

Fiche phénomène

Ransomware

Disclaimer:

Les informations sont proposées en tant que service aux victimes de diverses formes d'infections avec des logiciels malveillants qui se font passer pour la police.

La police n'est en aucune manière impliquée dans cette forme d'infection et de blocage.

Les méthodes et solutions jointes ici pour débloquer un PC bloqué sont purement informatives.

Bien que les méthodes citées aient été testées par la police et trouvées aptes dans une série de configurations de tests, la police ne peut en aucune manière garantir la solution effective à toutes les situations possibles.

L'application par les victimes des méthodes proposées se déroule sous leur propre responsabilité.

La police ne peut sous aucune condition être tenue responsable de tout dégât qui serait survenu à un PC suite à l'application des techniques proposées.

Editeur responsable

Federal Computer Crime Unit - FCCU
Direction criminalité économique et
financière
Police judiciaire fédérale

[Cliquez ici si vous êtes victime](#)



1 Description du phénomène

Le ransomware est un software malveillant (malware) qui bloque l'ordinateur de la victime. La plupart du temps, un paiement est demandé pour débloquer la machine, mais payer n'arrange rien dans la majorité des cas.



Politie
Federal Computer Crime Unit
Criminaliteit op het internet

Activite illegite dimeelee!

Ce blocage de l'ordinateur sert à la prévention de vos actes illicites. Le système d'exploitation a été bloqué à cause de la dérogation de loi de la Belgique de Belgique.
On a relevé l'infraction à la loi de votre IP adresse qui correspond à " [redacted] " on a réalisé la requête sur le site qui contient la pornographie, la pornographie d'enfant, la sodomie et des actes de violence envers les enfants. Également on a récupéré un vidéo avec les éléments de violence et la pornographie d'enfants. De même on a retrouvé l'envoi de courriel électronique sous forme de spam avec les dessous terroristes.

Vos coordonnées
IP: [redacted]
Localisation: [redacted]
ISP: [redacted]

Pour lever le blocage de l'ordinateur vous devez payer le recouvrement de 100 euros.

Il y a deux possibilités d'effectuer le paiement:

1) Abolition de dettes à l'aide du système de paiement Ukash:
Pour le faire vous devez remplir le champs du paiement avec le code donné, puis appuyer sur OK (en cas de deux codes disponibles, remplacez-les successivement l'un après l'autre appuyez sur OK).

Si le système informe d'une erreur, vous devez envoyer le code à l'adresse électronique cybercrime@lokalepolitie.be

2) Paiement à l'aide de Paysafecard:
Pour le faire vous devez remplir le champs du paiement avec le code (ou avec le mot d'ordre) et appuyer sur OK (en cas de deux codes disponibles, remplacez-les successivement l'un après l'autre appuyez sur OK).

En cas d'apparition d'une erreur, vous devez envoyer le code à l'adresse électronique cybercrime@lokalepolitie.be

Ukash Ou puis-je acheter un voucher Ukash?
Vous pouvez obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques et GAB.

www.charge.be **Becharge** - Utilisez Ukash en ligne 24/7 dès maintenant avec Bancontact / Mr. Cash.
Prepaid4me - Acheter Ukash avec Bancontact / Mr. Cash.

Également disponible auprès de votre revendeur:

paysafecard Ou puis-je acheter un voucher Paysafecard?
Vous trouverez paysafecard près de chez vous, en Belgique chez un grand nombre de stations services, de supermarchés et de bureaux de tabac

(Exemple d'un ransomware récent)

2 Mode de diffusion – effets dommageables

Le fichier malware peut se retrouver dans un e-mail reçu (en pièce jointe) mais aussi être incorporé dans une page web. Aujourd'hui, ces fichiers sont également diffusés via des liens et des films sur les sites de réseaux sociaux comme Facebook, Netlog, Google+, etc...

La variante e-mail contient généralement une pièce jointe .pdf, .zip ou .exe qu'on vous demande naturellement d'ouvrir.

