Police

# Federal Computer Crime Unit

## Logiciels malveillants bloquant les PC des utilisateurs et se faisant passer pour eCops, FCCU ou autres services de police étrangers

**Disclaimer**
Cette fiche a pour but d'informer les victimes de diverses formes d'infections par un logiciel malveillant se faisant passer pour un service de police.

La police n'est aucunement impliquée dans ce type d'infection et de blocage informatique.

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.

Depuis plusieurs jours de plus en plus d'utilisateurs de PC semblent être victimes d'un logiciel malveillant indiquant que le PC a été bloqué.

L'écran du PC bloqué ressemble à ceci :

eCops

**ATTENTION!**

**Votre ordinateur a été bloqué pour violation de la loi Belgique**

Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre des matériels pornographique impliquant des mineurs
- SPAM
- Utilisation des logiciels en infraction avec les droits d'auteur
- Partager des fichiers multimédia en infraction avec les droits d'auteur

Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochaines. Si vous ne payez pas dans dans le délai précisé, votre ordinateur sera confisqués et votre cas sera soumis au tribunal.

Vous pouvez payer l'amende avec l'aide des vouchers Ukash ou Paysafecard. Acheter les vouchers par Ukash ou Paysafecard de 200 €. Ensuite, ouvrez le tab «Payer amende», remplir le forme avec les codes et valuers des vouchers, et clique sur le bouton «Payer amende». Votre ordinateur sera débloqué dans les 24 heures suivantes.

Après le débloquage, nous suggérons que vous:

- Supprime toutes les fichiers multimédia en infraction avec les droits d'auteur.
- Supprime des logiciels en infraction avec les droits d'auteur.
- Installer un logiciel anti-virus, si vous n'en avez pas encore.
- Faire un scan anti-virus.

**Votre SE:** **Windows Seven** **Votre FAI:**
**Votre adresse IP:** **Votre ville:**

**Disclaimer**
Cette fiche a pour but d'informer les victimes de diverses formes d'infections par un logiciel malveillant se faisant passer pour un service de police.

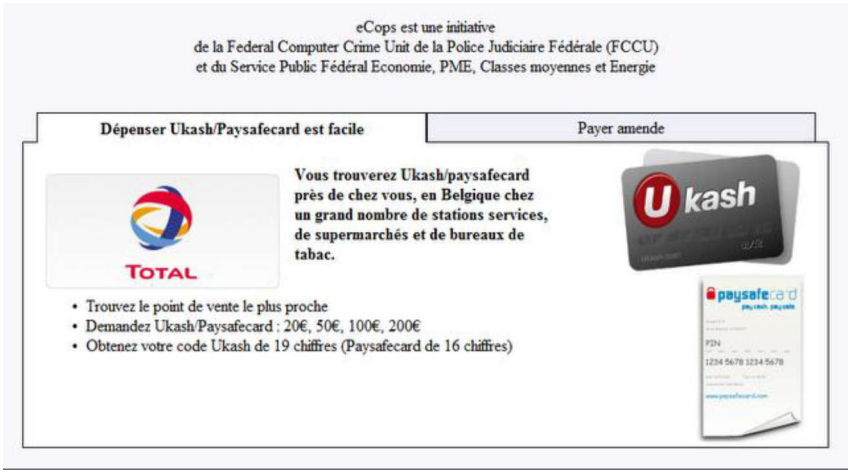
La police n'est aucunement impliquée dans ce type d'infection et de blocage informatique.

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.

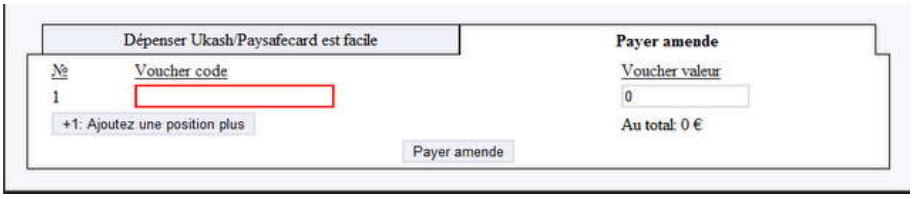
L'application des méthodes proposées se fait sous la propre responsabilité des victimes.

