Depuis le 10 décembre 2011, il apparaît que des particuliers sont victimes d'un code malveillant bloquant leur ordinateur. Ce code exécute une page comportant le logo de la Gendarmerie (mais aussi parfois de la police) et qui empêche toute action sur l'ordinateur infecté, à moins de régler en ligne une « amende » de 200 euros.

(Cf Capture du message en annexe)

Cette pratique est nommé RANSONWARE (logiciel de rançon).

Il consiste via des bannières publicitaires (notamment celles présentes sur les sites de pornographiques et de streaming) à injecter le code sur des ordinateurs dont le navigateur internet, ou les extensions JAVA et ADOBE FLASH, ne sont pas à jour.

Le particulier se retrouve alors avec le message en question et ne peux plus effectuer aucune action. Le code est invasif au point de ne pas permettre de reprendre la main après redémarrage de l'ordinateur, les victimes de ce week-end ne trouvant leur salut qu'après réinstallation totale de WINDOWS.

Cette pratique est bien sur illégale et il est bon évidemment d'indiquer aux victimes de ne pas payer.

Il peut également être utile de leur indiquer la marche à suivre pour récupérer leur système sans devoir tout réinstaller :

La version française existe sous 3 formes :

- Une forme qui créé une clef Run, à désinfecter, c'est facile il suffit d'aller en mode sans échec avec prise en charge du réseau et de scanner avec Malwarebyte : http://www.malekal.com/tutorial_MalwareBytes_AntiMalware.php
- Une autre forme qui modifie la clef Shell (cela remplace le bureau par le malware, le bureau est inactif, le malware le rempalace). Ceci est évoqué ce lien : http://www.malekal.com/2011/12/08/trojan-winlock-tropan-ransomware-virus-police-suite/
- Et la dernière variante qui remplace Explorer.exe dont nous allons parler ici

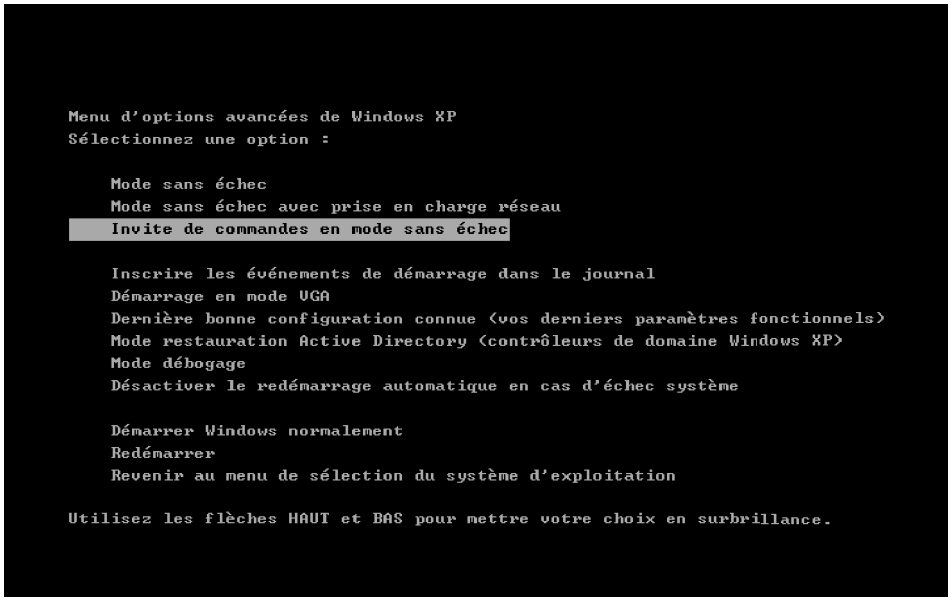
Voici la détection : http://www.virustotal.com/file-scan/report.html?id=d9c4b2f9b6fc87afb2ecfd6bf3227b1f5a488728ca7a24b9fab38eba78a09505-1323611473

```
File name: explorer.exe
Submission date: 2011-12-11 13:51:13 (UTC)
Current status: finished
Result: 6/ 43 (14.0%)   VT Community

Print results  Antivirus        Version Last Update     Result
BitDefender     7.2     2011.12.11      Trojan.Generic.KD.468202
Comodo  10920   2011.12.11      Heur.Suspicious
F-Secure        9.0.16440.0     2011.12.11      Trojan.Generic.KD.468202
GData   22      2011.12.11      Trojan.Generic.KD.468202
Kaspersky       9.0.0.837       2011.12.11
UDS:DangerousObject.Multi.Generic

Show all
MD5   : 6911baa817b5066b7566fc4d3cb1a207
SHA1  : 21007c5c048f4763750b912b5c89da54a86d34f2
SHA256: d9c4b2f9b6fc87afb2ecfd6bf3227b1f5a488728ca7a24b9fab38eba78a09505
```