Après avoir cliqué dessus, un document s'ouvrira qui contiendra peu d'informations intéressantes pour le destinataire.

A ce moment, un virus ou un Cheval de Troie sera installé sur votre ordinateur.

A partir de là, toutes les informations sensibles (mots de passe, données de carte de crédit, ...) peuvent être transmises aux cybercriminels sans que vous en ayez conscience.

3 Que faire pour éviter d'en être victime?

Dotez votre ordinateur d'un programme antivirus qui sera régulièrement mis à jour. Vous pouvez trouver sur Internet différents programmes antivirus gratuits. Veillez aussi à ce qu'un pare-feu soit activé. Un pare-feu standard existe déjà dans Windows mais il ne faut pas hésiter à installer un pare-feu alternatif. On en trouve également gratuitement sur Internet.

Veillez également à ce que tous les logiciels sur votre ordinateur soient mis à jour. Les fabricants de logiciels émettent régulièrement des mises à jour pour empêcher les failles de sécurité (par ex. Microsoft Windows, Acrobat Reader, Flashplayer, etc.).

Enfin n'oubliez pas: "faites preuve de bon sens". Un message avec pièce jointe dont vous ne connaissez pas l'expéditeur se trouve dans votre boîte mail? Effacez alors cet e-mail sans ouvrir la pièce jointe.

4 Que faire si vous êtes victime?

4.1 Plainte

NE PAYEZ PAS!

Si vous avez tout de même payé ou avez subi une forme quelconque de préjudice, il vous est vivement conseillé d'introduire une plainte auprès de la police locale pour diffusion de malware en vue de hacking, sabotage d'ordinateur et escroquerie.

Si vous avez payé, prenez contact aussi rapidement que possible avec:

Ukash	PaysafeCard
Blocage du PIN via le numéro de téléphone :	Blocage du PIN via le numéro de téléphone :
- 00 800 000 85274 ou	- 078/ 158 157 (hotline sur le ticket) ou
- 00 800 247 85274	- 00 800 0729 7233
Avec le numéro PIN et le montant du ticket	Avec le numéro PIN et le montant du ticket.

Prenez une photo de tous les écrans que vous voyez sur votre ordinateur et conservez-les pour les ajouter à votre dossier. Notez les dernières actions que vous avez effectuées sur votre ordinateur et l'heure de celles-ci.

4.2 Solutions potentielles (*)


* Les méthodes et solutions permettant de débloquer les PC infectés sont purement informatives. Bien que les méthodes mentionnées ci-jointes aient été testées et jugées appropriées sur certaines configurations, la police ne garantit nullement que la solution soit efficace pour toutes les situations existantes. L'application des méthodes proposées se fait sous la propre responsabilité des victimes. La police ne peut en aucun cas être tenue responsable pour tout dommage à un PC qui pourrait être survenu à la suite de l'application des techniques proposées.

4.2.1 Déblocage du ransomware en mode sans échec

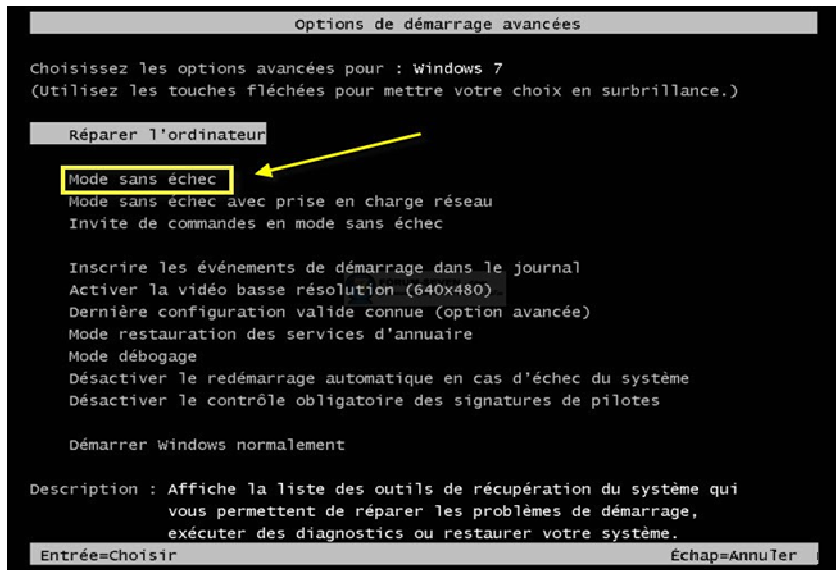
Une solution possible pour débloquer votre ordinateur consiste à le démarrer en mode sans échec. Windows démarre alors avec un jeu limité de fichiers et de pilotes.

