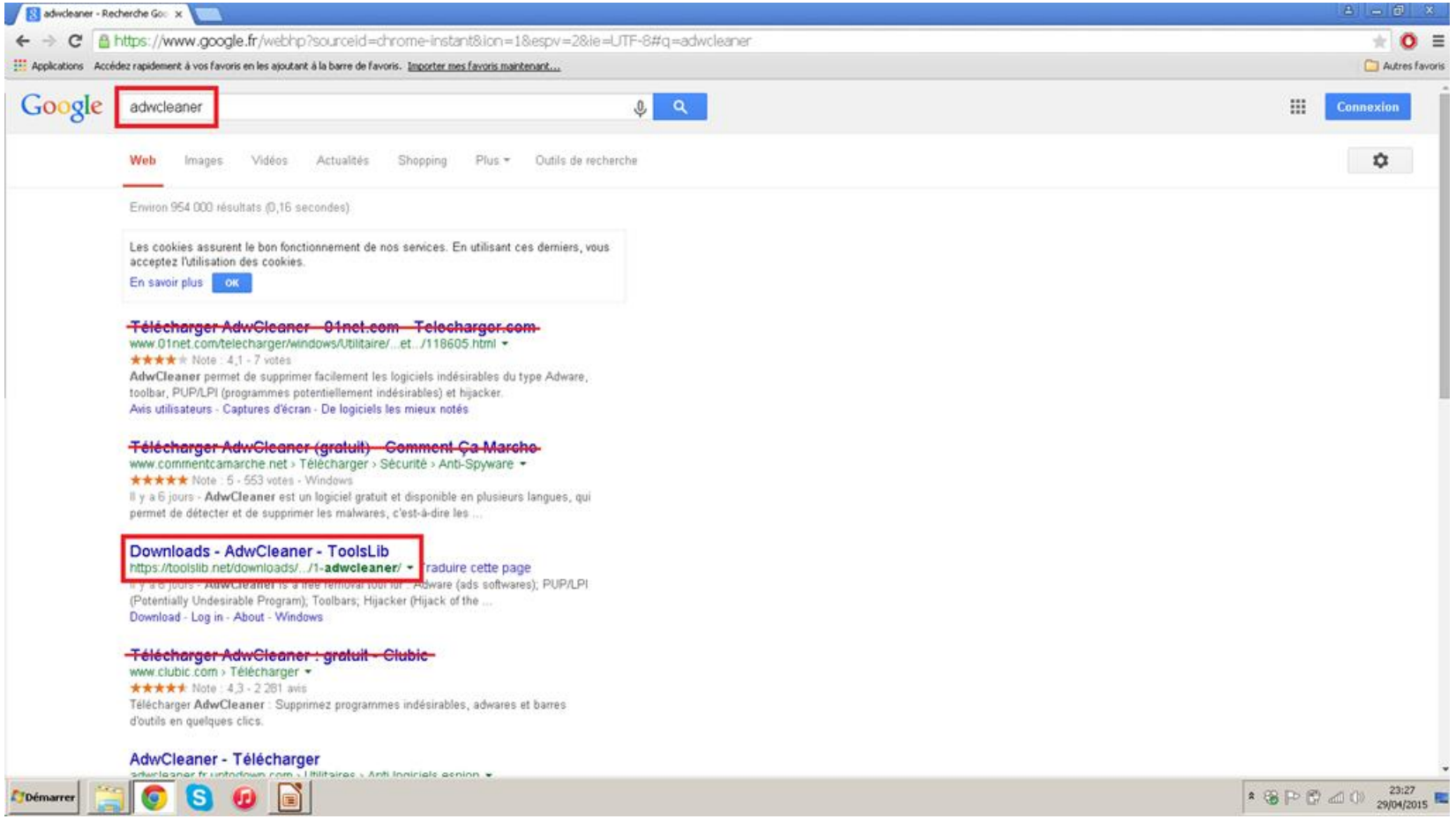
- Téléchargez et exécutez ce programme dit « portable », en effet lorsque vous exécutez ce programme il ne s'installe pas dans votre ordinateur. Il est 100 % gratuit et disponible sur le site « toolslib.net »

