# Tentative d'escroquerie par Internet

Souvent, suite à un surf sur des sites de streaming, un malencontreux clic sur une bannière publicitaire et votre ordinateur est infecté par un script malveillant exploitant une faille de sécurité du navigateur ou de ses extensions telles Java ou Flash Player.

L'ordinateur contaminé affiche un message menaçant de poursuites judiciaires et donne une injonction de payer une amende par voie électronique.  Cette technique d'escroquerie est appelée RANSONWARE et fleurit dans une multitude de pays.

Ce message peut prendre différentes formes :

**ATTENTION!**

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

Gendarmerie nationale

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 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 cliquе 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 XP** **Votre FAI:** **CHARTER COMMUNICATIONS**


Le système devient difficilement utilisable.

Il est évident qu'il ne faut rien payer !!!!  Gardez en tête que tous vos logiciels ainsi que votre Windows doivent toujours être « UpDate » ( à jour ).

## Procédure de désinfection

Sachant qu'il y a 3 sortes d'infections différentes, il faut procéder méthodiquement.

Démarrez votre PC en mode sans échec avec prise en charge du réseau en tapotant la touche F8 au démarrage de celui-ci.

Si vous ne possédez pas les logiciels adwcleaner et Malwarebytes, téléchargez-les et mettez-les à jour.

http://www.clubic.com/telecharger-fiche215092-malwarebytes-anti-malware.html
http://www.pcastuces.com/logitheque/adwcleaner.htm

Effectuez un scan approfondi avec Malwarebytes et supprimez tout ce qui est trouvé.
Lancez une recherche avec adwcleaner et cliquez sur « Suppression » pour supprimer les clés infectées décelées. Un redémarrage sera nécessaire.

Testez votre PC en mode normal. Si l'infection persiste, poursuivez la désinfection

Le malware a pu modifier la clef Shell pour remplacer le shell ( bureau Windows ) explorer.exe par lui-même sans doute par « mahmud.exe ».

Pour récupérer le vrai bureau et empêcher le malware de se lancer, il faut remettre la bonne clé Shell.

Selon votre Windows, vous pouvez tapoter F8 au démarrage du PC et une fois arrivé sur l'écran avec les différents choix, sélectionner « Réparer l'ordinateur ».

Une fois la réparation terminée, redémarrez en mode normal et testez.

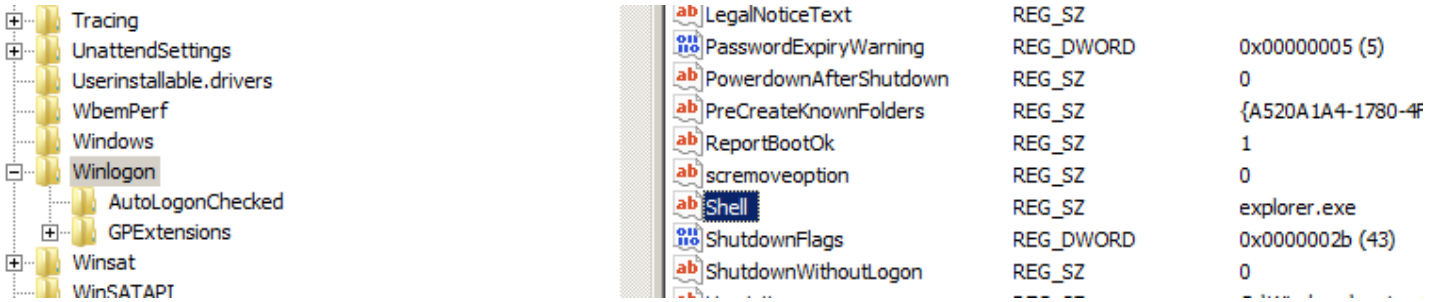
Si le résultat est toujours négatif ou si vous n'avez pas la mention « Réparer l'ordinateur », démarrez en mode sans échec puis allez sur « Démarrer » et sur « Exécuter » puis tapez « cmd » ( sans les guillemets ) et validez.

Dans l'invite de commande qui vient de s'ouvrir tapez « regedit » et validez.
Rendez-vous dans la ruche :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\

Sur la fenêtre de droite sélectionnez la ligne nommée « Shell ».

Si la ligne est saine vous devez avoir « explorer.exe » comme sur la capture suivante :




Si la clé est infectée vous avez autre chose qui finit probablement par mahmud.exe

Double-cliquez sur la clé Shell et effacez toute la ligne puis mettez « explorer.exe ».

Validez et redémarrez votre PC.

Vous pouvez faire cette manipulation via un LiveCD et en particulier avec Ultimate Boot CD que vous trouverez sur l'excellent site de Malekal.

http://www.malekal.com/download/UBCD4WinBuilder.iso

Il faudra graver l'image iso sur un cdr ou cdrw et démarrer son PC dessus. Pour cela le bios devra être réglé pour démarrer en 1er sur le cdrom.

Une fois l'interface de Ultimate Boot CD apparue, allez dans le menu Démarrer / Programs puis Registry Tools puis Registry Browser.

Positionnez vous sur HKEY_LOCAL_MACHINE

Cliquez sur le menu "File" et "Load Hive"

En bas positionnez "Files of Type" sur "All files", puis naviguez dans vos dossier pour aller dans C:Windows\System32\config\

Vous devez avoir une liste de fichiers, double-cliquez sur SOFTWARE (celui sans extension à la fin).

Un nom vous sera demandé, ce sera le nom du dossier contenant la ruche de votre base de registre de votre Windows, donnez par exemple le nom "DESINFECTION".

Déroulez l’arborescence du dossier "DESINFECTION" puis "SOFTWARE" puis "Microsoft" puis "Windows NT" puis "CurrentVersion" puis "Winlogon".

A droite chercher la clef Shell, double-cliquez dessus et mettez "explorer.exe" à la place de ce qu'il y a.

Validez et redémarrez l’ordinateur.  Le problème devrait être réglé.

**Je vous conseille de consulter le site http://www.malekal.com pour tous vos soucis d’infections virales.**