Comment procéder?

A. Mode sans échec

1. Retirez toutes les disquettes, CDs, DVD ou autre support multimédia de votre ordinateur, puis redémarrez-le.
2. Appuyez et maintenez enfoncée la touche  F8 lors du démarrage de l'ordinateur. Vous devez appuyer sur la touche F8 avant que le logo Windows n'apparaisse à l'écran. Si le logo Windows apparaît, attendez que l'invite de connexion de Windows s'affiche, éteignez l'ordinateur et recommencez à nouveau la procédure.
3. Vous êtes maintenant dans le menu "Options de démarrage avancées". Maintenant utilisez les touches fléchées pour sélectionner "Mode sans échec" ou "Safe Mode"

en surbrillance, puis appuyez sur "Entrée" ("Retour").



4. Si tout se passe bien, Windows va démarrer en "**Mode sans échec**" et l'écran de blocage du Ransomware n'apparaîtra pas.

B. Restaurer l'ordinateur à une date antérieure

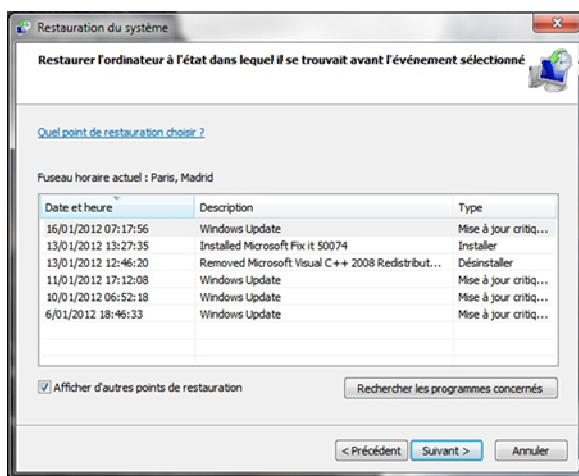
a) Pour Windows 7 ou Windows Vista

1. Cliquez sur le bouton "**Démarrer**" et entrez "**Restaurer**" dans le champ "**Rechercher les programmes et fichiers**". Dans la liste des résultats, cliquez sur "**restaurer votre ordinateur à une date antérieure**" ou "**Restauration du système**".

Cette méthode n'affecte pas vos fichiers personnels (tels que : vos photos, vidéos ou autres documents), même si il est toujours préférable de disposer d'un backup sur un support externe.

Il est possible que Windows vous demande d'entrer votre mot de passe administrateur ou de confirmer en cliquant sur un bouton.