Rendez-vous sur Google

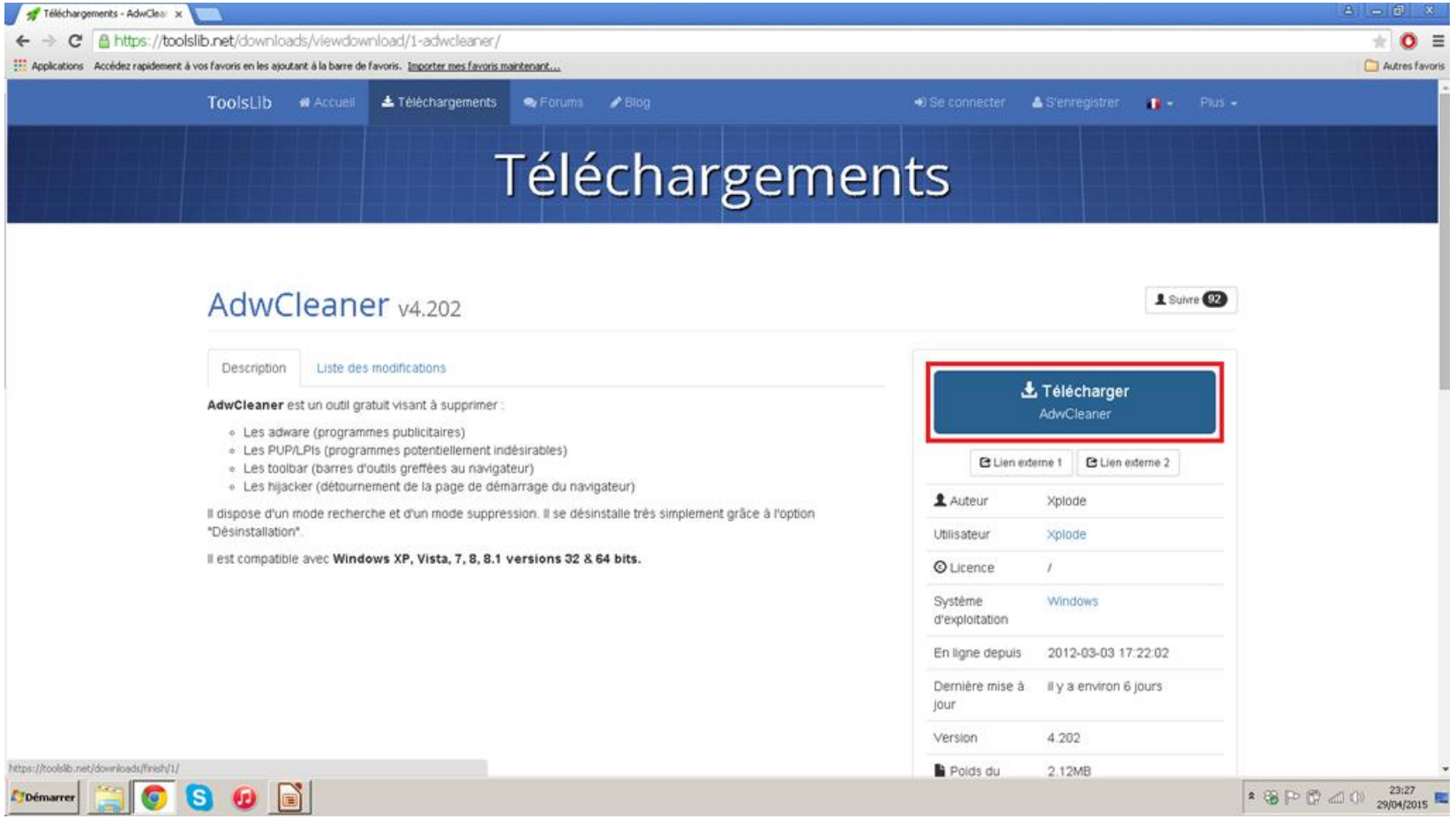


1. Tapez votre recherche

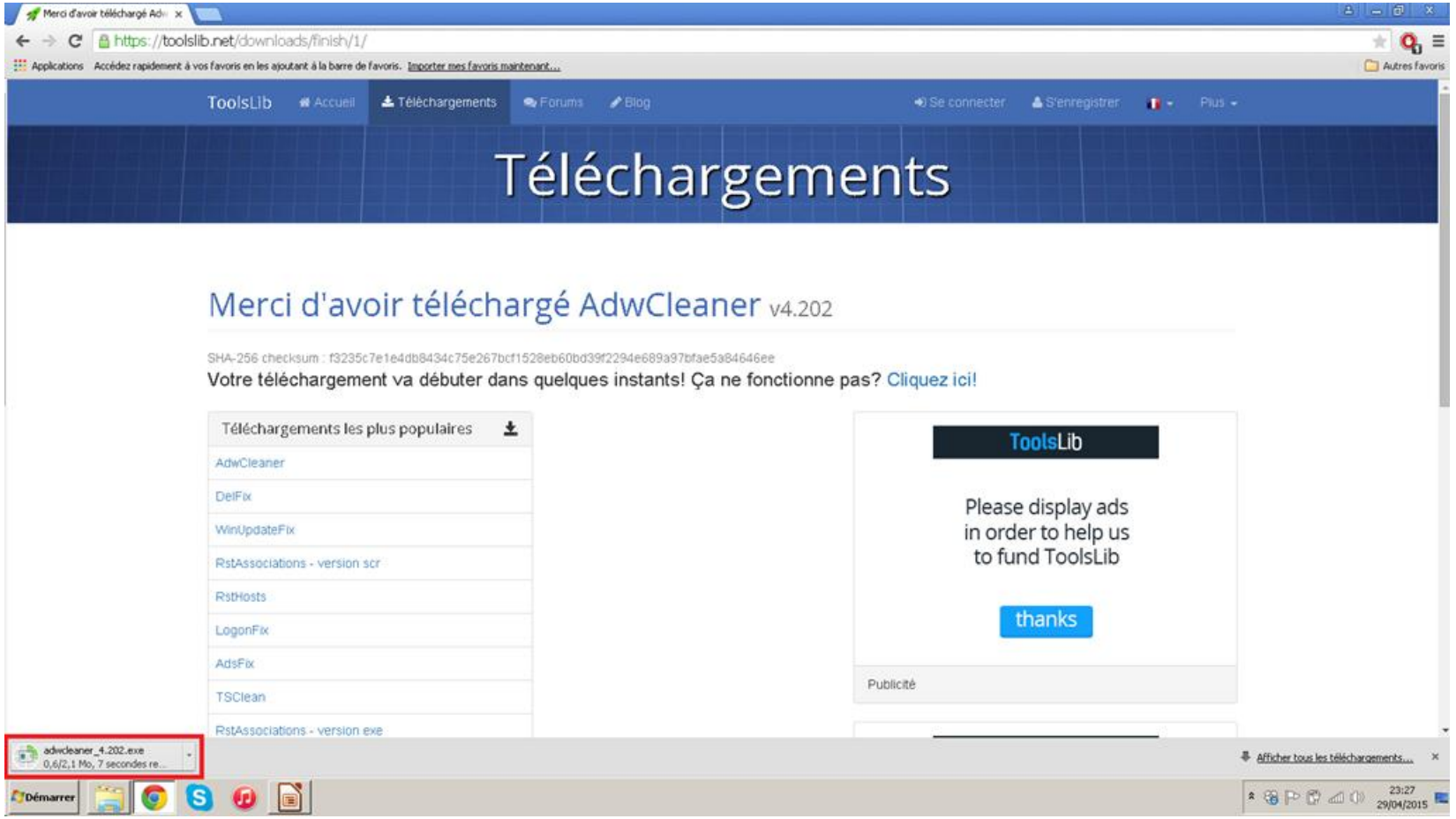
2.Cliquez sur le lien



Cliquez sur « Télécharger »