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.




Bien que l'écran fasse croire que le blocage se fait par eCops en raison de violations de certaines lois belges, ce n'est pas cas.

Par ce blocage, les cybercriminels tentent de vous faire payer une somme d'argent à leur profit.




Récemment une variante est apparue :

## Méthodes d'infection - effets indésirables

Les personnes qui ont un tel écran sur leur ordinateur ont été infectées.

De par les premières déclarations de victimes, il appert que la plupart ont été infectées pendant qu'elles jouaient sur des sites de jeux en ligne. Après avoir redémarré la machine, ils obtenaient cet écran et le PC était bloqué.

D'autres techniques d'infections connues pour ce virus sont :

- via une pièce jointe à un e-mail
- via des copies illégales de logiciels sur des réseaux peer-to-peer
- via des messages sur les réseaux sociaux comme Facebook qui pointent vers des sites web permettant de voir une vidéo. (Ce site indique que pour voir cette vidéo il faut mettre à jour un logiciel et installe en réalité le virus.)

Le PC de la victime est donc bloqué avec comme seule possibilité disponible de consulter les techniques de paiement.

A ce moment nous n'avons pas de renseignements supplémentaires sur les autres effets causés par ce logiciel malveillant. Les premières analyses des ordinateurs de victimes infectées sont en cours.

**Disclaimer**
Cette fiche a pour but d'informer les victimes de diverses formes d'infections par un logiciel malveillant se faisant passer pour un service de police.

La police n'est aucunement impliquée dans ce type d'infection et de blocage informatique.

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.

## Cas connus à l'étranger

Des cas similaires sont déjà connus à l'étranger. La différence est que, dans plusieurs cas, le logiciel malveillant cryptait également les données en plus du fait de bloquer le PC.

Les victimes n'ont donc plus accès à leurs fichiers et dossiers. S'ils ne disposent pas de copies de sauvegardes, tout est perdu.

L'expérience à partir des dossiers à l'étrangers montre que même lorsque les victimes payent, les ordinateurs sont très rarement débloqués ou décryptés.

## Que faire pour éviter l'infection ?

Installez un antivirus, mettez-le à jour et effectuez une analyse complète et immédiate du PC.

Faites une sauvegarde de vos données sur un disque dur externe et conservez ce disque sans qu'il soit constamment connecté à la machine.

## Que faire en tant que victime ?

### Actions immédiate

Prenez des photos des écrans bloqués et gardez-les pour la plainte.
Notez ce que vous étiez en train de faire sur votre ordinateur ainsi que les heures auxquelles vous les faisiez avant d'être infecté.

**NE PAYEZ PAS**

### Plainte

Vous pouvez vous rendre auprès de votre Police Locale afin de déposer plainte en qualité de victime. Si vous avez pris des photos, fournissez-les au service de police qui les annexera au procès-verbal.

Demandez leur de prévenir la FCCU.

Si vous avez payé, emmenez avec vous lors de la plainte toutes les informations (code du ticket) disponibles sur les moyens de paiement utilisés.  Apportez si possible le bon de paiement lors de votre déposition.

## Actions complémentaires

La FCCU coordonne le dossier au niveau central afin d'avoir une meilleure idée de l'ampleur de l'infection ainsi que des aspects techniques.

Dès que nous avons de plus amples informations, des notes complémentaires seront diffusées.