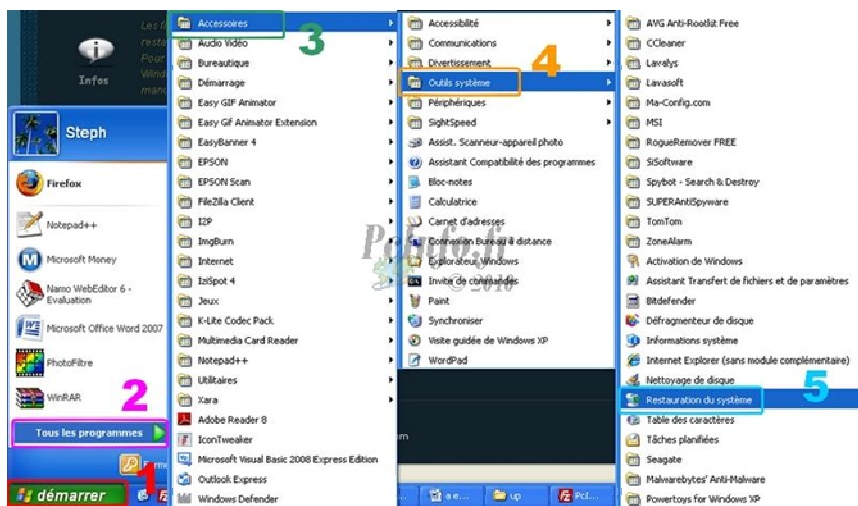
2. A l'aide de l'assistant vous pouvez choisir votre point de restauration. Eventuellement, vous pouvez également cocher la case "**Afficher d'autres points de restauration**".



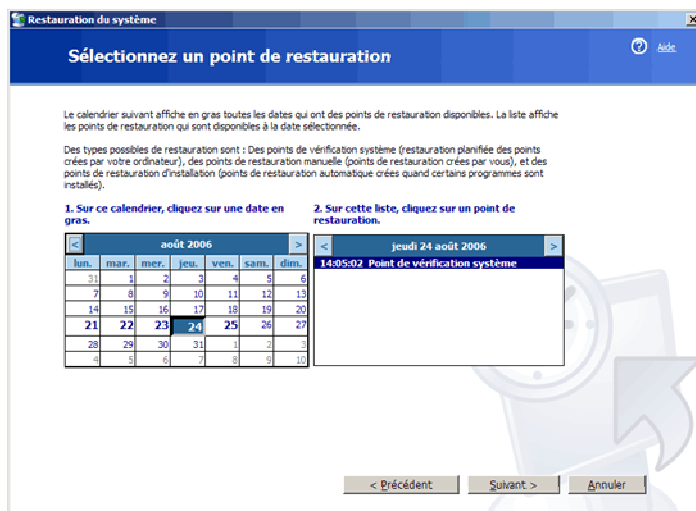
3. Cliquez sur "**Suivant**" et après confirmation, l'ordinateur va restaurer la configuration précédente (sélectionnée) et redémarrer.

b) Pour Windows XP

1. Cliquez sur le bouton "**Démarrer**".
2. Dans le menu programme allez dans Accessoires > Outils système > Restauration Système



1. Sélectionnez l'option "**Restaurer mon ordinateur à une date/heure antérieure**" et cliquez sur "**Suivant**".
2. Sélectionnez un point de restauration récent dans la liste ou cliquez sur une date en caractère gras dans le calendrier, et cliquez ensuite sur "**Suivant**".



3. Confirmez et cliquez sur "**Suivant**", l'ordinateur va alors restaurer la configuration sélectionnée et redémarrer.

- Après le redémarrage de l'ordinateur, une fenêtre Windows va s'afficher et vous informer qu'une restauration a été effectuée. Il vous reste à cliquer sur "**OK**".

C. Scanner votre ordinateur avec un antivirus / antimalware

Après le redémarrage de votre ordinateur, vous serez dans un environnement Windows normal.

Cela ne signifie pas que le virus a été complètement supprimé ou que d'autres logiciels malveillants ne se trouvent plus sur votre ordinateur !

Il est fortement recommandé d'effectuer les mises à jours de votre antivirus et d'effectuer un scan complet de votre ordinateur ; il est à noter que scanner un ordinateur en mode "Full scan" peut prendre plusieurs heures.

L'idéal restant une réinstallation complète de votre système d'exploitation.

4.2.2 Déblocage via "Windows Defender Offline"

Une deuxième solution potentielle pour débloquer votre ordinateur est d'utiliser le software gratuit "Windows Defender Offline" (délivré par Microsoft).