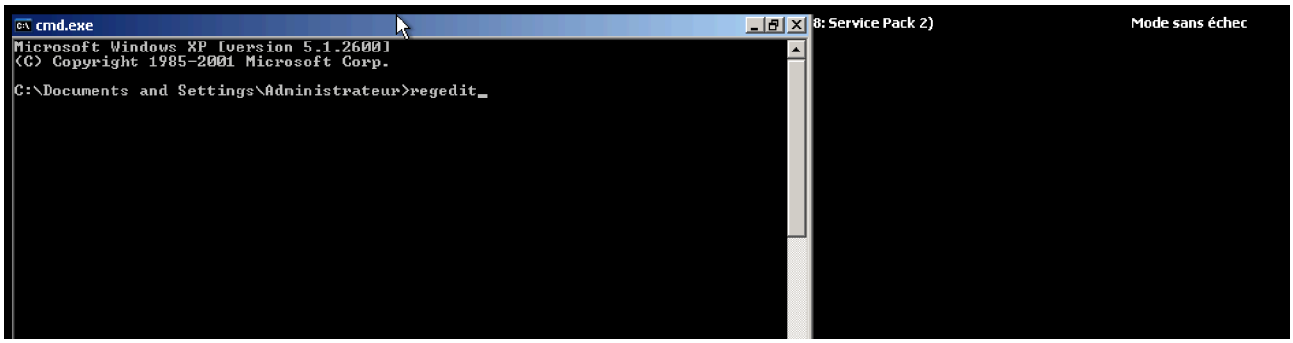
Pour désinfecter l'ordinateur, il faut donc remettre le « bon » Explorer.exe
Plusieurs solutions, soit le faire depuis un CD Live par exemple avec OTLPE simplement en copiant un explorer.exe.

Soit via un tour de passe passe.

Au démarrage de l'ordinateur, après le premier écran et avant le logo Windows, juste au changement d'écran, tapotez sur F8 pour obtenir les menu de démarrage et choisissez invite de commandes en mode sans échec.



Sur la fenêtre cmd.exe, tapez regedit et validez.



Déroulez l'arborescence suivante en cliquant sur les + :
HKEY_LOCAL_MACHINESoftWareMicrosoftWindows NTCurrentVersionWinlogon
A droite, chercher Shell, vous devez avoir explorer.exe – remplacer par iexplore.exe

Redémarrez l'ordinateur en mode normal.
Vous devriez avoir Internet Explorer qui se lance tout seul.
Téléchargez le explorer.exe correspondant à votre système :

- Windows XP SP2/SP3 : http://www.malekal.com/download/explorer_XP_SP2.zip - non

compressé : http://www.malekal.com/download/explorer_XP_SP2.exe

- Windows Vista : http://www.malekal.com/download/explorer_Vista_SP2.zip - non compressé : http://www.malekal.com/download/explorer_Vista_SP2.exe

Décompressez et copier le explorer.exe télécharger à la place de celui du système qui est malicieux => C:Windowsexplorer.exe.

ou directement, en prenant la version non compressée, enregistrez le fichier dans le dossier Windows à la place de celui malicieux.

Redémarrez l'ordinateur, vous devriez avoir accès à votre système.

Pensez à maintenir à jour vos logiciels (notamment Java, Adobe Reader et Flash), ces programmes non à jour permettent l'infection de votre système.

Source : Information issue du site MALEKAL.COM

ANNEXE
CAPTURE DU MESSAGE

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 dans le délai précisé, votre ordinateur sera confisqués et votre cas sera soumis au tribunal.