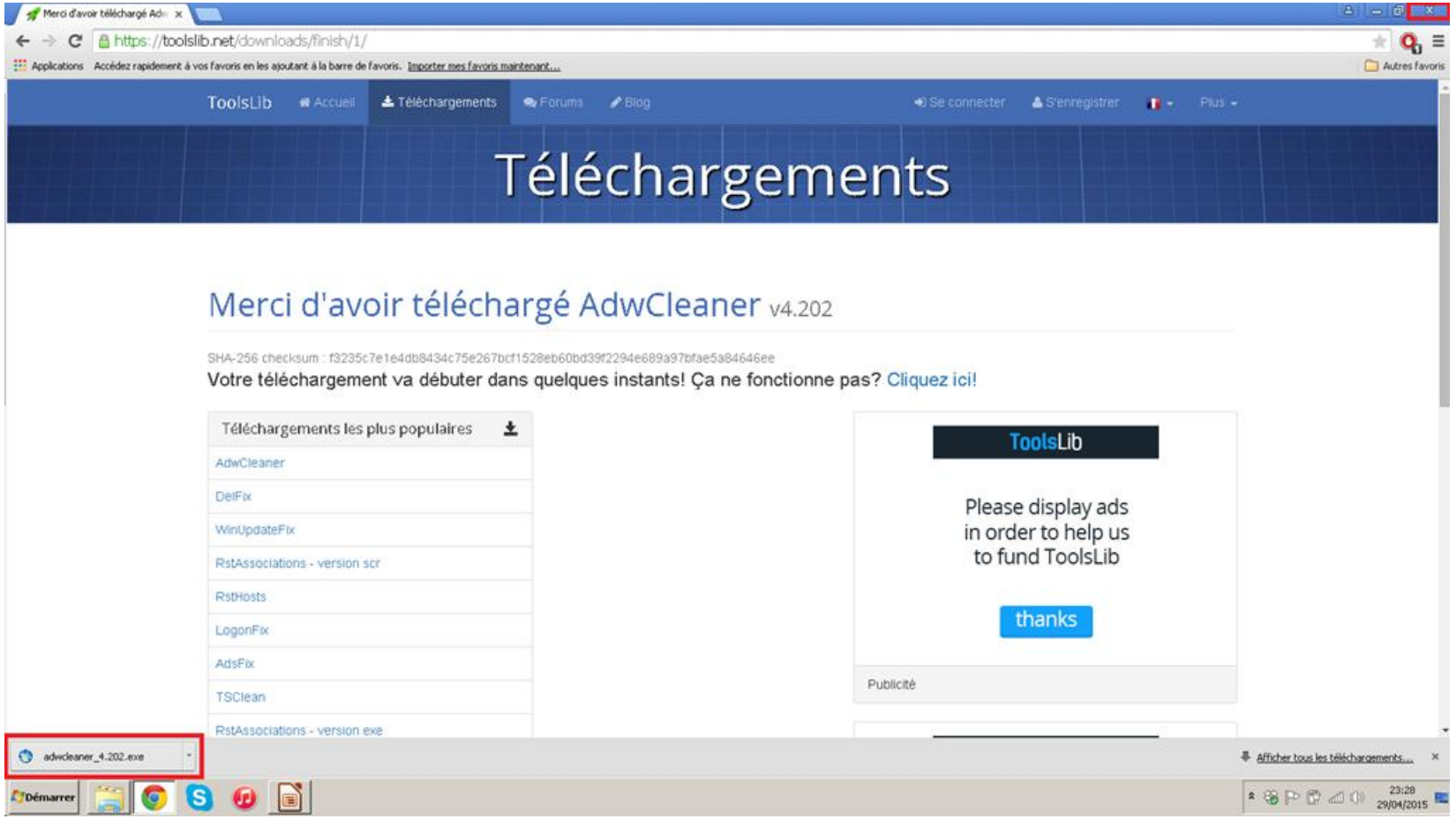


Le fichier est en cours de téléchargement

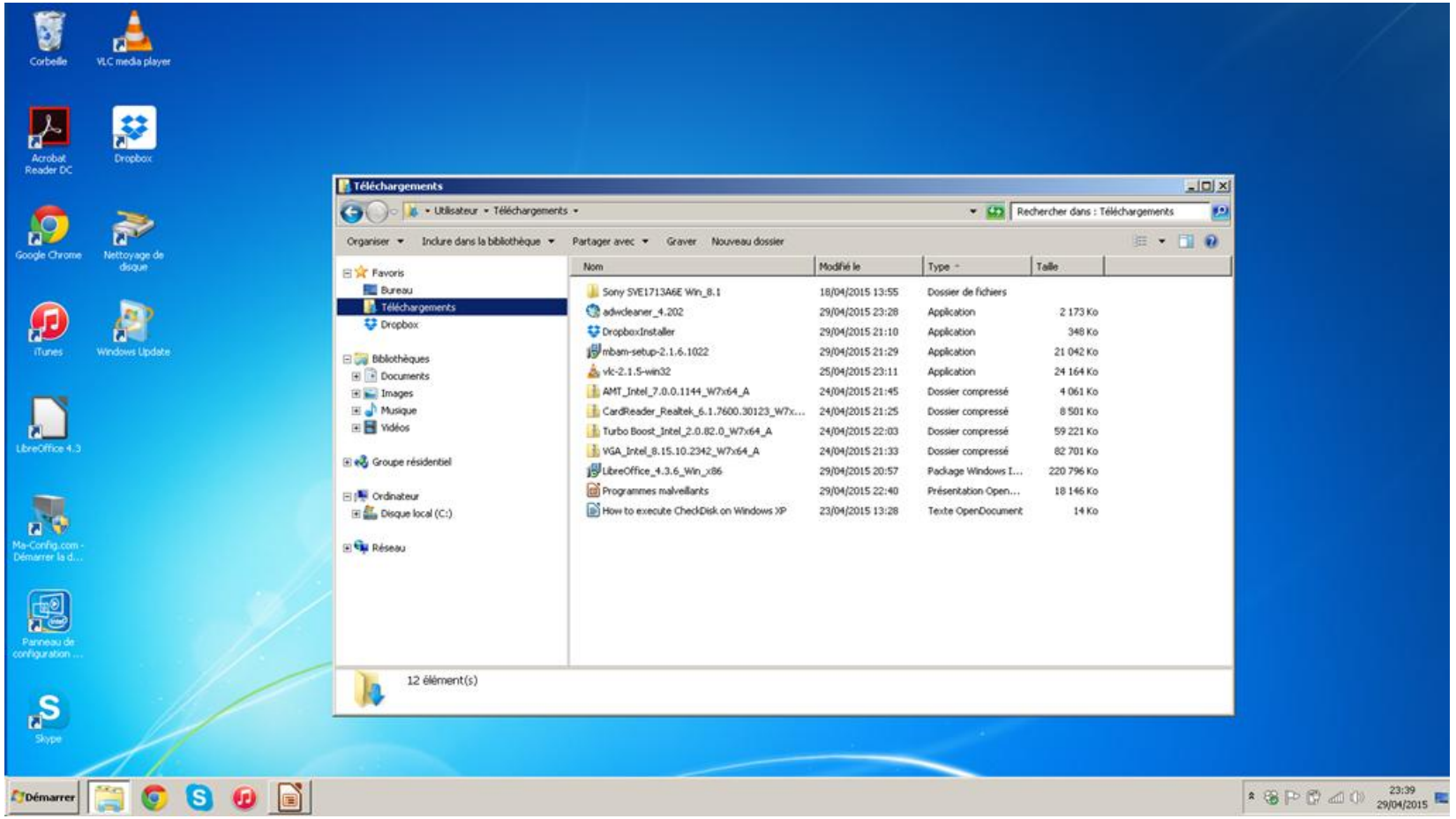