# Solution possible

## Suppression du ransomware eCops, FCCU ou autres services de police étrangers

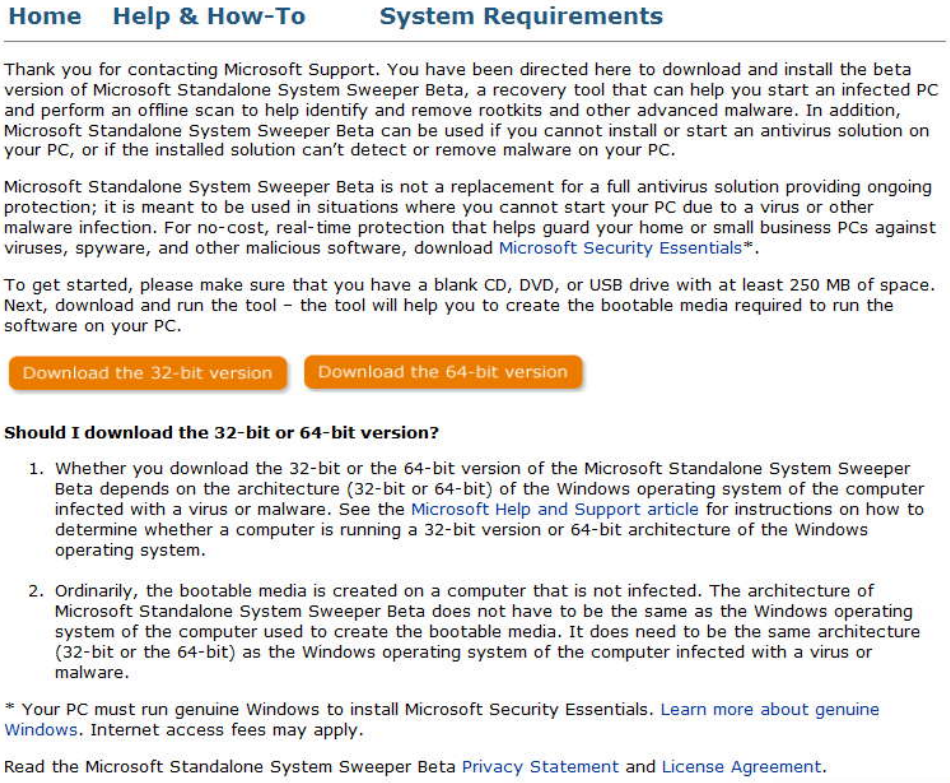
**Accessoires :**
**- Un ordinateur connecté à Internet et non infecté.**
**- Une clé USB**

Via l'adresse suivante il vous est possible de télécharger gratuitement le logiciel **Microsoft Standalone System Sweeper** : http://connect.microsoft.com/systemsweeper.

Ce logiciel permet de démarrer un ordinateur infecté au moyen d'une clé USB. Le logiciel va alors analyser l'ordinateur à la recherche de virus et logiciels malveillants (malwares).

Etapes:

- Téléchargez la bonne version du logiciel (32 bit ou 64 bit) sur http://connect.microsoft.com/systemsweeper.



Home  Help & How-To  System Requirements

Thank you for contacting Microsoft Support. You have been directed here to download and install the beta version of Microsoft Standalone System Sweeper Beta, a recovery tool that can help you start an infected PC and perform an offline scan to help identify and remove rootkits and other advanced malware. In addition, Microsoft Standalone System Sweeper Beta can be used if you cannot install or start an antivirus solution on your PC, or if the installed solution can't detect or remove malware on your PC.

Microsoft Standalone System Sweeper Beta is not a replacement for a full antivirus solution providing ongoing protection; it is meant to be used in situations where you cannot start your PC due to a virus or other malware infection. For no-cost, real-time protection that helps guard your home or small business PCs against viruses, spyware, and other malicious software, download Microsoft Security Essentials*.

To get started, please make sure that you have a blank CD, DVD, or USB drive with at least 250 MB of space. Next, download and run the tool – the tool will help you to create the bootable media required to run the software on your PC.

Download the 32-bit version  Download the 64-bit version

**Should I download the 32-bit or 64-bit version?**

1. Whether you download the 32-bit or the 64-bit version of the Microsoft Standalone System Sweeper Beta depends on the architecture (32-bit or 64-bit) of the Windows operating system of the computer infected with a virus or malware. See the Microsoft Help and Support article for instructions on how to determine whether a computer is running a 32-bit version or 64-bit architecture of the Windows operating system.

