e i g
Ecole d'ingénieurs
de Genève

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale
University of Applied Sciences
Western Switzerland

Étude des *Spywares*

Unité d'enseignement et de recherche UER4

Filière :
Télécommunication

Laboratoire :
Transmission de données

Étudiant :
DE SOUSA Bruno

Classe :
TE3

Session :
2005

Professeur responsable :
LITZISTORF Gérald

En collaboration avec :
TRUPHEME Florent

Entreprise :
Telecom System

e i g

Ecole d'ingénieurs
de Genève

Automne 2005

Session de diplôme

TRANSMISSION DE DONNEES
ETUDE DES *SPYWARES*

Descriptif :

Selon http://www.secuser.com/dossiers/spywares_generalites.htm, un *spyware*, en français "logiciel espion", est un programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via *internet* ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

Ce travail de diplôme propose de les étudier pour une cible Windows XP.

Travail demandé :

Principaux domaines d'étude de ce travail :

- Qui profite des *spywares* ?
- Quels types d'information transmettent-ils ?
- Comment sont-ils installés sur le poste de la victime ?
  Etudier les principaux vecteurs d'installation (voir article MISC, étude de cas)
- Quelles sont les caractéristiques des canaux de transmission utilisés ?
- Comment les détecter ?
  Tester l'efficacité des outils de détection
  Comparer avec analyse forensique
- Comment s'en protéger ?
  Droits de l'utilisateur, paramètres de sécurité XP & navigateurs
  Filtrage (regex) au niveau du *proxy* Bluecoat

L'étudiant proposera divers scénarios de tests destinés à un usage pédagogique orienté forensique.

Liens :
http://www.spywareguide.com/product_list_full.php
http://www.pcpitstop.com/spycheck/
http://www.malware.com/
http://www.securityfocus.com/infocus/1829
http://www.spywarewarrior.com/index.php
http://www.netrn.net/no_spyware.htm
http://www.benedelman.org/news/041105-1.html
http://www.benedelman.org/spyware/installations/
http://castlecops.com/HijackThis.html
Revue MISC 17 Le spyware : une menace de l'intérieur par Nicolas Ruff
http://www.chambet.com/publications/Fuite%20infos%20dans%20Office%20&%20Windows.pdf
http://actes.sstic.org/SSTIC03/Le_spyware_dans_Windows_XP/SSTIC03-article-Ruff-Le_spyware_dans_Windows_XP.pdf
http://www.microsoft.com/athome/security/spyware/software/default.mspx

Unité d'enseignement
Et de recherche UER4

Classe : TE3

Timbre de l'Ecole

ÉCOLE D'INGÉNIEURS
RÉPUBLIQUE ET CANTON DE GENÈVE
DIRECTION

Candidat :

M. DE SOUSA BRUNO

Filière d'études :

Télécommunication

Travail de diplôme soumis à une convention de stage en entreprise : non

Travail de diplôme soumis à un contrat de confidentialité : non

Professeur(s) responsable(s) :
Litzistorf Gérald

En collaboration avec : Telecom System (M. Truphème)

Table des matières

Préambule

Ce document a été élaboré lors de mon travail de diplôme de la session 2005.

Le sujet de ce projet a été proposé par M. Florent TRUPHEME et supervisé par M. Gérald LITZISTORF, responsable du laboratoire de transmission de données de l'École d'Ingénieurs de Genève.

Ce mémoire est divisé en quatre parties pouvant être résumées comme suit.

La première partie défini la nomenclature utilisée, ainsi que les actions et symptômes dus aux *spywares*.

La deuxième partie traite des méthodes d'infection utilisées pour installer un *spyware* sur une machine et les illustre par des exemples.

La troisième partie aide l'utilisateur à configurer sa machine de manière à diminuer les risques d'infection et présente une solution de protection matérielle en utilisant le Blue Coat ProxySG 400.

La quatrième partie montre les différentes possibilités pour se débarrasser des *spywares*, une fois qu'ils se sont installés sur la machine. Elle est ce qu'on peut appeler une étape *post-mortem*.

Sont ensuite présentées les conclusions tirées de ce projet.

De plus, pour faciliter la lecture de ce mémoire de diplôme, certaines conventions typographiques ont été adoptées :

- Verdana 10 normal : texte normal
- **Verdana 10 gras** : phrases ou termes importants
- *Verdana 10 italique* : termes anglais
- Verdana 8 normal : légendes et notes de bas de page
- `Courrier New 10 normal` :*logs*, codes sources et noms de fichiers/dossiers
- **`Courrier New 10 gras`** : phrases ou termes importants dans les *logs*

Je tiens aussi à remercier quelques personnes sans lesquelles ce projet aurait été beaucoup plus ardu :

- M. LITZISTORF pour son professionnalisme et ses critiques constructives tout au long de ce projet
- M. CONTRERAS, assistant du laboratoire, pour l'aide apportée tout au long du projet
- M. TRUPHEME pour m'avoir offert la possibilité d'étudier la problématique liée à ce sujet

1 Généralités

7 jours d'étude

1.1 Nomenclature

Le terme *malware* est une contraction des termes anglais ***mal****icious soft****ware***. C'est un terme générique désignant toute application malicieuse installée sur une machine, il comprend tous les termes définis ci-après.

Le terme *spyware*, traduit en français par logiciel espion, désigne tout logiciel, conçu dans le but de collecter des données personnelles sur un utilisateur (client) et de les envoyer secrètement à son créateur ou tout autre entité (serveur) via internet.

Les *adwares* (logiciels publicitaires), *pop-ups* et quelques *cookies*, sont parfois considérés comme des *spywares* car ils peuvent fonctionner sans le consentement de l'utilisateur. À la différence des *spywares* purs, certains *adwares* ne transmettent pas de données personnelles à leurs créateurs, ils ne font qu'afficher des bannières publicitaires, tout de même incommodes. Ils sont utilisés, le plus souvent, comme source de financement pour les éditeurs de *freewares* (logiciels gratuits), dans lesquels ils sont incorporés. Cependant, due à leur nature « envahissante » et au fait qu'ils utilisent très souvent les données collectées pour choisir le type de publicité à afficher, les *adwares* sont classés par certaines personnes comme des *spywares*.

Les *foistwares*, sont quant à eux des logiciels qui installent des applications supplémentaires au logiciel principal, en faisant croire à l'utilisateur qu'elles sont nécessaires au bon fonctionnement de celui-ci.

Les *hijackers* sont des logiciels qui « détournent » les réglages systèmes, le plus souvent ceux du navigateur. Ils modifient, entre autres, les pages d'accueil et de recherche.

Une *backdoor* est un programme donnant accès à un ordinateur sans tenir compte des règles de sécurité imposées.

Nous utiliserons, donc, ici le terme *spyware* pour toute application installée à l'insu de l'utilisateur et portant atteinte à sa vie privée (incluant les *adwares*, *foistwares* et *hijackers*).

1.2 Les actions exécutées par les *spywares*

Les actions entreprises par les logiciels espions peuvent être de différentes formes.

Ils peuvent entre autres :

- Créer des ***backdoors***.
- ***Logger*** les touches tapées au clavier.
- ***Tracker*** les sites internet visités par l'utilisateur.
- **Collecter** les données entrées dans les formulaires internet.
- **Afficher** de la publicité (*adwares*)

Les données, envoyées sans le consentement de l'utilisateur, sont ensuite utilisées à des buts publicitaires, de *tracking* ou même de fraude financière, lors du vol de numéros de carte de crédit, par exemple.

Les données transmises sont, cependant, très difficiles à analyser car la plus part des *spywares* communiquent au moyen de flux chiffrés.

1.3 Les symptômes

La présence d'un *spyware* sur une machine infectée ne passe pas inaperçue à l'utilisateur. Les différents symptômes pouvant survenir sont :

- Diminution des performances de la machine
- Affichage de messages d'erreur aléatoires
- Apparition d'icônes inconnus sur le bureau
- Modification des paramètres du navigateur (page d'accueil, page de recherche, …)
- Ajout de nouvelles barres d'outils (dans le navigateur ou sur le bureau)
- Redirection vers des sites non souhaités
- Affichage de fenêtres publicitaires

Si l'un de ces symptômes est vérifié sur votre machine, il se pourrait bien qu'elle soit infectée. L'utilisateur pourra se référer au §4, pour la détection et suppression des menaces présentes sur le système.

2 Infection

12 jours d'étude

A l'instar des virus, les *spywares* ne cherchent pas à se reproduire, ce qui est à l'origine de leur pseudo légalité. Ils utilisent, donc, d'autres méthodes d'infection.

2.1 *Bundled software*

Le moyen le plus efficace et aussi le plus répandu, est celui de l'empaquetage (***bundled software***) dans un autre logiciel. C'est le moyen utilisé par le *spyware* Gator.

Il consiste à empaqueter le logiciel espion dans un logiciel légitime. De nombreux éditeurs de programmes gratuits utilisent cette méthode pour générer des revenus. La méthode utilisée est très simple.

Il suffit d'installer le *spyware* en même temps que le logiciel original. Lorsque l'utilisateur démarrera le programme, des fenêtres publicitaires viendront s'afficher à l'écran.

Cette méthode est de loin la plus efficace, mais elle est surtout utilisée par les *adwares*, elle ne sera pas approfondie ici car son fonctionnement est connu.

2.2 Composants ActiveX (« *Drive-by install* »)

Un autre moyen, très efficace et répandu, est d'utiliser la technologie ActiveX de Microsoft[1]. Celle-ci consiste à incorporer le *spyware* dans un composant ActiveX disponible sur une page internet, permettant ainsi son installation via le navigateur.

Ce chapitre n'explique en aucun cas toute la problématique ActiveX. Pour une étude détaillée se référer à [ACVB6].

2.2.1 Définition

La technologie ActiveX est la réponse de Microsoft à la technologie des applets Java de Sun Microsystems[2]. Ces 2 technologies permettent l'insertion de code mobile dans les pages internet rendant ainsi un site web dynamique.

ActiveX est la dénomination web du modèle de programmation objet COM (*Component Object Model*). Elle permet d'insérer dans une page internet, un composant ActiveX qui sera téléchargé et exécuté automatiquement par le navigateur web.

Il convient de préciser qu'à l'origine, ActiveX n'était disponible que sur le navigateur Microsoft Internet Explorer (IE), ce qui semble logique vu que c'est une technologie propriétaire. Aujourd'hui, cependant, des *plugins* peuvent être installés sur d'autres navigateurs[3] (Mozilla Firefox, Netscape Navigator,…), permettant ainsi la prise en charge de cette technologie.