Le fichier est téléchargé,

vous pouvez refermer Internet

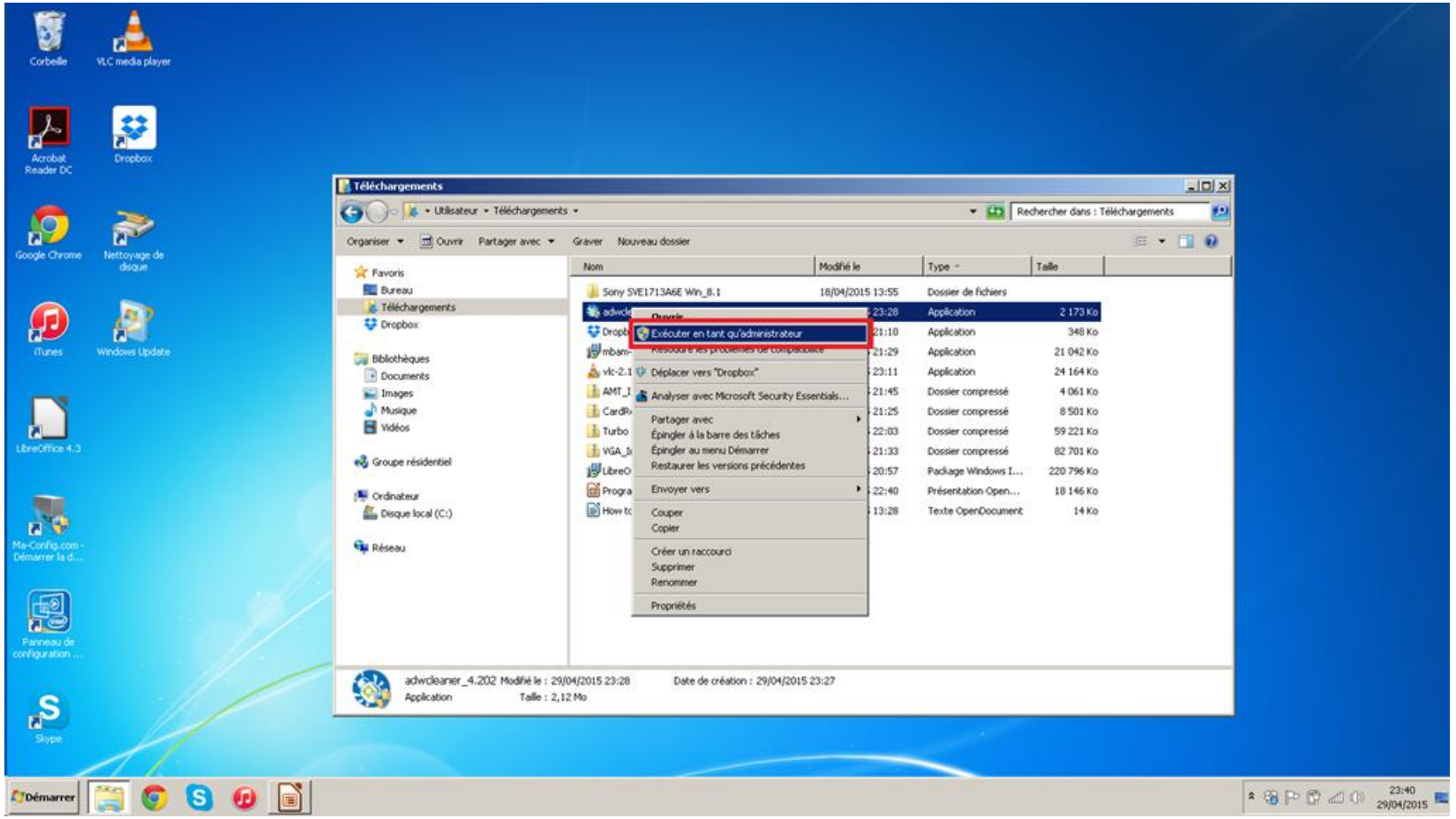


Rendez-vous dans votre dossier « Téléchargements »