2. Ordinarily, the bootable media is created on a computer that is not infected. The architecture of Microsoft Standalone System Sweeper Beta does not have to be the same as the Windows operating system of the computer used to create the bootable media. It does need to be the same architecture (32-bit or the 64-bit) as the Windows operating system of the computer infected with a virus or malware.

* Your PC must run genuine Windows to install Microsoft Security Essentials. Learn more about genuine Windows. Internet access fees may apply.

Read the Microsoft Standalone System Sweeper Beta Privacy Statement and License Agreement.

**Disclaimer**
Cette fiche a pour but d'informer les victimes de diverses formes d'infections par un logiciel malveillant se faisant passer pour un service de police.

La police n'est aucunement impliquée dans ce type d'infection et de blocage informatique.

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.

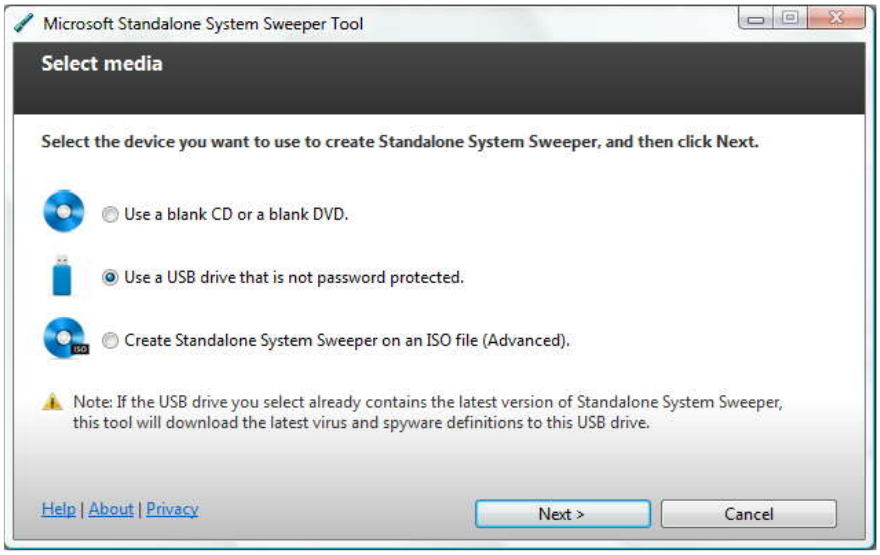
L'application des méthodes proposées se fait sous la propre responsabilité des victimes.

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.

Exécutez le logiciel téléchargé, vous obtenez l'écran suivant :

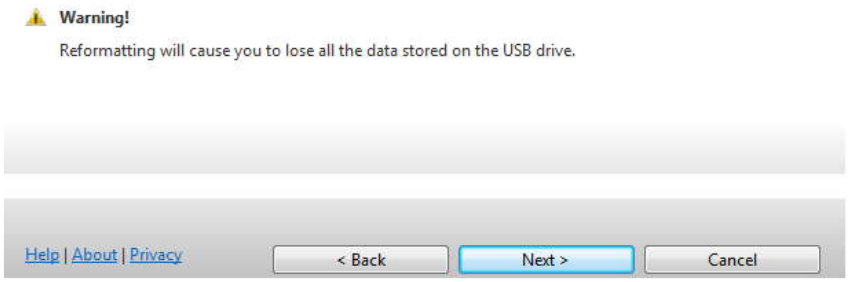

Cliquez sur Next (Suivant).

- Insérez la clé USB dans votre ordinateur. Notez que les données présentes sur la clé USB seront effacées.




- Vous avez plusieurs possibilités, nous allons poursuivre ici avec la clé USB. Il s'agit du second choix sur la liste.

Cliquez sur Next




- Un message vous indique que la clé USB sera formatée et que les données présentes seront perdues

Cliquez sur Next.

La clé USB "bootable" est maintenant en cours de création.

**Disclaimer**
Cette fiche a pour but d'informer les victimes de diverses formes d'infections par un logiciel malveillant se faisant passer pour un service de police.