[1] http://www.microsoft.com/
[2] http://java.sun.com/
[3] http://www.iol.ie/~locka/mozilla/plugin.htm

2.2.2 Caractéristiques

A l'instar de Java, qui évolue dans un environnement de type *sandbox* (bac à sable), la technologie ActiveX n'est pas limitée dans les actions qu'elle peut entreprendre sur la machine client. En effet, étant dérivée de COM, un composant ActiveX a accès à **tous** les éléments de la machine. On comprend bien, alors, pourquoi elle est utilisée par les développeurs de *spywares* ou autres logiciels malveillants.

De plus, étant un objet COM, un composant ActiveX possède les caractéristiques suivantes :

- Il peut être développé dans n'importe quel langage. La création de l'objet ActiveX sera alors effectuée par le compilateur
- Il nécessite certains fichiers DLL spécifiques pour pouvoir s'exécuter
- Réutilisation possible. Une fois le contrôle installé, il peut être réutilisé à n'importe quel moment
- Peut accéder à tous les éléments de la machine
- Le terme **composant ActiveX** englobe :
  - Les librairies dynamiques ActiveX (`*.dll`)
  - Les exécutables ActiveX (`*.exe`)
  - Les contrôles ActiveX (`*.ocx`)

Le terme contrôle ActiveX est utilisé pour la dénomination des 3 types de composants. Bien que n'étant pas exactement correcte, nous utiliserons désormais cette dénomination, car elle est employée par Microsoft.

Nous n'étudierons ici que le mécanisme de téléchargement d'un composant ActiveX sur une page internet. Pour la programmation même des composants, se référer à [ACVB6].

2.2.3 La sécurité dans ActiveX

Les objets ActiveX présentent des risques considérables sur le plan de la sécurité. Étant donné qu'ils ne sont en aucun cas limités dans les actions qu'ils peuvent entreprendre, ils peuvent modifier ou même supprimer tout élément sur la machine.

Microsoft a donc mis au point, un modèle de sécurité basé exclusivement sur les signatures numériques et certificats (*Authenticodes*). Ce certificat, délivré par une autorité de certification, telle VeriSign Inc[4], assure uniquement que le contrôle n'a pas été modifié par une tierce personne, depuis sa création. Il n'assure en aucun cas que l'ActiveX aura un comportement « honnête » et qu'il ne causera aucun dommage à l'utilisateur.

La décision finale revient donc à l'utilisateur, qui devra choisir, uniquement en fonction du signataire, s'il désire installer le contrôle ActiveX nécessaire, ou poursuivre sa visite sur la page web sans la fonctionnalité proposée.

[4] http://www.verisign.com/

Nous avons donc à faire à une politique de type tout ou rien. Soit on accepte le contrôle et dans ce cas, il peut effectuer ce que bon lui semble sur la machine, soit on ne l'accepte pas et il ne peut rien effectuer.

Ce niveau de sécurité n'étant pas optimal, il existe d'autres éléments permettant d'améliorer la sécurité :

- **Approuvé par l'administrateur** : chaque zone de sécurité dans IE possède cette option, permettant d'exécuter un contrôle ActiveX uniquement si l'administrateur de l'ordinateur l'a approuvé
- ***CodeBaseSearchPath*** : cette clé de registre permet de définir à partir de quels emplacements, le téléchargement d'un contrôle ActiveX est autorisé
- **Drapeaux « Sûr pour … »** : lors de la compilation d'un contrôle ActiveX, le programmeur a la possibilité de marquer son contrôle comme étant sûr pour l'initialisation et pour l'écriture de scripts. Un contrôle est marqué comme sûr pour l'écriture de scripts s'il n'accède ni à la base de registre ni à la mémoire et n'effectue pas directement une opération d'entrée/sortie sur la machine
- ***Kill bit*** : c'est une valeur de registre permettant d'interdire l'exécution d'un contrôle ActiveX déjà installé

Les options de sécurité d'IE nous permettent, aussi, de définir un certain niveau de sécurité. Elles seront traitées en §3.1.3, §3.1.4 et §3.1.5.

2.2.4 Les ActiveX par défaut

Lors de l'installation du système d'exploitation (SE), les composants ActiveX indispensables à son fonctionnement sont installés sur la machine.

La plus part des composants par défaut s'installent dans `C:\WINDOWS\system32`, cependant ce n'est pas une règle obligatoire. Chaque application peut installer ses ActiveX où elle le désire, Microsoft Outlook Express les placera donc dans `C:\Program Files\Outlook Express` et Microsoft Office 2003 dans `C:\Program Files\Microsoft Office`.

Une liste des ActiveX installés par défaut sur la machine se trouve sur le CD sous : `Autres\activex_par_defaut.xls`.

2.2.5 Installation d'un contrôle ActiveX depuis une page web

L'installation d'un ActiveX peut être effectuée à partir de tout support de données (disquette, CD-ROM, …). Nous allons ici détailler le processus lors de l'installation à partir d'une page web.

De manière à pouvoir être téléchargé et exécuté le plus rapidement possible, le contrôle ActiveX est souvent empaqueté avec tous les autres fichiers nécessaires (notamment les `*.dll`) à son exécution dans une archive `*.cab` (fichier cabinet), qui utilise une technique de compression sans pertes.

L'appel à ce contrôle se fait en insérant ces quelques lignes dans le code source de la page web :

```
<OBJECT
      CLASSID = « CLSID :xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx »
      CODEBASE = « www.site.com/controle.cab#version=1,0,0,0 »>
</OBJECT>
```

Où :

- **CLSID** : est l'identificateur de classe du contrôle, c'est une valeur unique et universelle. Il sera ajouté dans la base de registre lors de l'installation du contrôle

- **CODEBASE** : est l'URL à partir duquel le contrôle ActiveX pourra être téléchargé

- **Version** : spécifie la version du contrôle à télécharger. Cette option est utilisée, le plus souvent, pour mettre à jour un contrôle ActiveX

Dans le cas où l'utilisation d'un fichier `*.cab` n'est pas jugée nécessaire par le créateur de la page web, le contrôle peut être intégré directement sans compression. On procédera dans ce cas comme suit :

```
<OBJECT
      CLASSID = « CLSID :xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx »
      CODEBASE = « www.site.com/controle.ocx#version=1,0,0,0 »>
</OBJECT>
```

Cette solution télécharge uniquement le fichier `*.ocx` du contrôle, et exige l'installation préalable de toutes les `dll` de prise en charge sur l'ordinateur client.

Le processus complet d'installation d'un contrôle ActiveX, provenant d'un site internet, sur la machine client, passe par plusieurs étapes :

- **Acquisition** : le navigateur commence par vérifier si l'identificateur de classe de la balise `<OBJECT>` est présent dans la base de registre. S'il n'est pas présent, le contrôle est téléchargé sur la machine et on passe à l'étape suivante. S'il est présent on passe directement à l'étape exécution

- **Vérification** : le navigateur vérifie, ici, si le contrôle est signé et marqué comme sûr pour l'écriture de scripts

- **Installation** : cette étape installe le contrôle ActiveX sur la machine et l'enregistre dans la base de registre

- **Exécution** : le contrôle peut alors exécuter les actions pour lesquelles il a été programmé

Suivant les tests de sécurité passés et les options de sécurité du navigateur, des fenêtres interrogeant l'utilisateur peuvent s'afficher. Nous le verrons en §2.2.6.

Lors d'une prochaine visite sur cette page web, le navigateur s'aperçoit, à l'aide du champ `CLSID`, que le contrôle défini dans la balise `<OBJECT>` est déjà installé sur la machine. Il peut alors s'exécuter directement.

Remarque : Il existe une autre balise HTML permettant de télécharger des composants à partir d'une page web, c'est <HREF>. Cependant, elle n'est pas utilisée dans ce cas, car elle ne met à disposition aucune option de sécurité (vérification).

2.2.6 Infection à partir d'un ActiveX

En surfant sur le web, on tombe parfois sur des sites qui offrent certains services utiles. Cependant pour avoir accès à ces services, il nous est indiqué qu'il faut procéder à l'installation d'un logiciel requis. Ce premier exemple montre bien ce cas.

2.2.6.1 Mode administrateur

Pour illustrer cet exemple, nous procédons tout d'abord à une analyse du système avant infection, à l'aide de l'outil HijackThis, présenté en annexe A3.1, et de l'utilitaire Ajout/Suppression de programmes disponible dans le Panneau de configuration.

L'outil HijackThis nous donne le log suivant :

```
Logfile of HijackThis v1.99.1
Scan saved at 11:18:35, on 10.10.2005
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)

Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Program Files\VMware\VMware Tools\VMwareService.exe
C:\WINDOWS\Explorer.EXE
C:\Program Files\VMware\VMware Tools\VMwareTray.exe
C:\Program Files\VMware\VMware Tools\VMwareUser.exe
C:\WINDOWS\system32\wscntfy.exe
C:\WINDOWS\system32\wpabaln.exe
C:\Documents and Settings\BDS\Bureau\HijackThis.exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName
= Liens
O4 - HKLM\..\Run: [VMware Tools] C:\Program Files\VMware\VMware
Tools\VMwareTray.exe
O4 - HKLM\..\Run: [VMware User Process] C:\Program Files\VMware\VMware
Tools\VMwareUser.exe
O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} -
C:\Program Files\Messenger\msmsgs.exe
O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-
BB9E-00C04F795683} - C:\Program Files\Messenger\msmsgs.exe
O17 - HKLM\System\CCS\Services\Tcpip\..\{D5967F0E-E436-49D2-8335-
7F59DA95F3CE}: NameServer = 10.1.1.10
O23 - Service: Remote Packet Capture Protocol v.0 (experimental)
(rpcapd) - Unknown owner - %ProgramFiles%\WinPcap\rpcapd.exe" -d -f
"%ProgramFiles%\WinPcap\rpcapd.ini (file missing)
```

```
O23 - Service: VMware Tools Service (VMTools) - VMware, Inc. -
C:\Program Files\VMware\VMware Tools\VMwareService.exe
```

Fig. 1 - Admin - Log HijackThis avant infection (ActiveX)

Nous voyons que seuls les processus nécessaires au fonctionnement de Windows XP sont lancés :

- **`Smss.exe`** : *session manager subsystem*
- **`Winlogon.exe`** : *Windows login subsystem*
- **`Services.exe`** : *services control manager*
- **`Lsass.exe`** : *local security authentication server*
- **`Svchost.exe`** : *generic host process for Win32 services*
- **`Spoolsv.exe`** : *spooler service, responsible for managing spooled print services*
- **`Explorer.exe`** : *user shell*
- **`Wscntfy.exe`** : *Windows security center notification aplication*
- **`Wpabaln.exe`** : *responsible for licencing issues*

Ainsi que les programmes utilisés en ce moment :

- **`VMwareService.exe, VMwareTray.exe, VMwareUser.exe`** : processus faisant partie de l'environnement VMware décrit en annexe A1
- **`HijackThis.exe`** : générateur du log

Nous voyons ensuite les clés de registre utilisées :

- **`R0`** : le nom du dossier de liens est : Liens
- **`O4`** : `VMwareTray.exe` et `VMwareUser.exe` se lancent automatiquement au démarrage de la machine, à partir de la base de registre
- **`O9`** : Windows Messenger apparaît en tant que bouton supplémentaire et item menu dans IE
- **`O17`** : le serveur DNS est 10.1.1.10
- **`O23`** : WinPcap et `VMwareServices.exe` sont des services NT

Nous procédons aussi à une capture d'écran de l'utilitaire Ajout/Suppression de programmes.