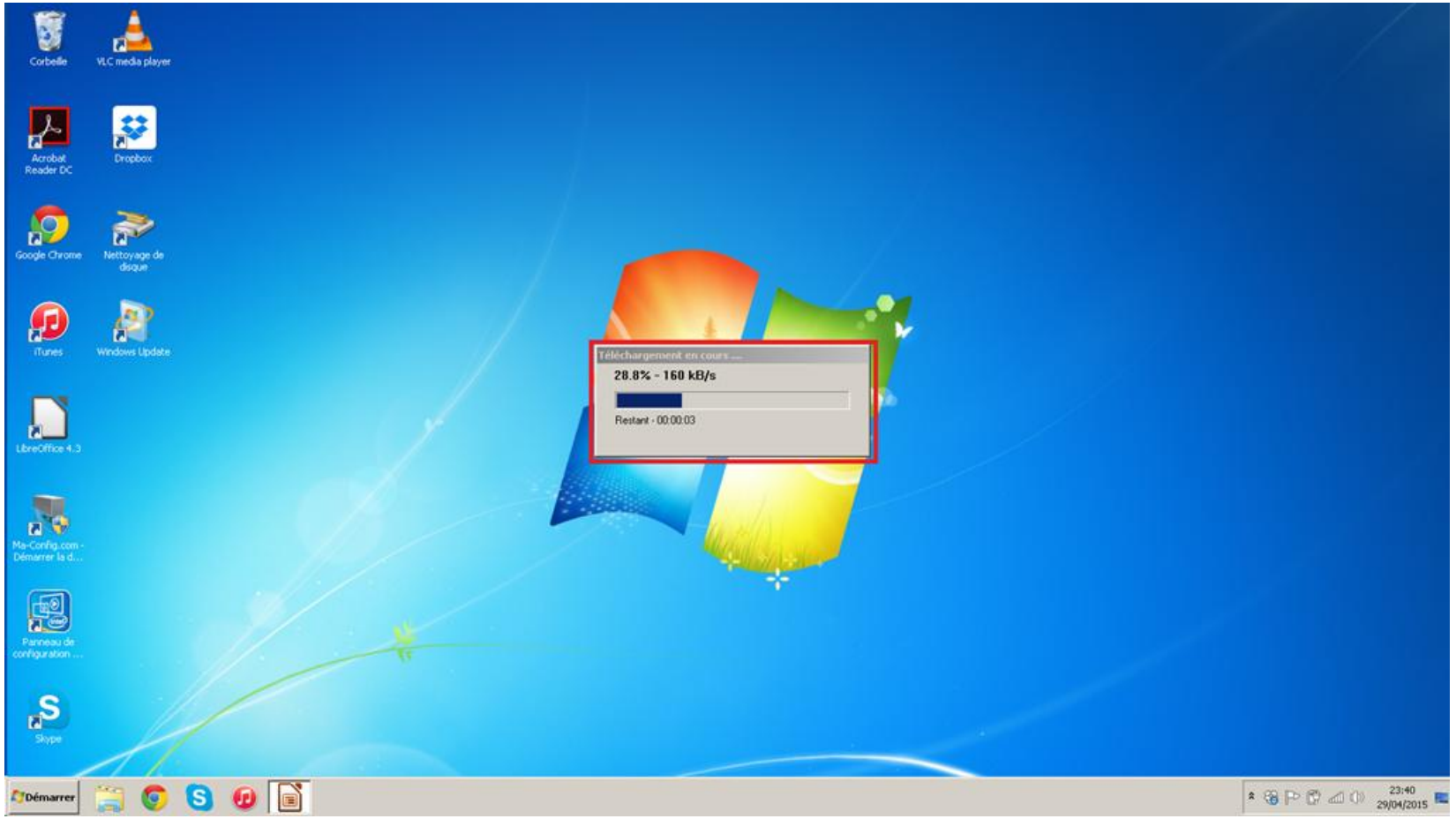


1. Cliquez droit sur « adwcleaner »

2. Cliquez gauche sur « exécuter.. »

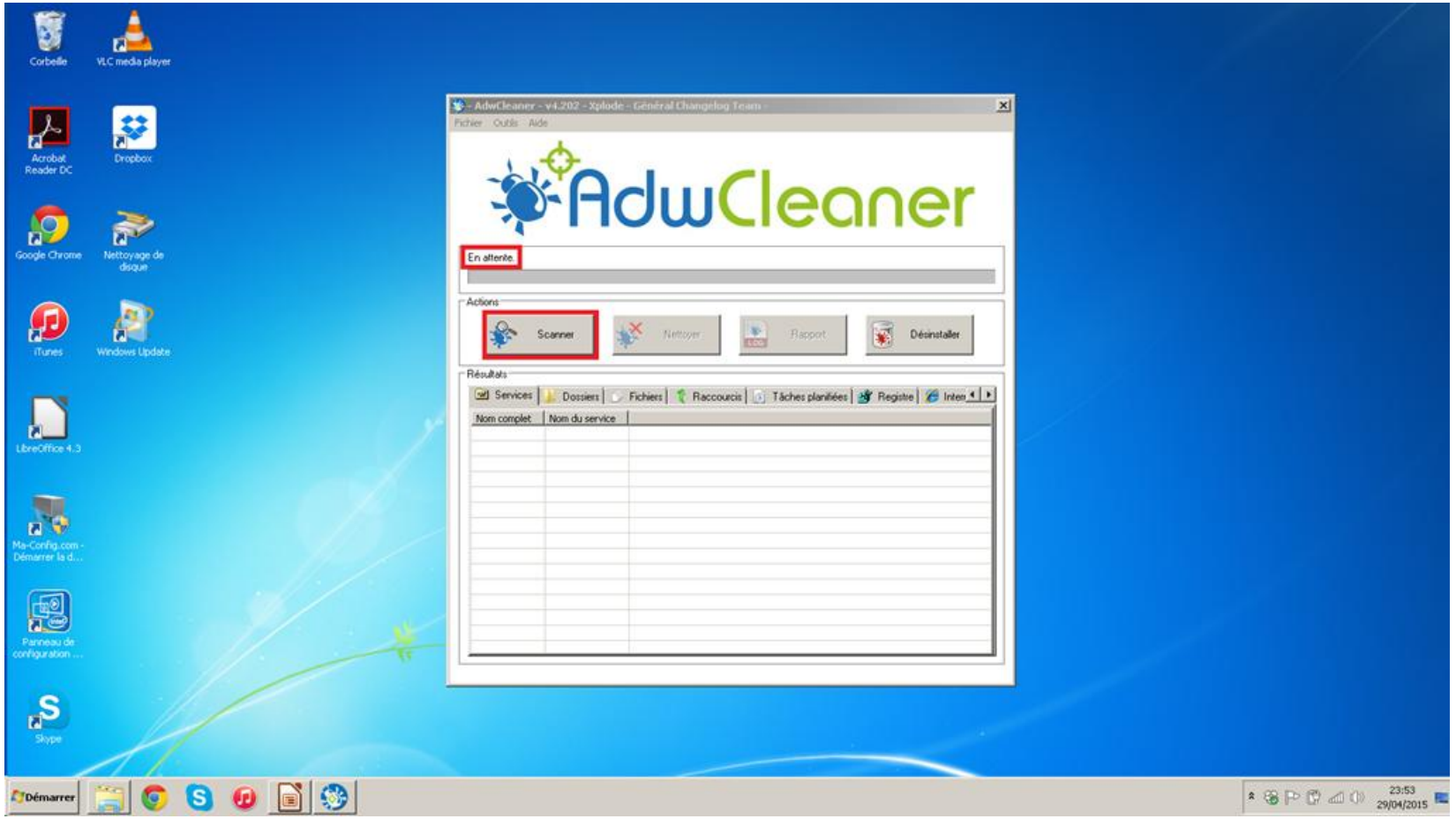


Le programme met à jour sa base de données