Equipement:

- Un ordinateur non infecté connecté à Internet
- Une clé USB

Configurations requises:

Tant le pc qui est infecté par un virus ou un malware que le pc qui est utilisé pour créer un support bootable doivent répondre aux configurations requises suivantes.

Système d'exploitation :

- Windows XP Service Pack 3
- Windows Vista, Windows Vista avec SP1, Windows Vista avec SP2 ou plus
- Windows 7, Windows 7 avec SP1 ou plus
- Windows Developer Preview, Windows 8 Consumer Preview

Mémoire vive:

- Windows XP: 512 MB RAM ou plus
- Windows Vista, Windows 7, Windows Developer Preview: 1 GB RAM ou plus

Résolution vidéo: 800 X 600 ou plus

Espace disque disponible: 500 MB

Vous pouvez télécharger gratuitement le logiciel "Windows Defender Offline" à l'adresse suivante:

<http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline?SignedIn=1>

Vous devez télécharger ce logiciel à partir de votre ordinateur non infecté. Il est prévu pour configurer une clé USB avec laquelle vous pouvez démarrer l'ordinateur infecté. Le logiciel scannerá alors l'ordinateur à la recherche des virus et malwares.

Etapes suivantes:

Etape 1. Téléchargez la bonne version en fonction du système d'exploitation de l'ordinateur infecté (32 bit ou 64 bit):

<http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline?SignedIn=1>

What is Windows Defender Offline?

Sometimes, malicious and other potentially unwanted software, including rootkits, try to install themselves on your PC. This can happen when you connect to the Internet or install some programs from a CD, DVD, or other media. Once on your PC, this software might run immediately, or it might run at unexpected times. Windows Defender Offline can help remove such hard to find malicious and potentially unwanted programs using definitions that recognize threats. Definitions are files that provide an encyclopedia of potential software threats. Because new threats appear daily, it's important to always have the most up-to-date definitions installed in Windows Defender Offline. Armed with definition files, Windows Defender Offline can detect malicious and potentially unwanted software, and then notify you of the risks.

To use Windows Defender Offline, you need to follow four basic steps:

1. Download Windows Defender Offline and create a CD, DVD, or USB flash drive.
2. Restart your PC using the Windows Defender Offline media.
3. Scan your PC for malicious and other potentially unwanted software.
4. Remove any malware that is found from your PC.

Windows Defender Offline will walk you through the details of these four steps when you're using the tool. If you've been prompted in Microsoft Security Essentials or Windows Defender to download and run Windows Defender Offline, it's important that you do so, to make sure that your data and your PC isn't compromised.

To get started, find a blank CD, DVD, or USB flash drive with at least 250 MB of free space and then download and run the tool—the tool will help you create the removable media.

Note

We recommend that you download Windows Defender Offline and create the CD, DVD, or USB flash drive on a PC that isn't infected with malware—the malware can interfere with the media creation.

[Download the 32-bit version](#)

[Download the 64-bit version](#)