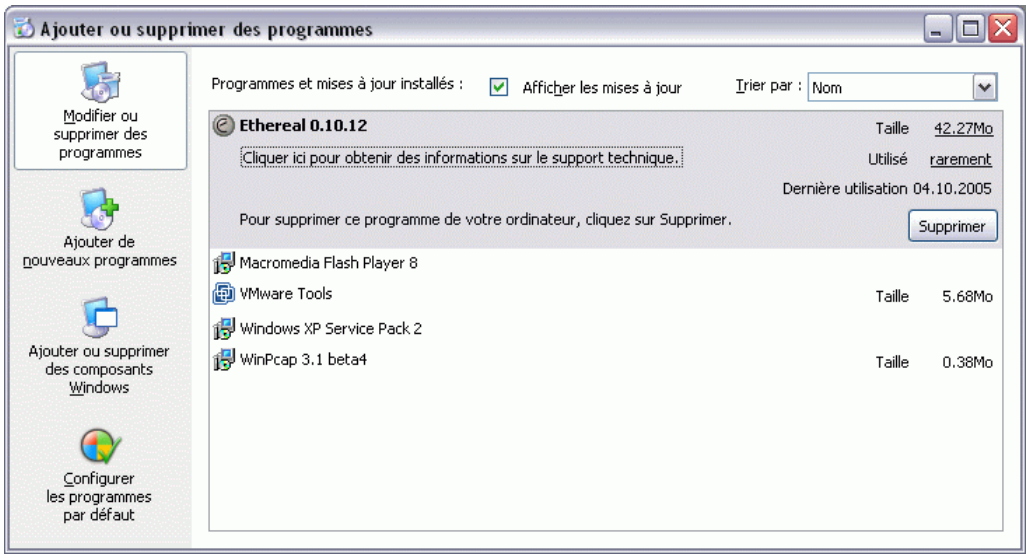


Fig. 2 - Admin - Programmes avant infection (ActiveX)

Nous remarquons la présence des logiciels légitimes Ethereal, Macromedia Flash Player, VMware et WinPcap. Ainsi que le SP2 de Windows XP.

Nous nous dirigeons ensuite vers le site www.cracks.am, qui met à notre disposition des numéros de série et des patches pour certains logiciels. Nous décidons alors de poursuivre et de télécharger un patch pour un logiciel quelconque.

Pour cela, allons directement à l'adresse www.cracks.am/d.x?82506 qui nous permet de télécharger un patch pour un logiciel serveur ftp.

La page s'affiche et nous invite à installer l'ActiveX, soit disant, nécessaire.

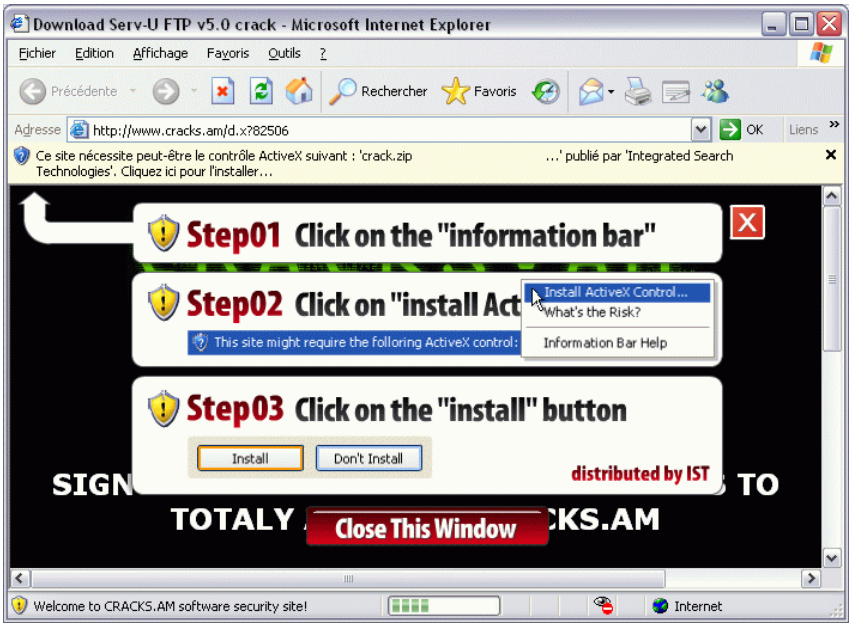


Fig. 3 - Admin - Avis ActiveX (ActiveX)

Nous procédons à l'installation de l'ActiveX.

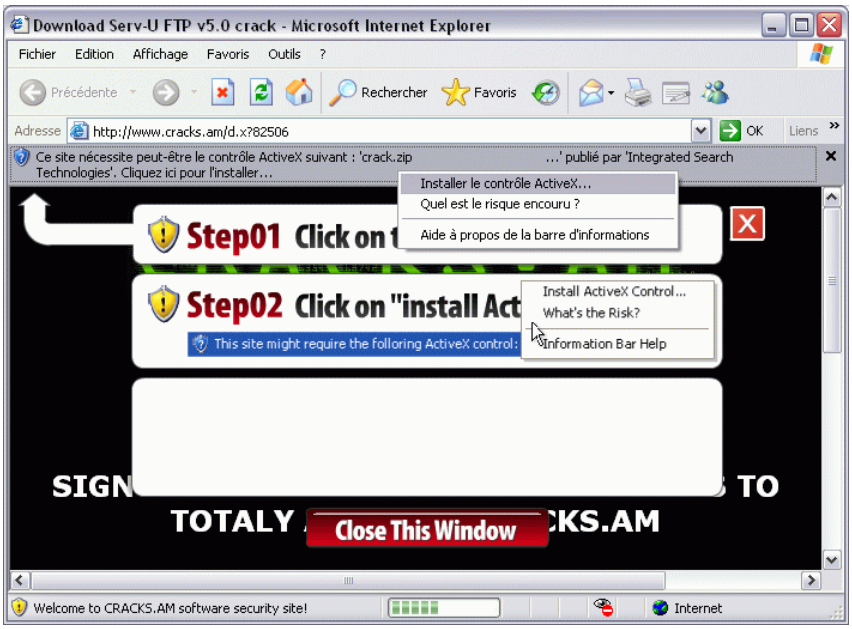


Fig. 4 - Admin - Installation ActiveX (ActiveX)

Un avertissement de sécurité nous demande alors si on désire installer ce logiciel. Il nous indique le nom de l'éditeur.

Fig. 5 - Admin - Avertissement de sécurité (ActiveX)

Nous analysons le certificat présent.

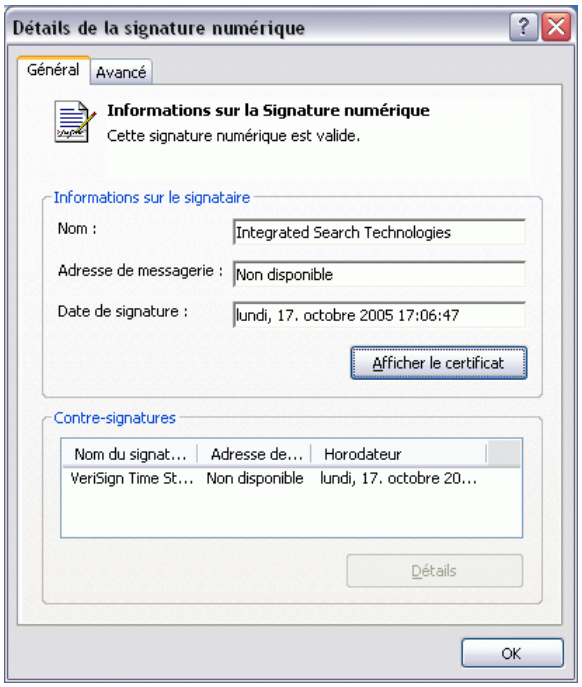


Fig. 6 - Admin - Détails signature numérique (ActiveX)

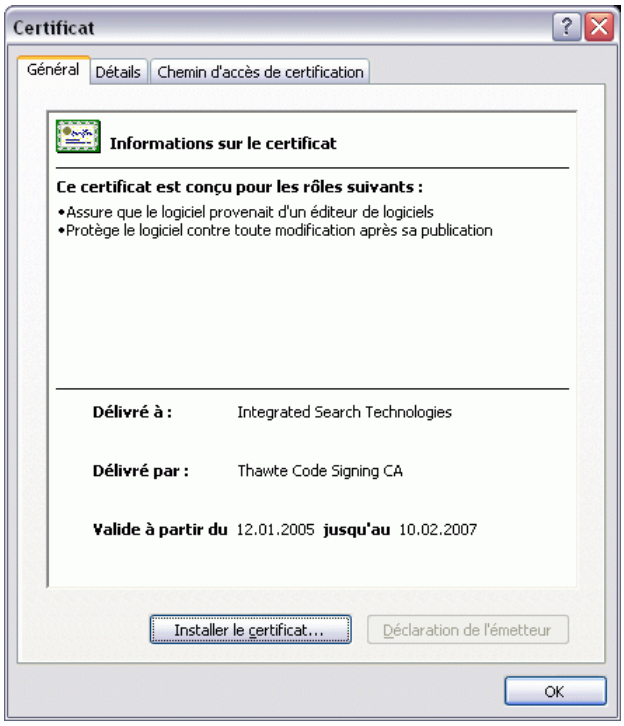


Fig. 7 - Admin - Certificat (ActiveX)

Ayant vérifié que le certificat a bien été délivré par une CA reconnue. Nous choisissons de l'installer, espérant finalement obtenir le fichier désiré.