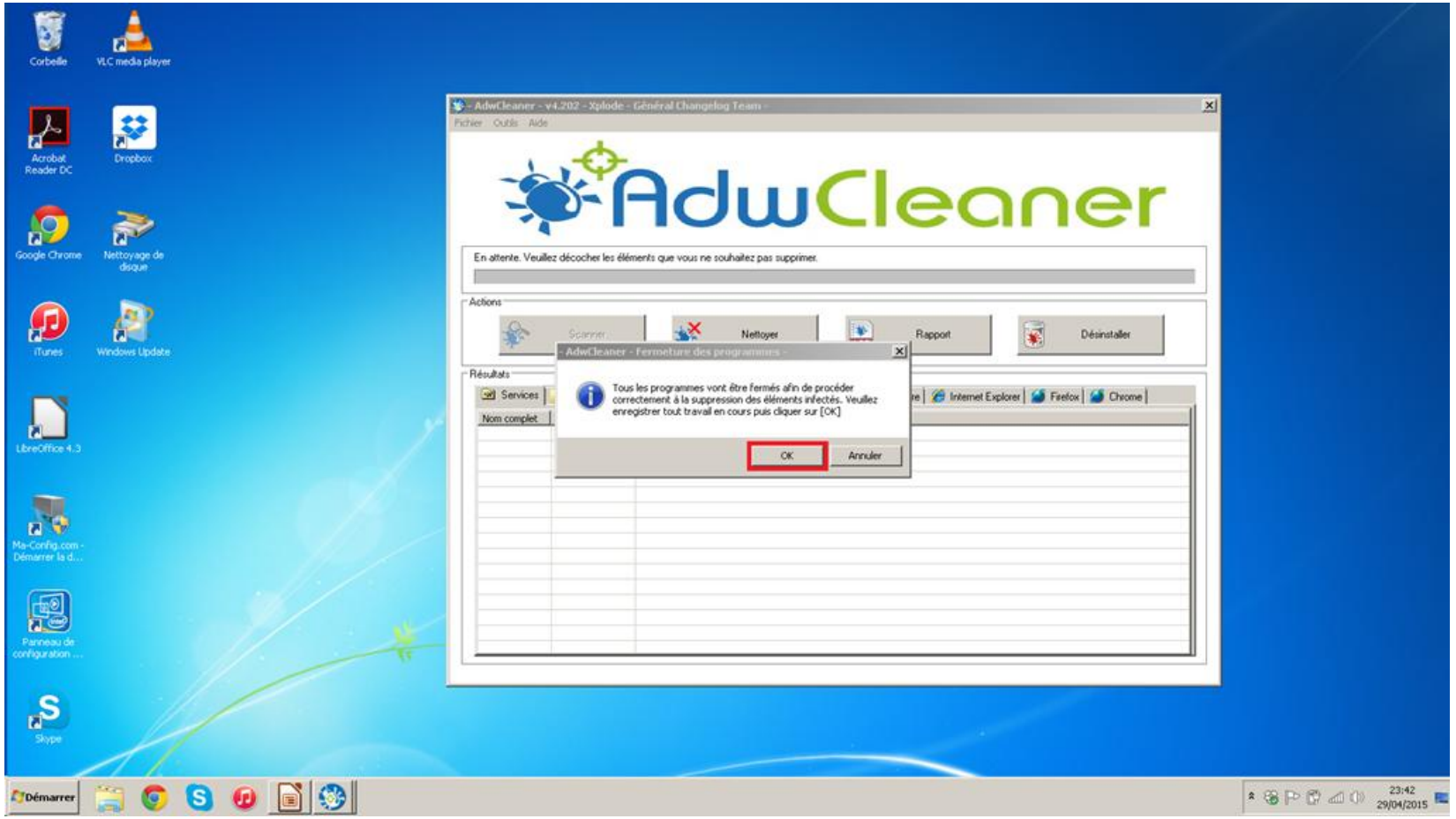
Le programme s'ouvre,

cliquez sur « Scanner »



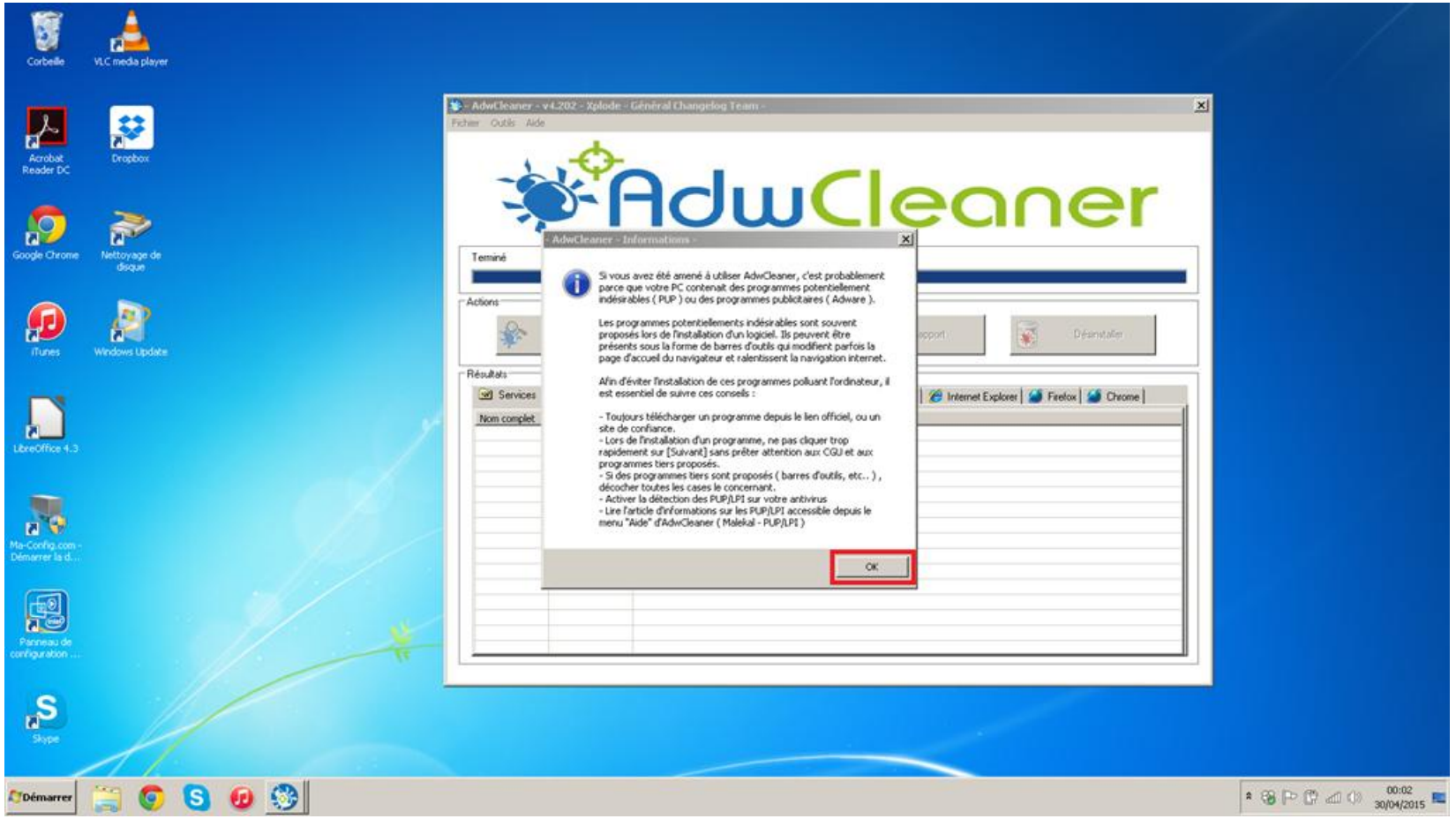
Une fenêtre apparaît,

cliquez sur « OK »