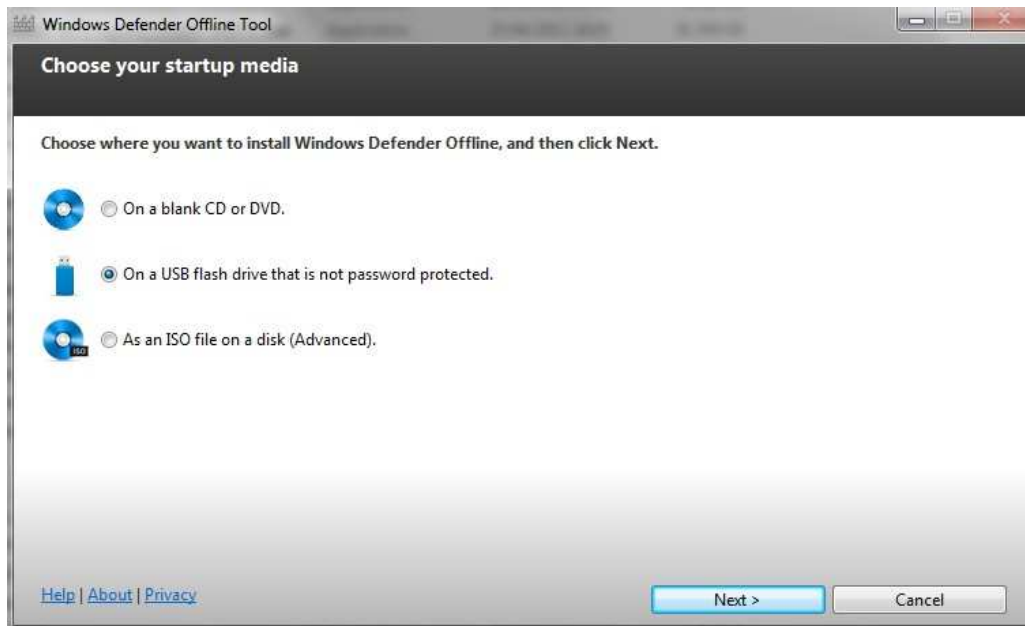
If you're not sure which version to download, see [Is my PC running the 32-bit or 64-bit version of Windows?](#)

Etape 2. Exécutez le logiciel téléchargé, vous obtenez alors l'écran suivant:



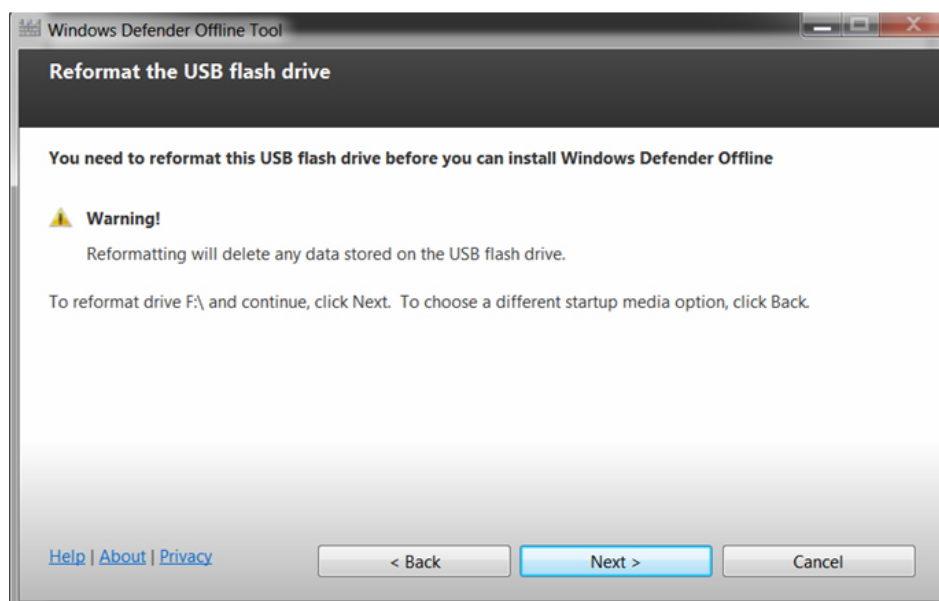
Cliquez sur Next.

Etape 3. Insérez la clé USB dans l'ordinateur. **Veillez à ce qu'aucune donnée ne se trouve sur cette clé USB car celle-ci sera formatée.**



Vous avez le choix entre différents supports. Nous optons ici pour une clé USB, le 2ème choix sur l'écran.