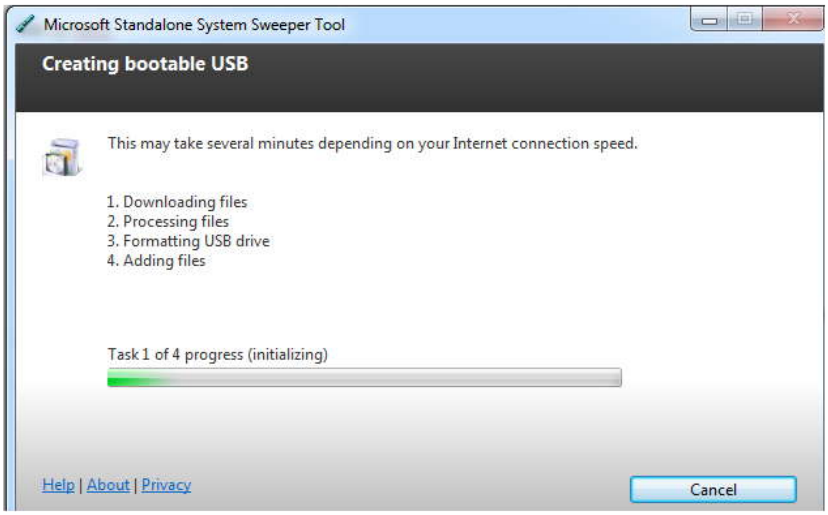
La police n'est aucunement impliquée dans ce type d'infection et de blocage informatique.

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.

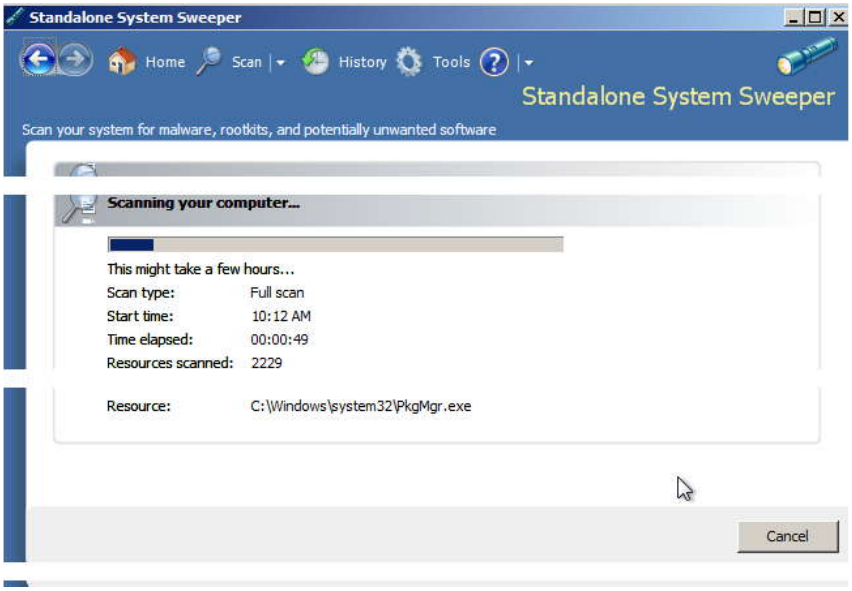
L'application des méthodes proposées se fait sous la propre responsabilité des victimes.

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.




Après cette 4ème étape, vous obtenez une clé USB bootable. Cela signifie que vous pouvez démarrer votre ordinateur sur base de cette clé USB. Par défaut l'ordinateur n'est pas configuré pour démarrer sur base de la clé USB, il faut donc forcer le démarrage sur cette option. Cela se fait via une touche au démarrage ou en configurant le BIOS. Si vous n'êtes pas familier avec cela, nous vous conseillons de vous faire aider par quelqu'un qui s'y connait.

Une fois l'ordinateur démarré avec la clé USB, un scan débute sur la machine.




Lorsque l'analyse est terminée, l'ordinateur devrait fonctionner à nouveau de façon normale. Il est conseillé toutefois d'effectuer une nouvelle analyse complète avec un antivirus et un antimalware à jour. L'idéal serait de réinstaller Windows sur votre ordinateur.