Une autre fenêtre apparaît,

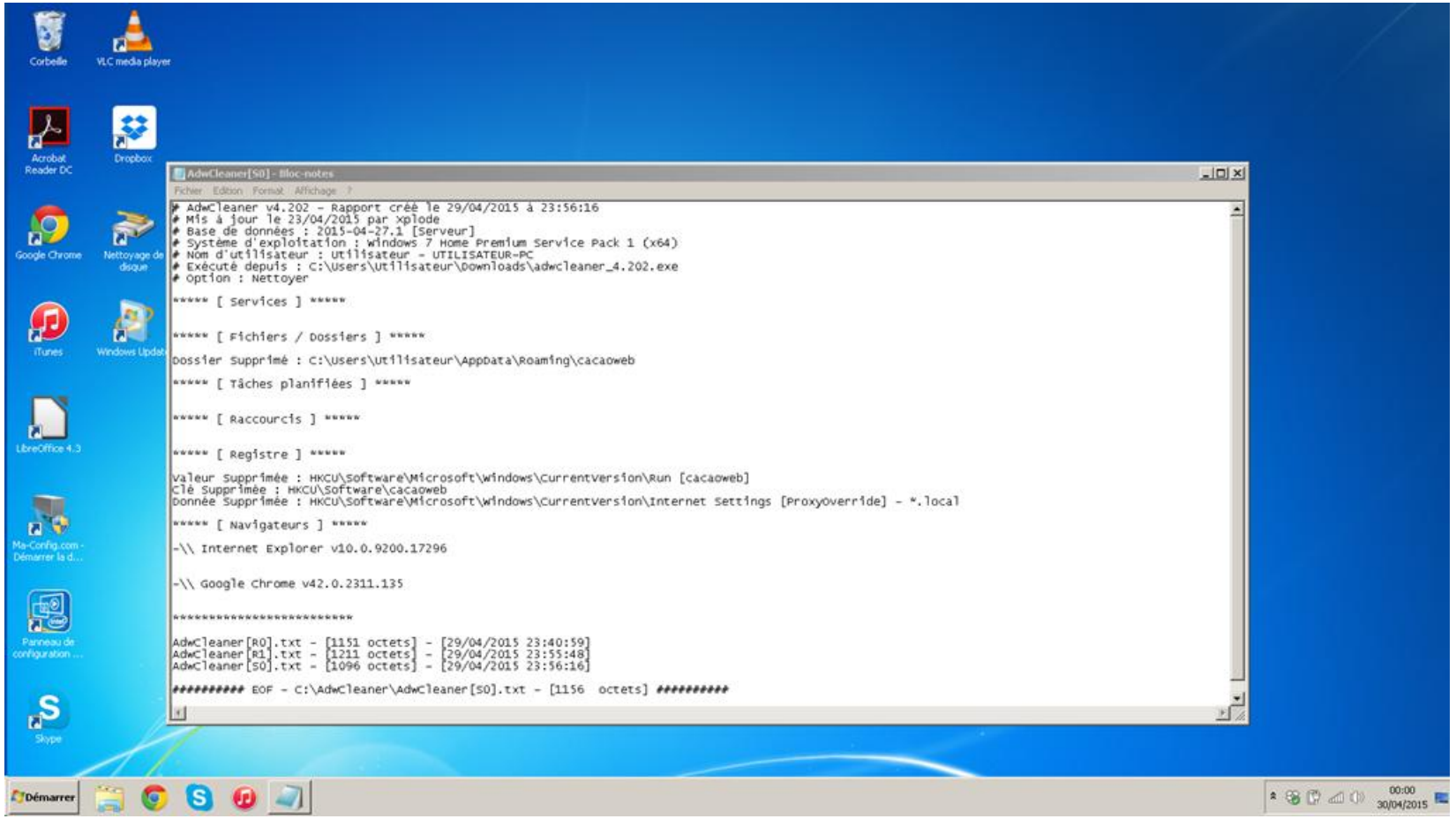
cliquez sur « OK »



Cliquez encore sur « OK »,

l'ordinateur redémarre

Après avoir redémarré, l'ordinateur affiche le rapport, refermez-le.



Répétez l'opération si nécessaire !!

5.3.1 ADWCleaner

Désinstallation

- Lorsque « ADWCleaner » ne détecte plus rien au bout de 2 analyses minimum, alors vous pouvez désinstaller le programme. Même si proprement dit, le programme ne s'est pas installé dans votre ordi, il a tout de même crée un dossier nommé « ADWCleaner » à la racine de votre disque local « C: ». Désinstaller le programme supprimera ce dossier, qui contient la quarantaine, et supprimera également le fichier exécutable de votre dossier « Téléchargement ».

Exécutez le programme, cliquez sur

« Désinstaller »