À notre grande surprise une nouvelle page web s'ouvre et nous indique que l'installation de la barre d'outils est maintenant terminée. Il faut alors se demander s'il était indiqué quelque part qu'on allait installer une barre d'outils !

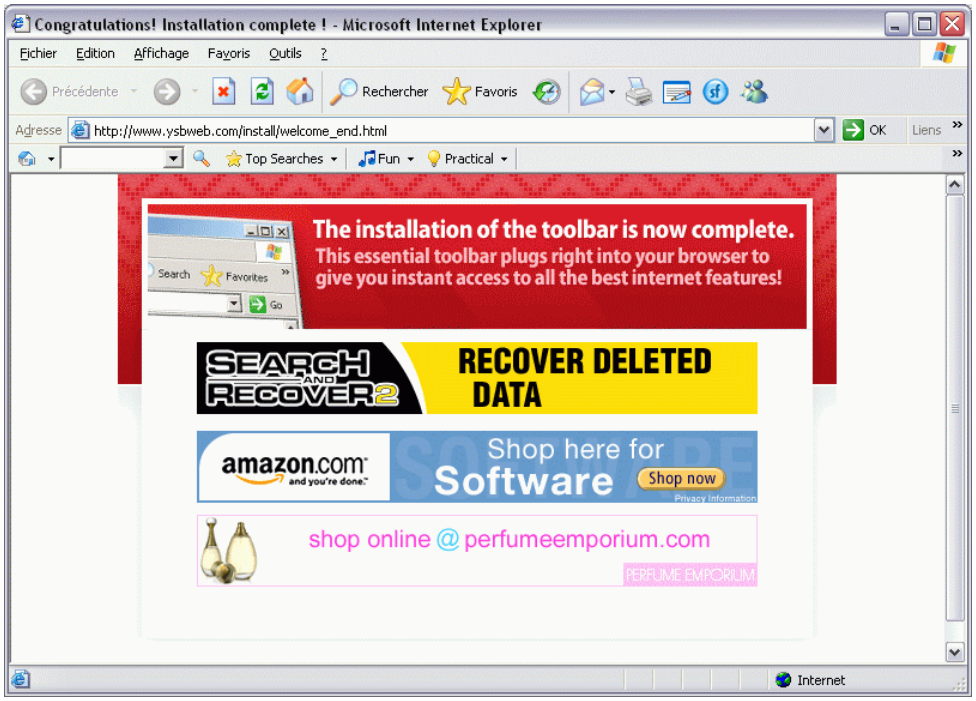


Fig. 8 - Admin - Confirmation de l'installation de la barre d'outils (ActiveX)

Nous espérons alors pouvoir, enfin, avoir accès au fichier désiré, cependant lorsqu'on referme cette fenêtre, une autre installation nous attend.

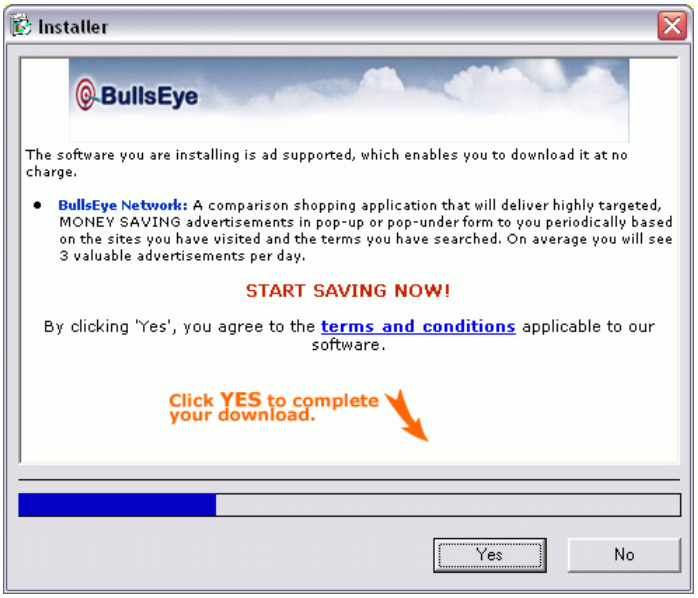


Fig. 9 - Admin - Installation BullsEye (ActiveX)

Une fois cette installation terminée, nous avons enfin accès au fichier désiré depuis le début.

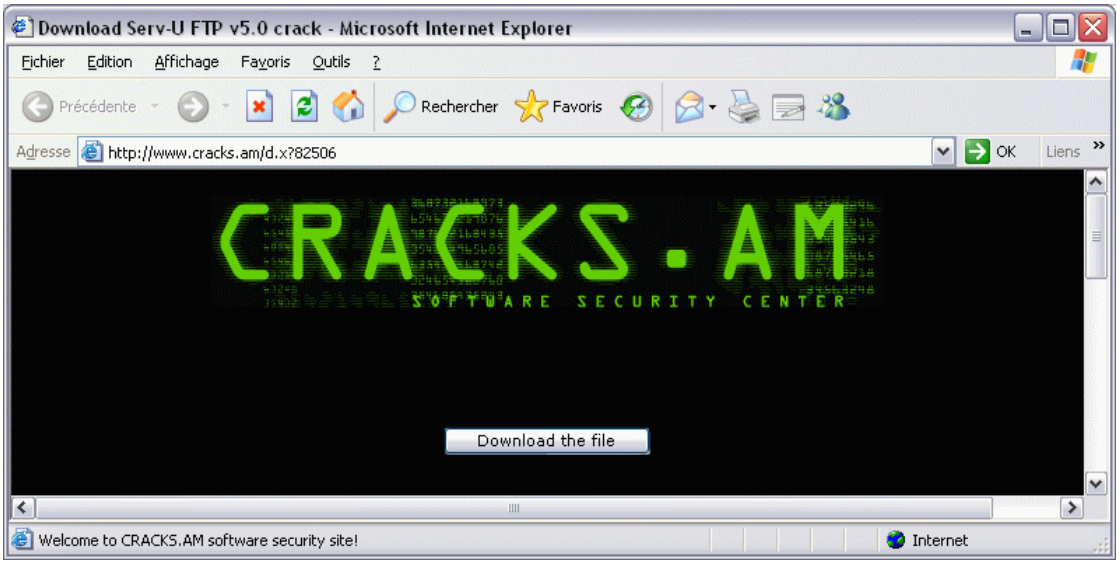


Fig. 10 - Admin - Téléchargement du fichier désiré (ActiveX)

Après toutes ces péripéties, il convient de refaire une analyse à l'aide de HijackThis.

```
Logfile of HijackThis v1.99.1
Scan saved at 11:33:42, on 10.10.2005
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)

Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
```

```
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Program Files\VMware\VMware Tools\VMwareService.exe
C:\WINDOWS\Explorer.EXE
C:\Program Files\VMware\VMware Tools\VMwareTray.exe
C:\Program Files\VMware\VMware Tools\VMwareUser.exe
C:\WINDOWS\system32\wscntfy.exe
C:\WINDOWS\system32\wpabaln.exe
C:\Program Files\ISTsvc\istsvc.exe
C:\WINDOWS\lgkkulr.exe
C:\Program Files\SurfAccuracy\SAcc.exe
C:\Program Files\Internet Optimizer\optimize.exe
C:\Program Files\BullsEye Network\bin\bargains.exe
C:\Documents and Settings\BDS\Bureau\HijackThis.exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName
= Liens
R3 - URLSearchHook: (no name) - _{CFBFAE00-17A6-11D0-99CB-00C04FD64497}
- (no file)
O2 - BHO: BHObj Class - {00000010-6F7D-442C-93E3-4A4827C2E4C8} -
C:\WINDOWS\nem220.dll
O2 - BHO: BAHelper Class - {A3FDD654-A057-4971-9844-4ED8E67DBBB8} -
C:\Program Files\SideFind\sfbho.dll
O2 - BHO: ADP UrlCatcher Class - {F4E04583-354E-4076-BE7D-ED6A80FD66DA}
- C:\WINDOWS\system32\msbe.dll
O3 - Toolbar: ISTbar - {FAA356E4-D317-42a6-AB41-A3021C6E7D52} -
C:\Program Files\ISTbar\istbarcm.dll
O4 - HKLM\..\Run: [VMware Tools] C:\Program Files\VMware\VMware
Tools\VMwareTray.exe
O4 - HKLM\..\Run: [VMware User Process] C:\Program Files\VMware\VMware
Tools\VMwareUser.exe
O4 - HKLM\..\Run: [IST Service] C:\Program Files\ISTsvc\istsvc.exe
O4 - HKLM\..\Run: [cjmBBu8i] C:\WINDOWS\lgkkulr.exe
O4 - HKLM\..\Run: [SurfAccuracy] C:\Program Files\SurfAccuracy\SAcc.exe
O4 - HKLM\..\Run: [Internet Optimizer] "C:\Program Files\Internet
Optimizer\optimize.exe"
O4 - HKLM\..\Run: [Power Scan] "C:\Program Files\Power
Scan\powerscan.exe" /aid:138770
O4 - HKLM\..\Run: [BullsEye Network] C:\Program Files\BullsEye
Network\bin\bargains.exe
O9 - Extra button: SideFind - {10E42047-DEB9-4535-A118-B3F6EC39B807} -
C:\Program Files\SideFind\sidefind.dll
O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} -
C:\Program Files\Messenger\msmsgs.exe
O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-
BB9E-00C04F795683} - C:\Program Files\Messenger\msmsgs.exe
O15 - Trusted Zone: http://ny.contentmatch.net (HKLM)
O16 - DPF: {7C559105-9ECF-42B8-B3F7-832E75EDD959} (Installer Class) -
http://www.tbcode.com/ist/softwares/v4.0/0006_cracks.cab
O17 - HKLM\System\CCS\Services\Tcpip\..\{D5967F0E-E436-49D2-8335-
7F59DA95F3CE}: NameServer = 10.1.1.10
O23 - Service: Remote Packet Capture Protocol v.0 (experimental)
(rpcapd) - Unknown owner - %ProgramFiles%\WinPcap\rpcapd.exe" -d -f
"%ProgramFiles%\WinPcap\rpcapd.ini (file missing)
O23 - Service: VMware Tools Service (VMTools) - VMware, Inc. -
C:\Program Files\VMware\VMware Tools\VMwareService.exe
```

Fig. 11 - Admin - Log HijackThis après infection (ActiveX)

Nous remarquons alors que de nouveaux processus sont maintenant lancés :

- **Istsvc.exe : IST service *spyware*.** Ce fichier est reconnu comme étant un *spyware*
- **Lgkkulr.exe** : ce fichier n'est connu d'aucune base de données, car son nom est aléatoire. Cependant, à l'aide de Process Explorer, présenté en annexe A3.5, on peut voir qu'il est utilisé par Istsvc.exe, l'exécutable vu ci-dessus
- **SAcc.exe : SurfAccuracy.** Cet exécutable est reconnu comme un *adware*
- **Optimize.exe : Internet Optimizer.** Reconnu comme un *malware* (*foistware*)
- **Bargains.exe : BullsEye Network.** Reconnu comme un *adware*.