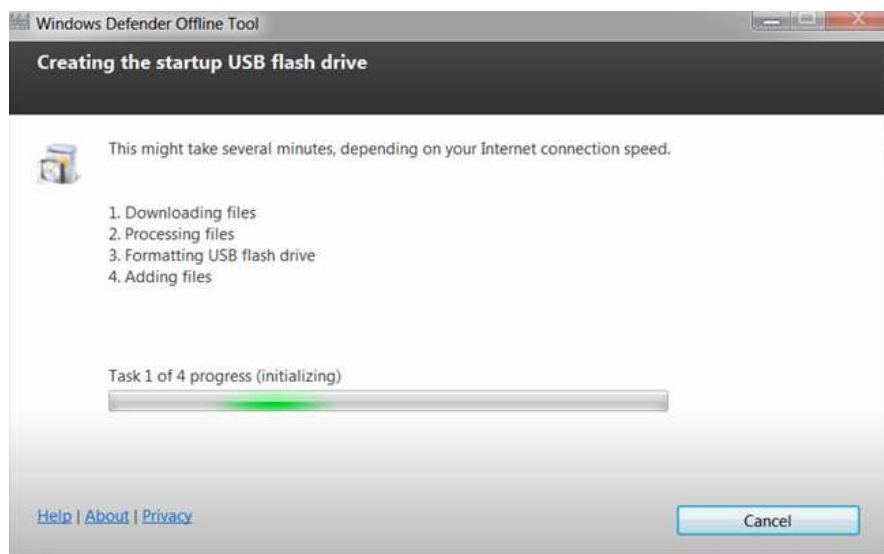
Cliquez sur Next.



Vous êtes averti que la clé USB va être formatée.

Cliquez sur Next.

Etape 4. La clé USB bootable est maintenant en cours de création.



Après cette 4ème étape 4, vous obtenez une clé USB bootable. Cela signifie que vous pouvez démarrer votre ordinateur bloqué avec cette clé USB.

Etape 5. Débarrasser l'ordinateur infecté des virus et malwares

Lorsque vous voulez utiliser une clé USB bootable, vous devez d'abord vérifier, dans le BIOS, que l'ordinateur peut être démarré à partir d'une clé USB.

Le BIOS (Basic Input/Output System) est un programme intégré dans les pc et avec lequel le système d'exploitation est démarré lorsque vous mettez l'ordinateur en marche.

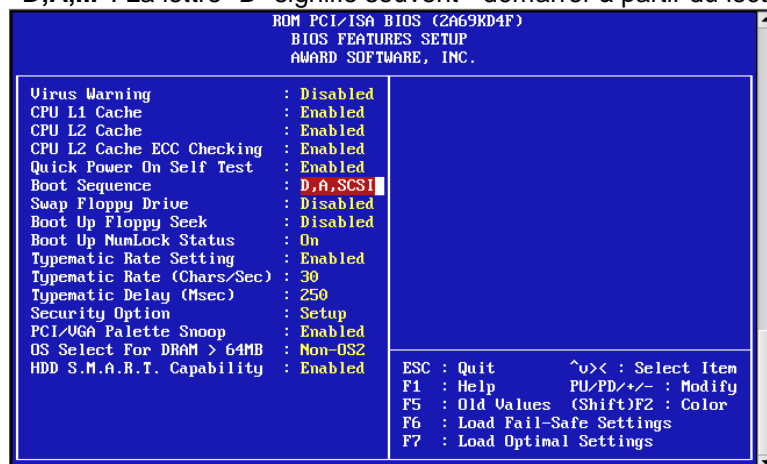
Soyez prudent lorsque vous modifiez les paramètres du BIOS. L'interface BIOS est développée pour des utilisateurs expérimentés et si vous en modifiez la configuration, il existe un risque que l'ordinateur ne démarre plus correctement. Si vous n'êtes pas familier avec cette procédure, il vaut mieux faire appel à quelqu'un d'expérimenté.

Comment arriver dans le BIOS?

La procédure diffère selon les fabricants de BIOS. Généralement, vous devez appuyer sur une touche (comme F2, F12, DEL, ESC) ou une combinaison de touches après avoir mis l'ordinateur en marche mais avant que Windows ne soit lancé. Vous utilisez ensuite les touches fléchées pour aller sur "Boot Sequence" ou sur l'onglet "Boot".