Une fenêtre apparaît,

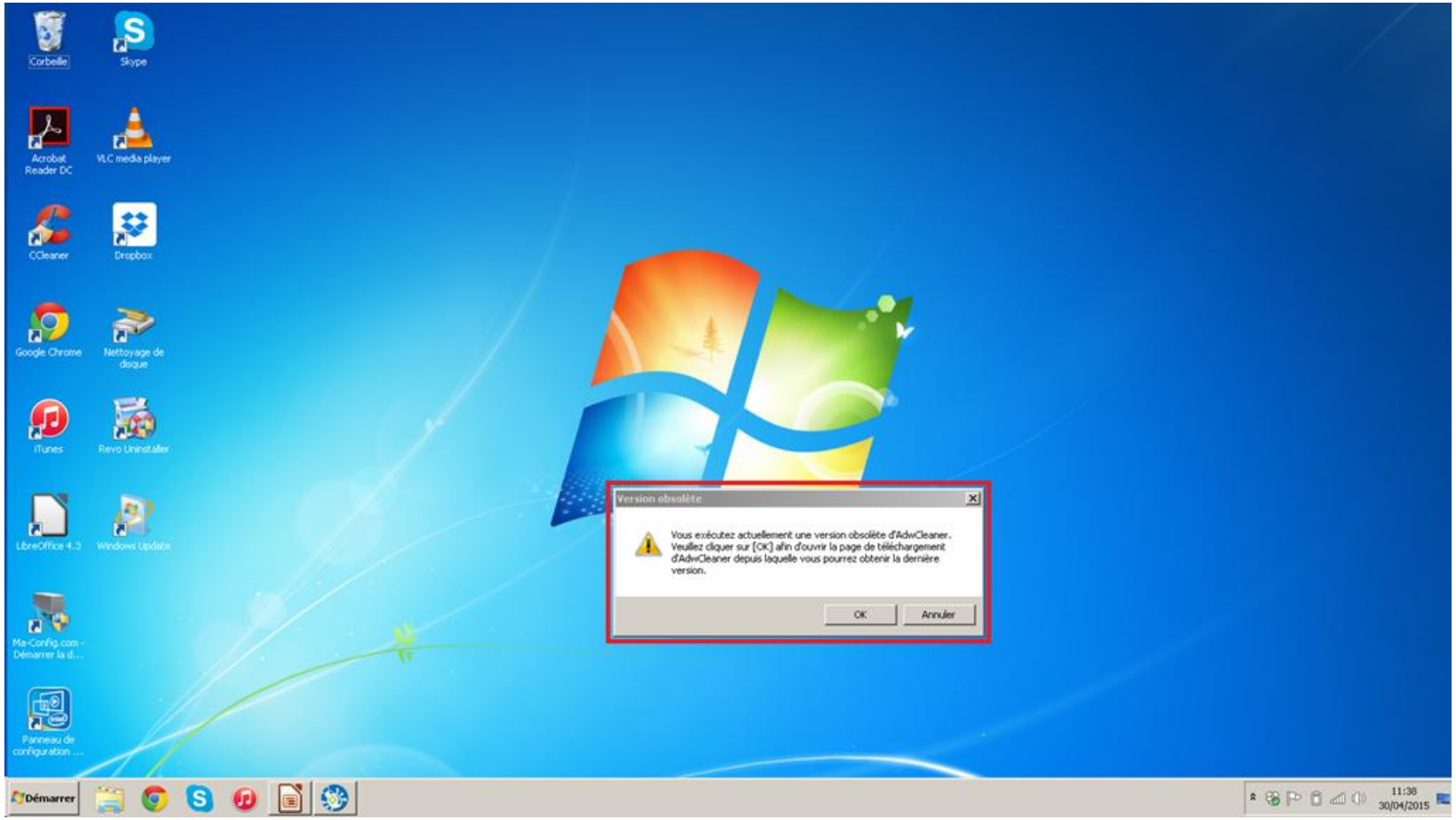
Cliquez sur « Oui »

Le programme est maintenant désinstallé !

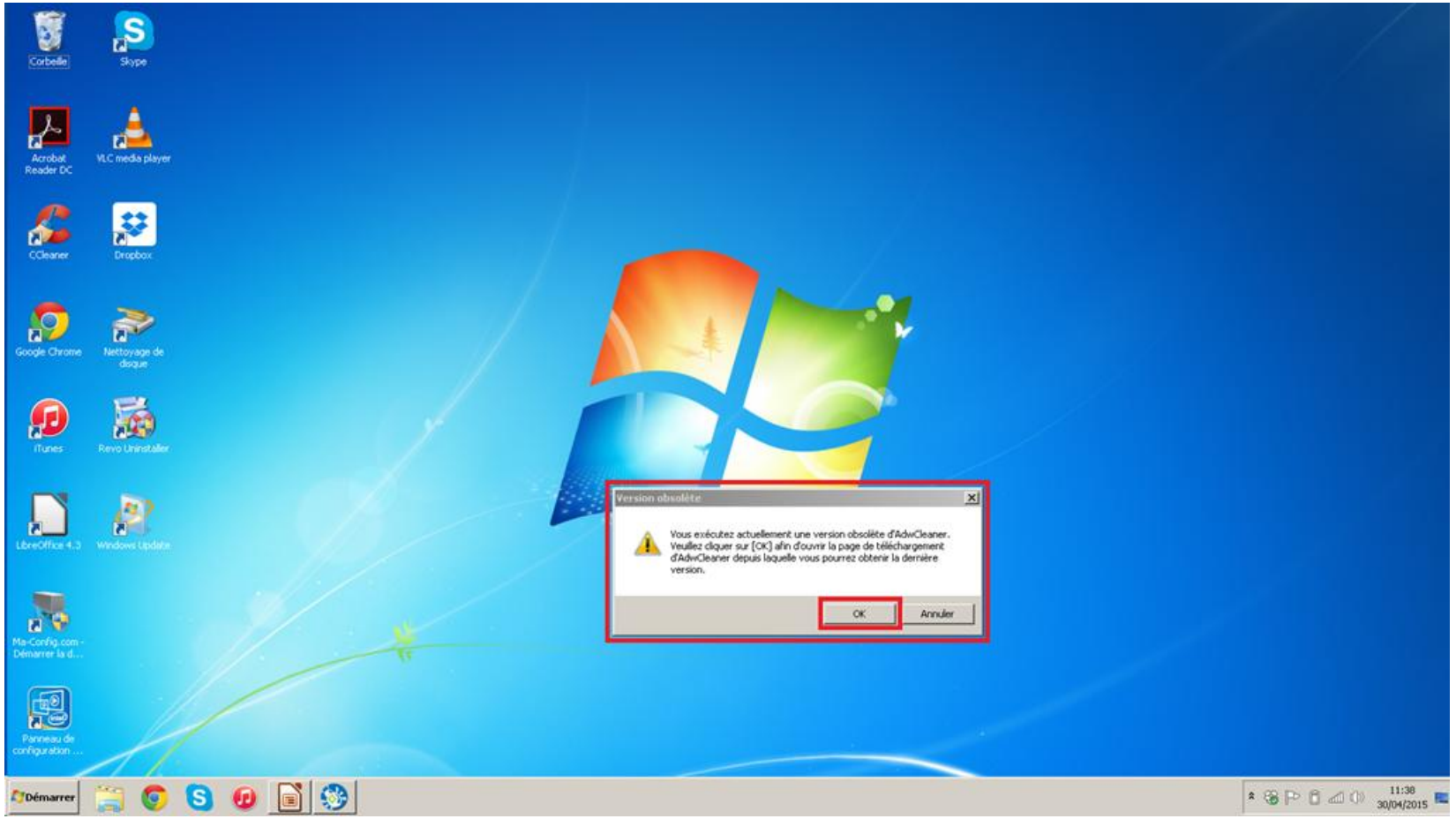
5.3.2 Vous utilisez une version obsolète

- Il arrive qu'au bout de quelques jours (7 à 10 en moyenne) une nouvelle version soit publiée par l'éditeur. La suite en image..

Lorsque vous exécutez le programme, cette fenêtre apparaît :



Cliquez sur « OK » et suivez les étapes



6. Notes et référence

- La plupart de mes sources, en ce qui concerne les définitions proviennent de Wikipédia, l'encyclopédie libre en ligne
- https://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal

- Vous trouverez les logiciels cités ici :
- - Adobe Reader :
- https://get.adobe.com/fr/reader/
- - Malwarebytes :
- https://fr.malwarebytes.org/