Tous ces processus s'avèrent être des *spywares* (ou dérivés). Nous avons donc été attaqués.

L'analyse des clés de registre nous confirme cela, car en plus des clés présentes auparavant, ces différents processus se sont inscrits dans la base de registre et seront lancés au prochain démarrage.

- **R3** : la page de recherche de IE a été détournée (*hijacked*)
- **02** : quelques BHO sont venus s'ajouter à IE : Internet Optimizer (`nem220.dll`), SideFind *adware* (`sfbho.dll`) et eXact Advertising (`msbe.dll`)
- **03** : une barre d'outils est aussi venue s'incorporer à IE (ISTBar)
- **04** :6 nouveaux programmes se lancent au démarrage du système (IST Service *spyware*, `lgkkulr.exe`, SurfAccuracy, Internet Optimizer, BullsEye Network et Power Scan)
- **09** : un bouton SideFind est venu s'ajouter à celui de Windows Messenger
- **015** : http://ny.contentmatch.net a été ajouté à la liste *Trusted Zone*
- **016** : nous voyons ici quel a été l'objet ActiveX téléchargé par IE, il s'agit de 0006_cracks.cab

Il convient de préciser qu'un BHO est un simple programme démarrant automatiquement au lancement d'IE. La plus part du temps, les BHOs sont utilisés en tant qu'*adwares*.

Nous en déduisons que, le soit disant, contrôle ActiveX nécessaire n'était en fait destiné qu'à installer quelques *adwares* et *spywares* sur notre machine.

Certains de ces logiciels malveillants apparaissent alors dans `Ajout/Suppression de programmes`. Ils pourront donc, à priori, être retirés du système sans trop de difficultés.

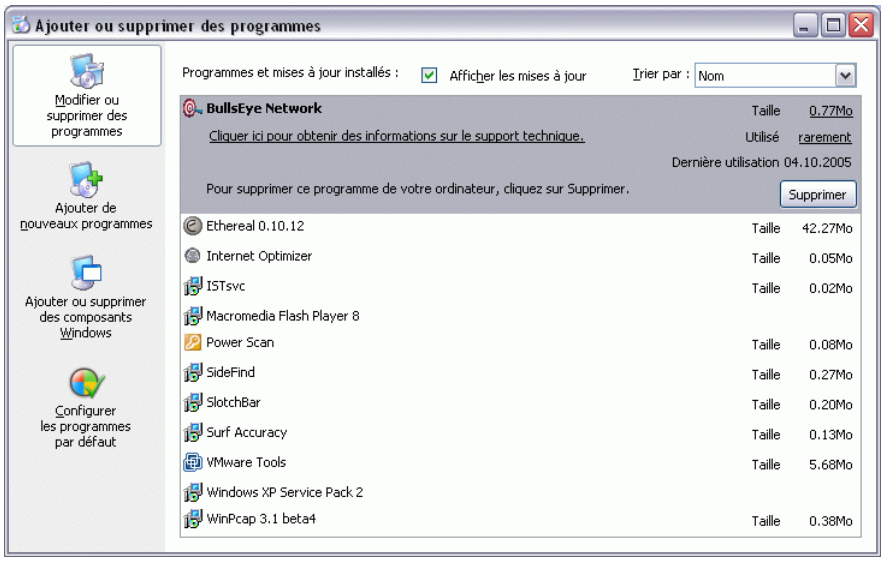


Fig. 12 – Admin - Programmes après infection (ActiveX)

À l'aide du logiciel Ethereal, présenté en Annexe A3.2, observons maintenant comment l'ActiveX est téléchargé.

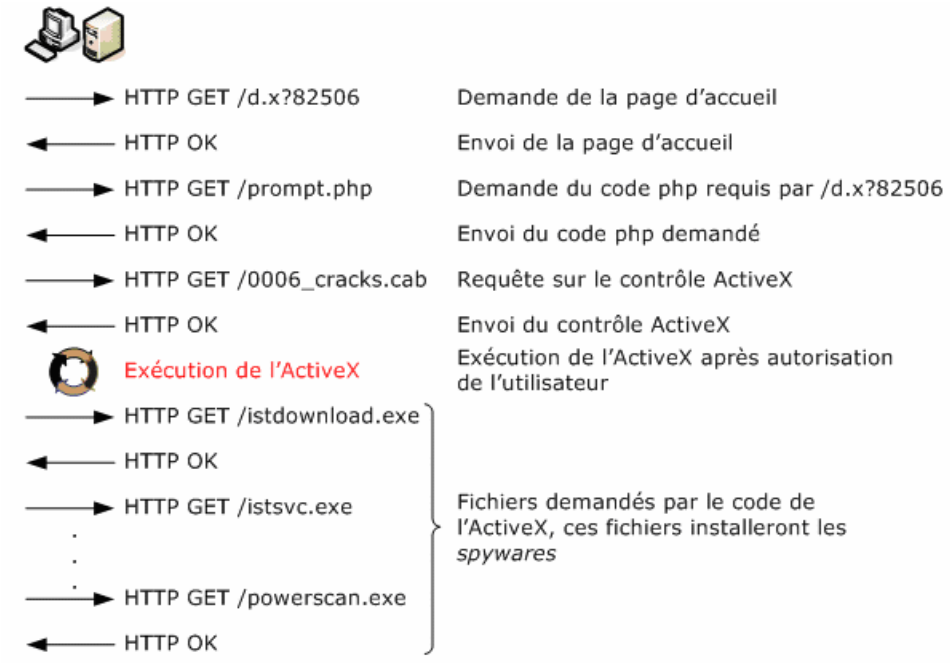


Fig. 13 - Admin - Échange HTTP pour installation (ActiveX)

Le détail complet de l'échange des paquets et des exécutables téléchargés, se trouve sur le CD sous `Tests infection\01 - spyware cracks.am\captures reseau\admin\capture_installation_admin.txt`.

Étant en mode Administrateur, les logiciels ont pu s'installer sans difficultés car l'utilisateur possède **tous** les droits sur la machine.

2.2.6.2 Mode utilisateur

Essayons de répéter la même procédure sur une machine virtuelle propre, cette fois en mode utilisateur.

Le log HijackThis est le suivant :

```
Logfile of HijackThis v1.99.1
Scan saved at 10:39:47, on 11.10.2005
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)

Running processes:
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\system32\wscntfy.exe
C:\Program Files\VMware\VMware Tools\VMwareTray.exe
C:\Program Files\VMware\VMware Tools\VMwareUser.exe
C:\Documents and Settings\user\Bureau\HijackThis.exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName
= Liens
O4 - HKLM\..\Run: [VMware Tools] C:\Program Files\VMware\VMware
Tools\VMwareTray.exe
O4 - HKLM\..\Run: [VMware User Process] C:\Program Files\VMware\VMware
Tools\VMwareUser.exe
O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} -
C:\Program Files\Messenger\msmsgs.exe
O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-
BB9E-00C04F795683} - C:\Program Files\Messenger\msmsgs.exe
O17 - HKLM\System\CCS\Services\Tcpip\..\{D5967F0E-E436-49D2-8335-
7F59DA95F3CE}: NameServer = 10.1.1.10
O23 - Service: Remote Packet Capture Protocol v.0 (experimental)
(rpcapd) - Unknown owner - %ProgramFiles%\WinPcap\rpcapd.exe" -d -f
"%ProgramFiles%\WinPcap\rpcapd.ini (file missing)
O23 - Service: VMware Tools Service (VMTools) - VMware, Inc. -
C:\Program Files\VMware\VMware Tools\VMwareService.exe
```

Fig. 14 - User - Log HijackThis avant infection (ActiveX)

Comme dans le cas administrateur, seuls les processus nécessaires à Windows sont lancés.

Les programmes installés sont les mêmes que ceux présents dans le cas administrateur.

Nous allons ensuite de nouveau sur le site www.cracks.am/d.x?82506.

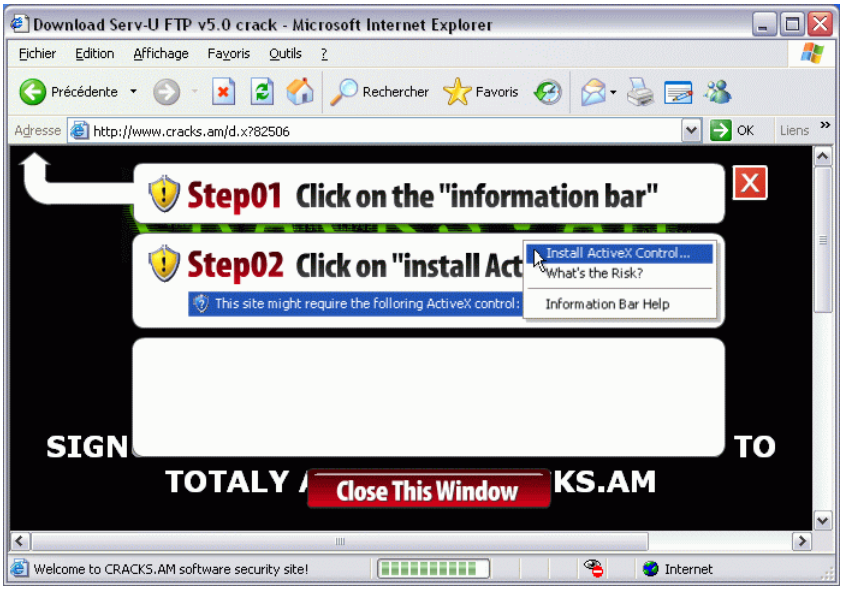


Fig. 15 - User – Avis ActiveX (ActiveX)

Nous nous apercevons qu'il n'est pas possible d'installer le contrôle ActiveX puisque la barre de notification ne le propose pas. Nous en expliquerons plus loin la raison.

Il suffit alors de cliquer sur « *Close This Window* » et le fichier voulu est alors disponible.

