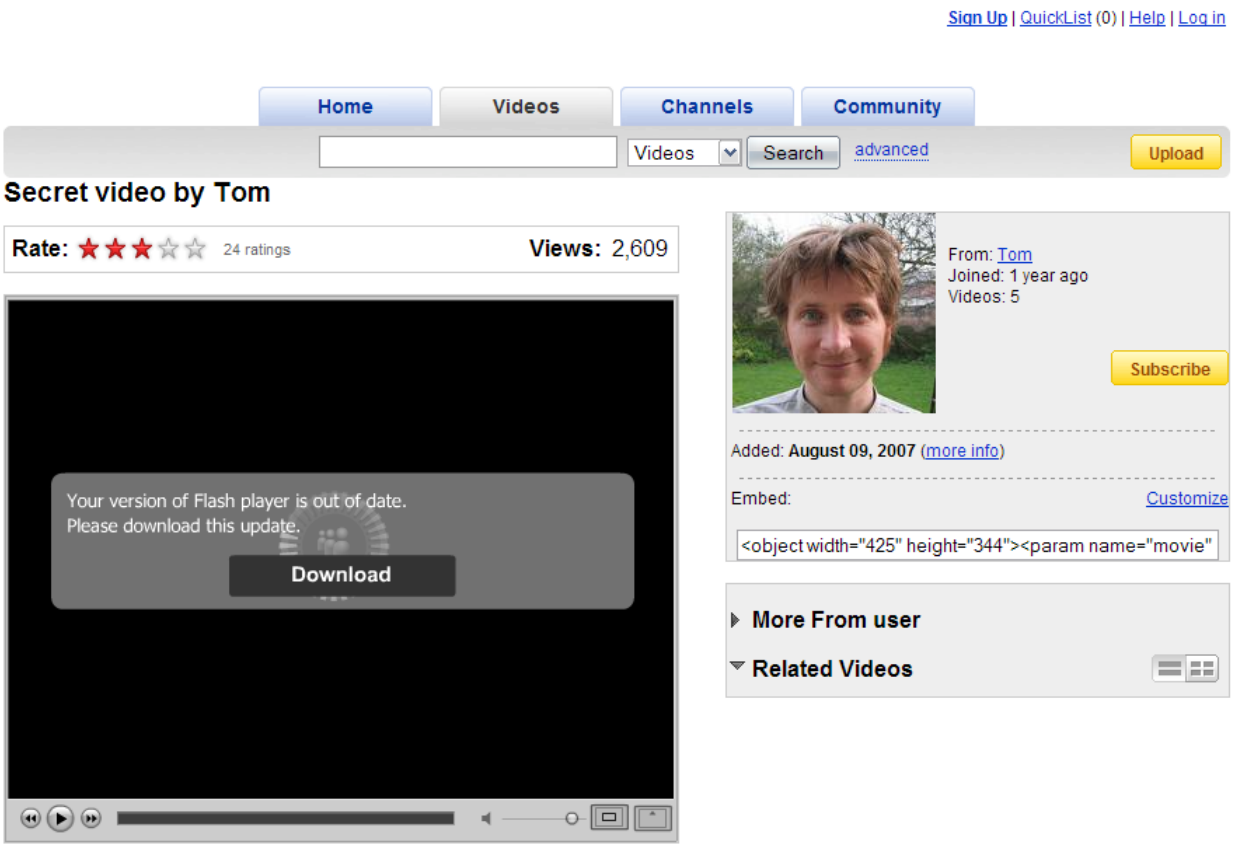
Supprimer KoobFace

```
<?php include('menu_horizontal.php'); ??>
<?php include('menu.php'); ??>
```

Supprimer le trojan KoobFace

KoobFace est un trojan qui se propage sur les réseaux sociaux (MySpace, FaceBook etc..).
Une fois infecté, le compte du réseau sociaux est utilisé pour poster des messages contenant des liens redirigeant vers des pages de téléchargement de vidéos.



Il est alors stipulé que vous devez télécharger Flash pour visualiser la vidéo, un faux fichier Flash est alors proposé qui n’est en fait que le programme d’installation de

l’infection.

Bref du social engineering reprenant le principe des Faux codec.

L’infection installe un proxy qui permet en autre de voler les mots de passe de connexion.

KoobFace utilise aussi des méthodes de propagations dont :

- Les exploits sur site WEB
- Les Faux codec via des sites pornographiques.

Vous trouverez plus d’informations sur la page suivante : Net-Worm.Win32.Koobface sur FaceBook et MySpace

Détection de KoobFace

Les lignes visibles sur HijackThis :

- de ligne R1 avec le ProxyServer localhost:7171 et le programme proxy dll32, dll32.sm, SYSDLL etc.
- de ligne avec un fichier généralement court se terminant par deux chiffres ex: pp02.exe ld08.exe freddy36.exe
- Eventuellemnt d’une ligne O2 BHO avec une série de chiffre et helper, exemple : **O2 – BHO: 272329 helper** – {437A43D5-E5C3-4959-BBD0-F2BFB1EDC6FD} – C:\Windows\System32syslocsysloc.dll

Supprimer KoobFace

- Téléchargez HijackThis : et dézipez le sur le bureau.
- Lancez un scan HijackThis en cliquant sur le bouton : *Do a scan and save log file*
- Repérez et cochez les lignes caractéristiques de l’infection expliquées dans le paragraphes précédent, exemples :
  - *R1 – HKCUSoftwareMicrosoftWindowsCurrentVersionInternet Settings,ProxyServer = http=localhost:7171*

        - *R1 – HKCUSoftwareMicrosoftWindowsCurrentVersionInternet Settings,ProxyOverride = *.local;<local>*
        - *O4 – HKLM..Run: [sysldtray] c:windowsld08.exe*
        - *O4 – HKLM..Run: [sysftray2] C:windowsfreddy36.exe*
        - *O4 – HKLM..Run: [pp] C:windowspp02.exe*
        - *O4 – HKLM..Run: [sysldtray] c:windowsld02.exe*
        - *O4 – HKCU..Run: [SYSDLL] SYSDLL*
        - *O4 – HKCU..Run: [dll] rundll32 dll32,sm*
    - Cliquez sur Fix Checked
        - Désactivez le proxy ajouté par l'infection pour cela :
        - **Sur Firefox**, Menu Editions / Préférences puis onglet Avancés.
        - Cliquez sur Réseau et Paramètres.
        - Choisissez « Ne pas mettre de Proxy ».
        - **Sur Internet Explorer**, c'est le menu Outils / Options Internet.
        - Onglet Connexions puis en bas, vous pouvez désactiver le proxy.
    - Redémarrez l'ordinateur

Eventuellement utilisez Combofix pour nettoyer le reste :

- Désactivez la protection de votre Antivirus
- Téléchargez Combofix de sUBs
- Double-clicquez sur combofix.exe et laissez vous guider.

Mettez à jour votre Antivirus et faites un scan complet avec.

Autres Liens

Pour plus d'informations, sur le fonctionnement des spywares et les conseils à suivre :
Fonctionnement et suppression des Vers/Spywares/Malwares sous Windows
Guide de suppression des malwares (SpySherrif, Spyaxe, SpywareStrike, Winbound, etc..)

- Les outils de suppressions de Spywares/Malwares spécifiques
- Sécuriser le navigateur Windows Internet Explorer
- Tutorial installation et configuration d’Antivir
- Tutorial et configuration du Firewall de Windows XP