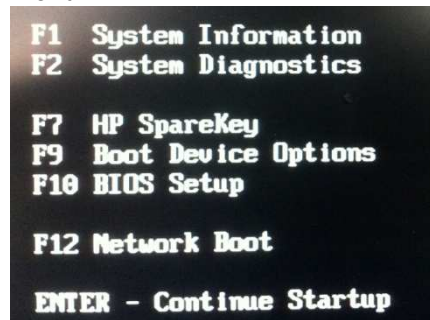
Nous donnons ici 2 exemples :

Pour les ordinateurs plus anciens, l'ordre de démarrage (boot sequence) doit être changé en "D,A,...". La lettre "D" signifie souvent "démarrer à partir du lecteur CD ou d'un port USB".



Pour les ordinateurs plus récents, vous pouvez rencontrer ce qui suit:

Après avoir appuyé sur la touche pour avoir accès au BIOS (F2, F12, DEL, ESC), vous obtenez un menu:



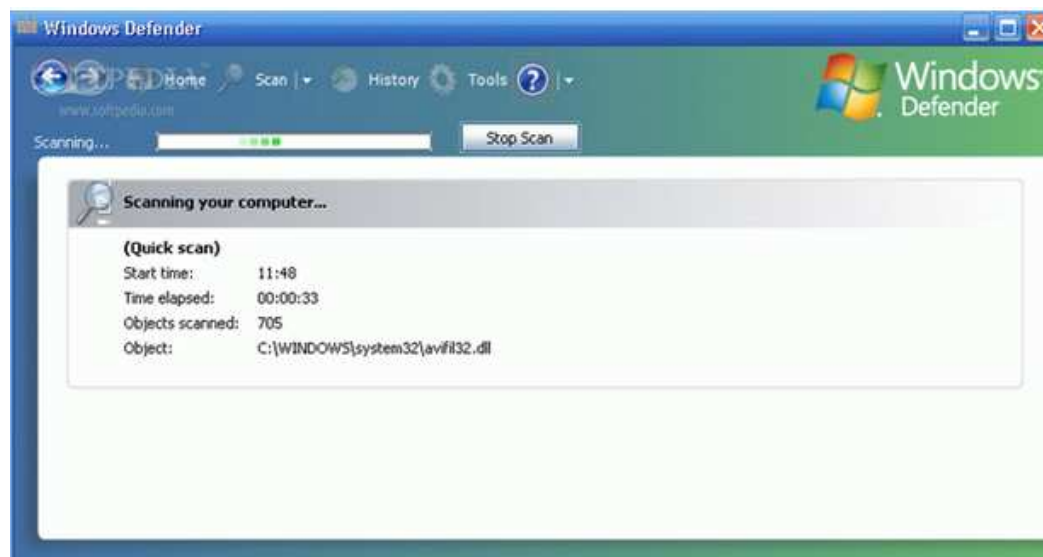
Après avoir appuyé sur la touche de fonction F9, les Boot Device Options apparaissent:



Vous placez alors la clé USB bootable créée par Windows Defender Offline dans un port USB et vous sélectionnez USB hard Drive 1 (ou une indication similaire avec USB) dans le menu de démarrage.

Si le BIOS est correctement installé et la clé USB insérée, l'ordinateur démarrera à partir de la clé USB et le scan des malwares sera lancé.

Si tout est correctement installé et que l'ordinateur ne démarre pas à partir de la clé USB, essayez alors une nouvelle fois après avoir inséré la clé dans un autre port USB.



Lorsque le scan est achevé, redémarrez à nouveau votre ordinateur normalement.

4.3 Mesures

Lorsque votre ordinateur a démarré normalement, vous devez encore exécuter un scan complet avec un programme antivirus mis à jour.

Si vous voulez être tranquille à 100%, il vaut mieux réinstaller le système d'exploitation Windows.