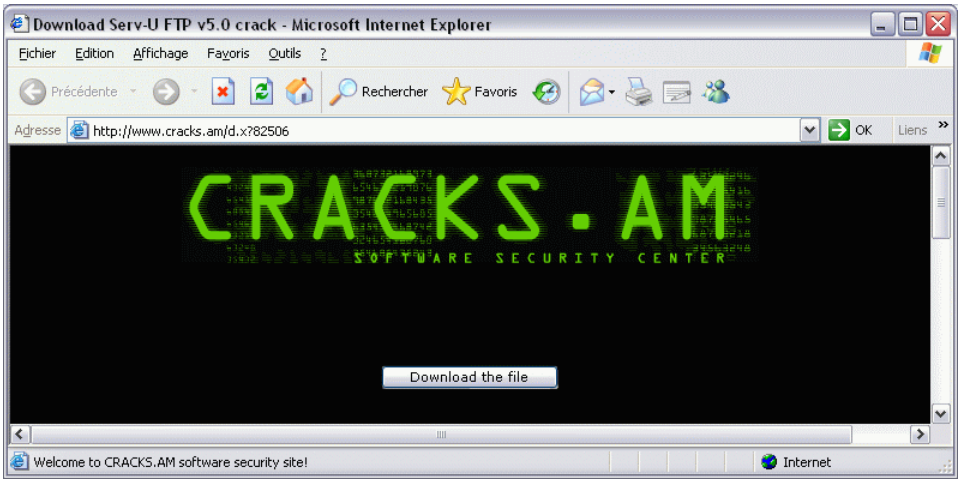


Fig. 16 - User - Téléchargement du fichier désiré (ActiveX)

Il convient, tout de même, d'effectuer à nouveau un log HijackThis, qui confirmera qu'aucun logiciel n'a été installé ou modifié.

```
Logfile of HijackThis v1.99.1
Scan saved at 10:59:20, on 11.10.2005
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)

Running processes:
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\system32\wscntfy.exe
C:\Program Files\VMware\VMware Tools\VMwareTray.exe
```

```
C:\Program Files\VMware\VMware Tools\VMwareUser.exe
C:\Documents and Settings\user\Bureau\HijackThis.exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName
= Liens
O4 - HKLM\..\Run: [VMware Tools] C:\Program Files\VMware\VMware
Tools\VMwareTray.exe
O4 - HKLM\..\Run: [VMware User Process] C:\Program Files\VMware\VMware
Tools\VMwareUser.exe
O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} -
C:\Program Files\Messenger\msmsgs.exe
O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-
BB9E-00C04F795683} - C:\Program Files\Messenger\msmsgs.exe
O17 - HKLM\System\CCS\Services\Tcpip\..\{D5967F0E-E436-49D2-8335-
7F59DA95F3CE}: NameServer = 10.1.1.10
O23 - Service: Remote Packet Capture Protocol v.0 (experimental)
(rpcapd) - Unknown owner - %ProgramFiles%\WinPcap\rpcapd.exe" -d -f
"%ProgramFiles%\WinPcap\rpcapd.ini (file missing)
O23 - Service: VMware Tools Service (VMTools) - VMware, Inc. -
C:\Program Files\VMware\VMware Tools\VMwareService.exe
```

Fig. 17 - User - Log HijackThis après infection (ActiveX)

On peut constater que ce log est identique à celui fait avant d'aller sur la page web.

La liste des programmes installés n'a, quant à elle, pas été modifiée.

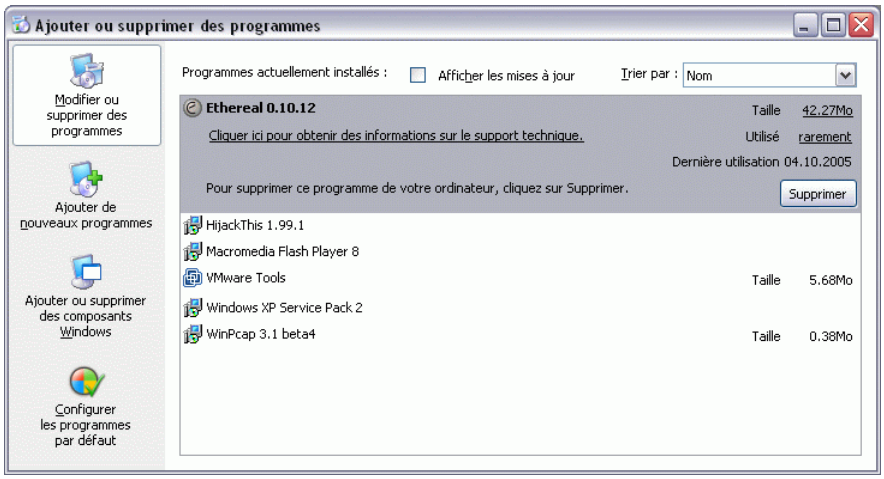


Fig. 18 - User - Programmes après infection (ActiveX)

Expliquons maintenant pourquoi l'installation du contrôle ActiveX n'a pas été possible.

Comme décrit précédemment, le processus d'installation d'un ActiveX passe par plusieurs phases. Dans la phase d'acquisition, la base de registre est accédée pour vérifier si le contrôle existe déjà sur le système. Il convient alors d'observer les accès à la base de registre en utilisant le logiciel Regmon, présenté en annexe A3.3.

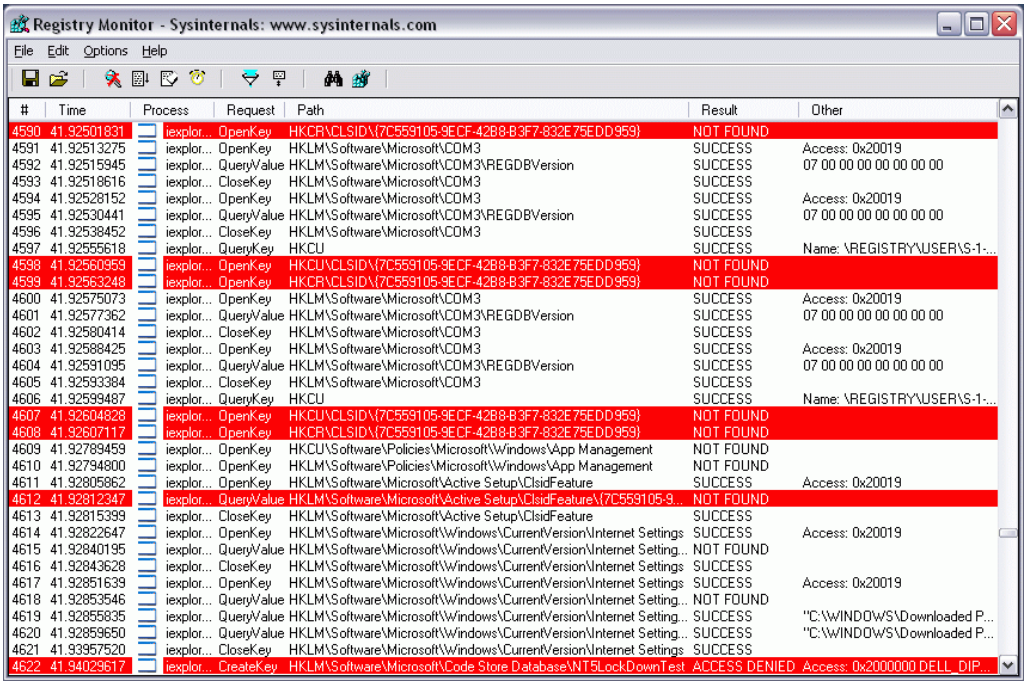


Fig. 19 - User - Accès à la base de registre (ActiveX)

Nous constatons qu'une recherche du CLSID du contrôle ActiveX est entreprise à plusieurs endroits. Ce même contrôle n'ayant pas été installé auparavant sur la machine, le résultat de ces recherches est négatif (NOT FOUND).

IE tente alors de créer une clé de registre (# 4622) pour enregistrer la présence de code mobile. Or, n'oublions pas que nous sommes en mode utilisateur et n'avons pas la permission pour écrire dans `HKLM`. L'accès est donc refusé.

N'ayant pas la possibilité d'enregistrer le contrôle ActiveX, le navigateur ne peut donc pas l'utiliser. Il continue l'affichage de la page sans effectuer cette opération.

L'échange HTTP est donc comme suit :

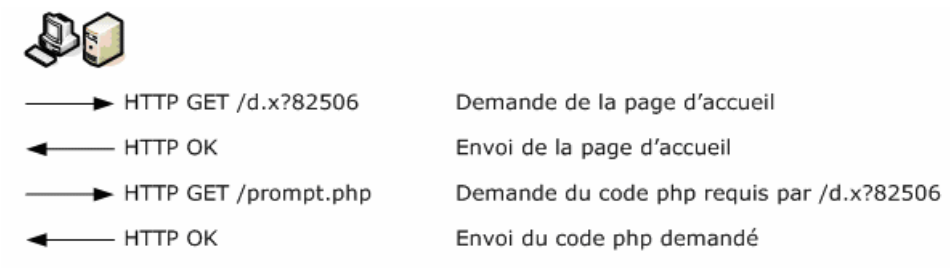


Fig. 20 - User - Échange HTTP pour installation (ActiveX)

Comme vu précédemment, l'enregistrement de l'ActiveX nécessite l'écriture dans la base de registre. Or, l'utilisateur n'ayant pas le droit de modifier certaines clés, le contrôle ActiveX n'est pas téléchargé. L'affichage de la page se poursuit sans l'ActiveX.

L'échange complet se trouve sur le CD sous `Tests infection\01 - spyware cracks.am\captures reseau\user\capture_installation_user.txt`.

2.2.6.3 Envoi et récupération d'informations par les *spywares*

Le but premier d'un *spyware* étant de transmettre des informations à son serveur, il nous faut réaliser une capture réseau des échanges HTTP, de manière à connaître les informations échangées. Nous retournons ici en mode administrateur et réalisons une capture.

Fig. 21 - Envoi et récupération de données 1 (ActiveX)

Quelques temps plus tard, un autre échange a lieu.