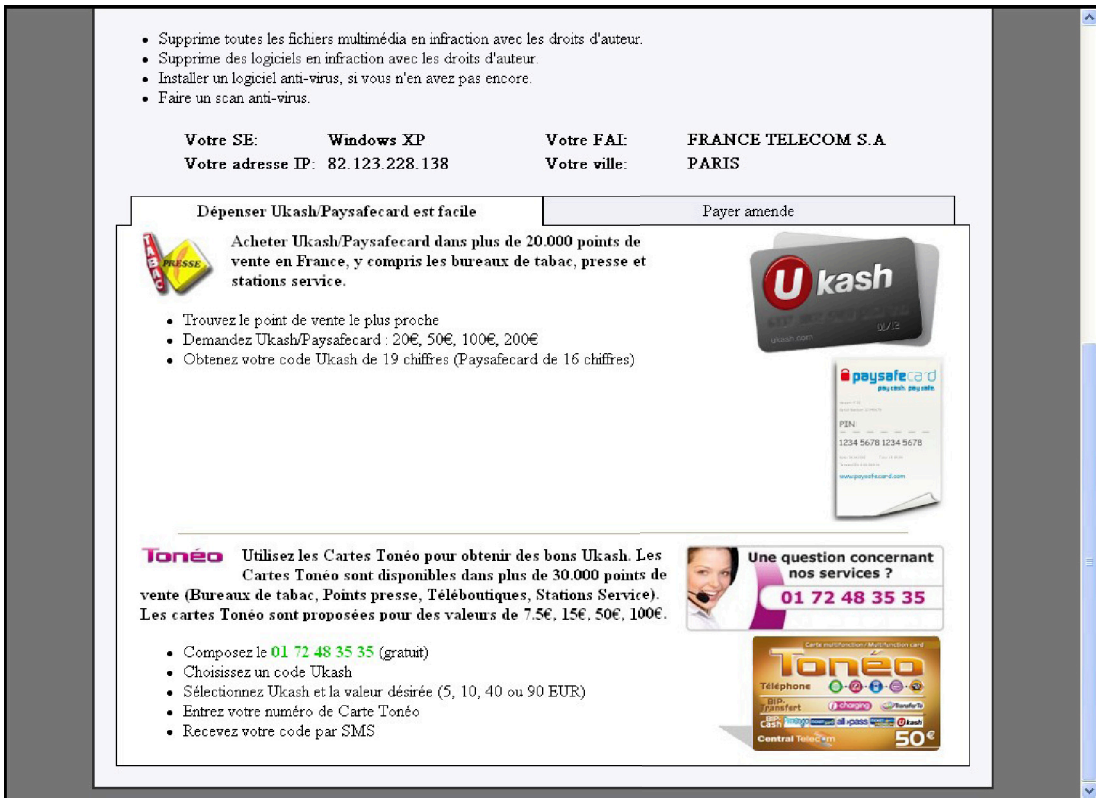
Vous pouvez payer l'amende avec l'aide des vouchers Ukash ou Paysafecard. Acheter les vouchers par Ukash ou Paysafecard de 200 €. Ensuite, ouvrez le tab «Payer amende», remplir le forme avec les codes et valuers des vouchers, et clique sur le bouton «Payer amende». Votre ordinateur sera débloqué dans 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 XP**	**Votre FAI:**	**FRANCE TELECOM S.A**
Votre adresse IP:	**82.123.228.138**	**Votre ville:**	**PARIS**

Dépenser Ukash/Paysafecard est facile | Payer amende



- 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:**	**FRANCE TELECOM S.A**
Votre adresse IP:	**82.123.228.138**	**Votre ville:**	**PARIS**

Dépenser Ukash/Paysafecard est facile | Payer amende

Acheter Ukash/Paysafecard dans plus de 20.000 points de vente en France, y compris les bureaux de tabac, presse et stations service.

- Trouvez le point de vente le plus proche
- Demandez Ukash/Paysafecard : 20€, 50€, 100€, 200€
- Obtenez votre code Ukash de 19 chiffres (Paysafecard de 16 chiffres)

Tonéo **Utilisez les Cartes Tonéo pour obtenir des bons Ukash. Les Cartes Tonéo sont disponibles dans plus de 30.000 points de vente (Bureaux de tabac, Points presse, Téléboutiques, Stations Service). Les cartes Tonéo sont proposées pour des valeurs de 7.5€, 15€, 50€, 100€.**

- Composez le 01 72 48 35 35 (gratuit)
- Choisissez un code Ukash
- Sélectionnez Ukash et la valeur désirée (5, 10, 40 ou 90 EUR)
- Entrez votre numéro de Carte Tonéo
- Recevez votre code par SMS

Une question concernant nos services ?
01 72 48 35 35