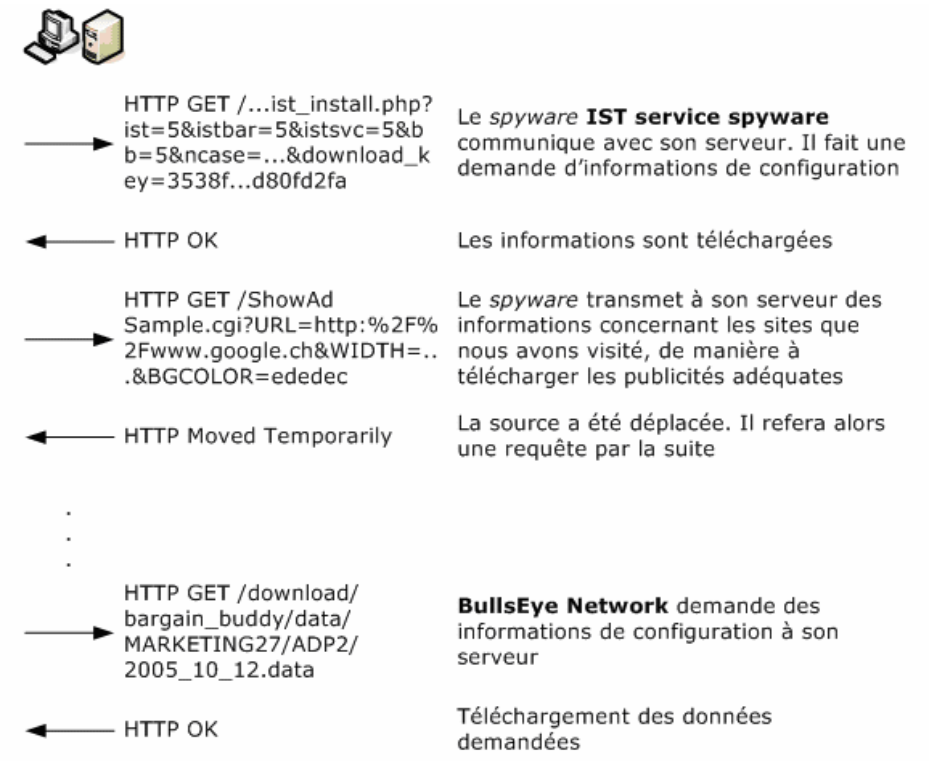


Fig. 22 - Envoi et récupération de données 2 (ActiveX)

Les échanges complets se trouvent sur le CD sous `Tests infection\01 - spyware cracks.am\captures reseau\admin\transmission_spyware_1_admin.txt` et `Tests infection\01 - spyware cracks.am\captures reseau\admin\transmission_spyware_2_admin.txt`.

Ces 2 échanges ne sont qu'un aperçu, des nombreuses informations transmises par les *spywares*.

2.3 Installation en utilisant des failles de sécurité du navigateur

La réalisation d'exploits, se basant sur des failles du navigateur ou du système d'exploitation, est très souvent utilisée pour installer des menaces sur une machine distante.

Les techniques utilisées sont le plus souvent liées à des « *buffer overflow* », elles permettent ensuite l'exécution de code sur la machine distante et donc l'installation de *spywares*.

Dernièrement une vulnérabilité[5] d'Internet Explorer dans la gestion des formats icône et curseur[6] a permis l'installation du *spyware* SearchMeUp sur des milliers de machines.

L'étude d'un exploit utilisant une faille est une opération très intéressante, mais cependant très longue et compliquée. Elle ne sera pas mise en œuvre ici, car il est très difficile de trouver un site utilisant cette méthode et restant actif plus d'un jour ou deux.

[5] http://www.reseaux-telecoms.net/actualites/lire-mariage-det-x92-un-*spyware*-et-det-x92-une-faille-ie-10841.html
[6] http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx

3 Protection

15 jours d'étude

3.1 Protection logicielle

Le fait d'avoir un *spyware* présent sur sa machine peut être très néfaste, du point de vue performances système, mais surtout en ce qui concerne la confidentialité des données.

Il existe plusieurs moyens de limiter les risques d'infection.

3.1.1 *Windows XP Security Checklist*

Tout d'abord il faut configurer le SE de manière à avoir une machine sécurisée contre les attaques informatiques en général, sans se focaliser sur les *spywares*. Il faut pour cela prendre quelques précautions de base de manière à avoir une bonne configuration du poste client. Il faut entre autres :

- Utiliser des mots de passe pour tous les comptes de la machine
- Désactiver le compte Invité
- Renommer le compte Administrateur
- N'utiliser les comptes administrateurs que lorsque c'est réellement nécessaire
- Désactiver le partage de fichiers simple (`Poste de travail -> Outils -> Options des dossiers -> Affichage`, désactiver la coche « Utiliser le partage de fichiers simple »)
- Désactiver les partages par défaut (`HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters`, créer une valeur de type `REG_DWORD` nommée `AutoShareWks` et la mettre à 0)
- Désactiver le bureau à distance (Click droit sur `Poste de travail -> Propriétés -> Utilisation à distance`, désactiver la coche « Autoriser les utilisateurs à se connecter à distance à cet ordinateur »)
- Désactiver les services non nécessaires (`Panneau de configuration -> Outils d'administration -> Services`, désactiver « Accès à distance au registre, Service de découvertes SSDP, Telnet… »).

Ces mesures offrent une bonne protection de base, cependant beaucoup d'autres peuvent être prises, pour une liste exhaustive se référer à [CHECKL].

3.1.2 Windows Update

Les *spywares* utilisent certaines failles d'IE et de Windows pour s'installer, il devient alors indispensable de maintenir à jour les logiciels utilisés et d'appliquer tous les patchs disponibles (`Panneau de configuration -> Mises à jour automatiques -> Installation automatique`).

3.1.3 Configuration de la zone « Internet »

Sachant que le téléchargement d'un ActiveX à partir d'Internet est un des vecteurs d'installation les plus répandus, il convient de définir un haut niveau de sécurité du navigateur pour ces composants.

Nous allons pour cela configurer les paramètres de sécurité du navigateur IE disponibles sous `Internet Explorer -> Outils -> Options Internet -> Sécurité -> Personnaliser le niveau`.

Les champs nous intéressant sont ceux sous « Contrôles ActiveX et plugins » :

Contrôles ActiveX et plugins	**Faible**	**Moyen**	**Élevé**	**Recommandé**
Comportement de fichiers binaires et des scripts (*Binary and script behaviors*)	Activer	Activer	Désactiver	Désactiver
Contrôles ActiveX reconnus sûrs pour l'écriture de scripts (*Script ActiveX controls marked safe for scripting*)	Activer	Activer	Désactiver	Demander
Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés (*Initialize and script ActiveX controls not marked as safe*)	Demander	Désactiver	Désactiver	Désactiver
Demander confirmation pour les contrôles ActiveX (*Automatic prompting for ActiveX controls*)	Activer	Désactiver	Désactiver	Activer
Exécuter les contrôles ActiveX et les plugins (*Run ActiveX controls and plugins*)	Activer	Activer	Désactiver	Demander
Télécharger les contrôles ActiveX non signés (*Download unsigned ActiveX controls*)	Demander	Désactiver	Désactiver	Désactiver
Télécharger les contrôles ActiveX signés (*Download signed ActiveX controls*)	Activer	Demander	Désactiver	Demander

Fig. 23 - Réglages IE6 - Contrôles ActiveX et plugins

Remarque : l'ordre des champs n'est pas le même sur la version anglaise du navigateur.

Les réglages idéaux pour une sécurité absolue sont ceux définis dans le niveau de sécurité « Élevé ». Cependant, beaucoup de pages ne sont pas affichées correctement lors de l'utilisation de ce niveau.

Nous adopterons ici le niveau de sécurité « Élevé », dans lequel on modifiera les éléments indiqués sous « Recommandé », de manière à laisser à l'utilisateur le choix d'utiliser, ou pas, certains composants ActiveX.

Après quelques temps et une analyse réfléchie des conséquences, ces mêmes réglages pourront être modifiés selon les habitudes de l'utilisateur.

Une autre solution est d'utiliser le niveau de sécurité « Élevé » et d'ajouter les sites auxquels ont fait entièrement confiance à la zone « Sites de confiance ».

3.1.4 Configuration de la zone « Sites de confiance »

Cette zone fonctionne selon un modèle « liste blanche ».

Lorsqu'on fait entièrement confiance à un site, il peut être ajouté à cette zone. Pour cela cliquer sur l'icône « Sites de confiance », dans les propriétés d'IE6, puis sur « Sites… » et ajouter le domaine ou le site à la liste, sous la forme : ***.unige.ch**. Ce qui indique que tous les sites du domaine unige.ch seront traités selon le niveau de sécurité défini pour cette zone.

Étant donné que seuls les sites auxquels on fait complètement confiance sont insérés dans cette zone, le niveau de sécurité peut être celui par défaut (Faible), qui autorise presque tous les contrôles ActiveX et demande l'autorisation de l'utilisateur pour les autres.

3.1.5 Configuration de la zone « Sites sensibles »

Contrairement à la zone précédente, le modèle utilisé ici est celui de « liste noire ».

Lorsqu'un site frauduleux ou malintentionné est détecté, il peut (ou doit) être ajouté à cette zone, de la même manière que pour la zone précédente. Nous aurons dans cette catégorie des sites tels : ***.180solutions.com** ou ***.absolutdialer.com**.

Le niveau par défaut pour cette zone est « Élevé », ce qui interdit tous les ActiveX et téléchargements de fichiers.

3.1.6 Utilisation de l'ActiveX *kill bit*

Cette méthode est elle aussi basée sur un modèle de « liste noire ».

Il existe un bit (*kill bit*) qui permet d'empêcher l'utilisation d'un contrôle ActiveX, quel qu'il soit. Ce bit peut être modifié directement dans la base de registre, dans les paramètres d'IE sous `Internet Explorer -> Outils -> Options Internet -> Programmes -> Gérer les modules complémentaires` ou à travers un logiciel externe.

Lors de la modification à travers IE, seuls les Activex qui ont déjà été utilisés au moins une fois peuvent être désactivés (Choisir l'ActiveX à bloquer et cliquer sur « Désactiver » puis « OK »).

Si l'opération est effectuée manuellement dans le registre, les ActiveX n'ayant pas encore été utilisés peuvent aussi être désactivés en ajoutant leurs `CLSIDs`, ce qui évite de les télécharger ne serait-ce qu'une fois.

Chaque ActiveX contient un identificateur de classe (CLSID), cet identificateur est enregistré dans la base de registre. Prenons par exemple le contrôle ActiveX 0006_cracks.cab téléchargé au §2.2.6.1, son CLSID est {7C559105-9ECF-42B8-B3F7-832E75EDD959}. Nous voulons empêcher toute utilisation ou téléchargement de cet ActiveX. Il suffit pour cela de créer une clé correspondante au CLSID dans la base de registre et de mettre le *kill bit* à 1.

Plus concrètement, nous procéderons comme suit :

- **CreateKey HKLM \ Software \ Microsoft \ Internet Explorer \ ActiveX Compatibility\{7C559105-9ECF-42B8-B3F7-832E75EDD959}**
- **SetValue … \ ActiveX Compatibility \ {7C559105-9ECF-42B8-B3F7-832E75EDD959} \ Compatibility Flags DWORD=0x400**
- **CloseKey … \ ActiveX Compatibility \ {7C559105-9ECF-42B8-B3F7-832E75EDD959}**

Les CLSIDs des ActiveX reconnus comme malicieux, peuvent ainsi être ajoutés à cette liste avant infection. Il faudra pour cela utiliser une base de données tel [CASTLE] ou utiliser un logiciel tel *Spyware*Blaster (§3.1.7).

Il en est de même pour les *cookies* des sites reconnus comme malicieux. Ils peuvent être ajoutés manuellement en utilisant IE (Propriétés Internet -> Confidentialité -> Sites…) ou directement dans la base de registre.

3.1.7 *Spyware*Blaster 3.4[7]

*Spyware*Blaster est un utilitaire gratuit, de Javacool Software Llc., qui permet de maintenir à jour une liste de contrôles ActiveX, de *cookies*, de sites indésirables et de configurer le navigateur (IE ou Firefox) pour qu'il ne les accepte pas. Il est donc basé sur un modèle « liste noire ».

De plus, il possède quelques outils très utiles permettant, entre autres, de rétablir les pages par défaut d'IE et d'ajouter une liste personnalisée de contrôles ActiveX à bloquer.

Pour pouvoir avoir accès à toutes les fonctionnalités du logiciel, l'utilisateur doit posséder les droits administrateur sur la machine, car le logiciel modifie et crée certaines clés de registre disponibles sous HKLM. Cependant, quelques fonctions ne nécessitent pas de droits privilégiés, car elles ne modifient ou créent que des clés disponibles sous HKCU.

[7] http://www.javacoolsoftware.com/

Après installation, il est conseillé de faire une mise à jour à partir de la base de données en cliquant sur « *Download Latest Protection Updates* », et d'activer toutes les protections disponibles, en cliquant sur « *Enable All Protection* ».

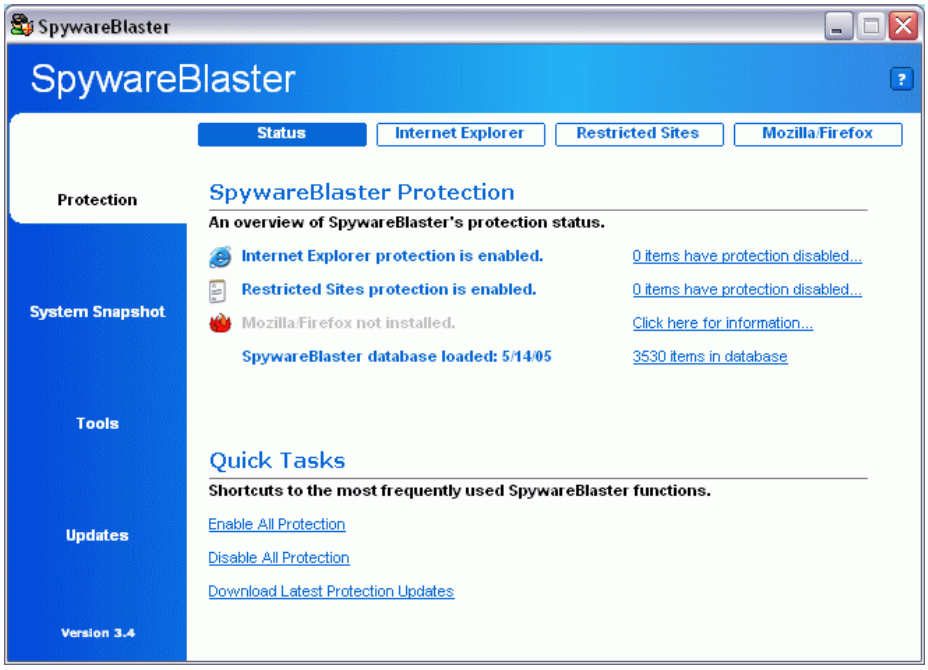


Fig. 24 - *Spyware*Blaster - Écran d'accueil

Pour mieux comprendre le fonctionnement du logiciel, nous utilisons le logiciel Regmon lors de l'activation de toutes les protections, de manière à contrôler les accès à la base de registre.

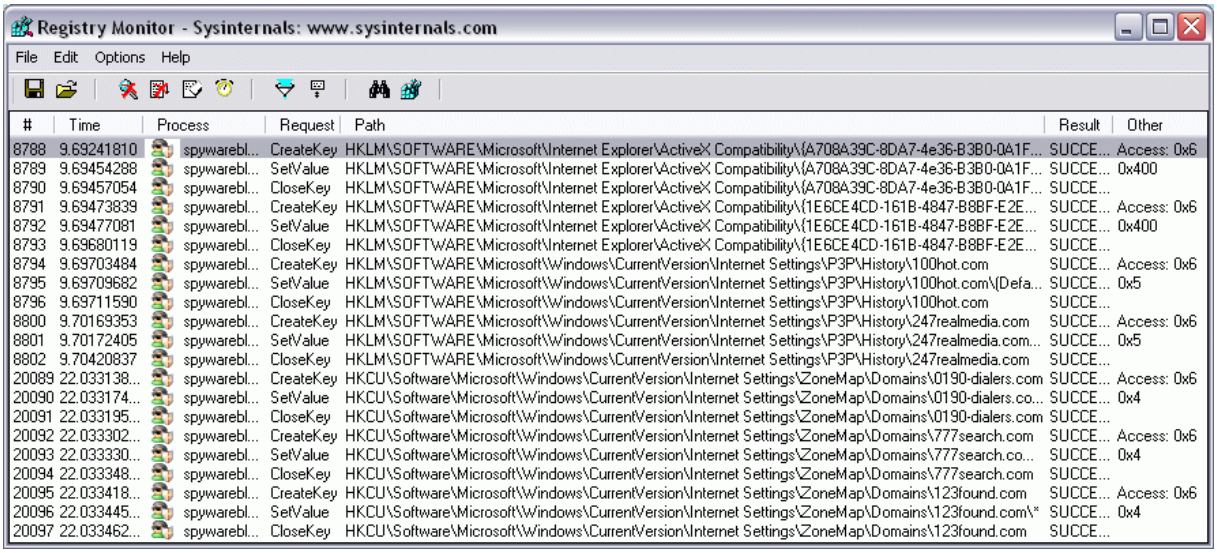


Fig. 25 - *Spyware*Blaster - Accès à la base de registre

Nous remarquons que la technique du *kill bit* (0x400) a été utilisée pour désactiver les ActiveX présents dans la base de données du logiciel (accès #8789, #8792). Ces modifications sont effectuées sous `HKLM` et nécessitent donc des droits administrateur.

Les *cookies* sont, quant à eux, placés dans l'historique de P3P (*Protocol for Privacy Protection*) de la machine et sont refusés (0x5) (accès #8795, #8801). Dans le cas ou l'utilisateur ne possède pas les droits administrateur, les cookies seront placés dans l'historique de l'utilisateur (HKCU). On peut aussi ajouter des sites pour lesquels les *cookies* sont acceptés, il faut pour cela que la valeur (`par défaut`) soit à 0x1.

Dernier point à remarquer dans cette capture, les domaines contenus dans la base de données sont ajoutés dans la base de registre et on leur affecte la zone 4 (accès #20090, #20093, #20096), qui est la zone « Sites sensibles ». Les sites de confiance seraient eux affectés à la zone 2. Les droits administrateur ne sont pas nécessaires pour réaliser ce point puisque les clés ajoutées se trouvent sous HKCU.

Une comparaison de la base de registre avant/après activation des protections disponibles, en mode administrateur et utilisateur, effectuée à l'aide de l'outil ARM, se trouve sur le CD sous `Test SpywareBlaster\admin_modifs_redo.reg` et `Test SpywareBlaster\user_modifs_redo.reg`.

3.1.8 Utilisation d'un agent de protection temps réel

Un agent de protection temps réel permet de maintenir une protection constante contre l'installation ou l'exécution de *malwares* sur la machine.

Il détecte toute tentative d'exécution ou d'écriture de la part d'un logiciel suspect, ainsi que toute tentative de modification d'un des paramètres définis comme protégés, tels les paramètres TCP/IP, le fichier HOSTS ou encore les réglages d'IE.

Il fonctionne en tâche de fond. La méthode de protection utilisée est basée sur les *hooks* systèmes, c'est-à-dire que les messages entrants/sortants du système sont interceptés et analysés par l'agent. Ils pourront par la suite être refusés ou acceptés selon le choix de l'utilisateur. De plus, certaines clés de registre sont régulièrement vérifiées (paramètres IE, association de fichiers, …), de manière à s'assurer qu'elles n'ont pas été modifiées.

Les agents de protection choisis sont ceux disponibles dans les outils présentés sous §4.3.2 et §4.4.2.

3.1.9 Utilisation d'un pare-feu

L'utilisation d'un pare-feu peut être très utile lorsque le *spyware* communique avec son serveur. Il permet de bloquer les communications de et vers le *spyware*.

Sachant que les *spywares* utilisent presque toujours le port 80 (HTTP) pour communiquer avec leurs serveurs, il faudra opter pour un pare-feu applicatif tels Kerio Personal Firewall[8] ou McAfee Personal Firewall Plus[9].

[8] http://www.kerio.com/kpf_home.html
[9] http://download.mcafee.com/fr/

3.1.10 Naviguer de manière plus sûre

Certaines personnes vous diront qu'elles n'ont jamais été infectées par un *spyware* ou autre *malware*. Ceci vient du fait qu'elles prennent les précautions nécessaires pour les éviter.

Ces quelques précautions concernant la navigation sont :

- Ne pas naviguer sur des sites à contenu pornographique ou de jeux
- Ne jamais télécharger à partir d'un site que vous ne connaissez pas. Se renseigner auprès d'autres internautes si nécessaire
- Ne jamais refermer un pop-up en cliquant à l'intérieur de la fenêtre (boutons « OK » ou « Agree »), toujours utiliser Alt-F4 ou la 'X' rouge en haut à droite de la fenêtre. Ou même bloquer les pop-ups
- Ne pas lire le contenu actif des messages électroniques, sauf s'il provient d'une source sûre
- Se méfier des logiciels installés avec les *freewares*
- Lire toutes les alertes de sécurité et les EULAs (*End-User Licence Agreements*) des logiciels installés

Si après toutes ces mesures prises, un *spyware* arrive encore à s'installer sur la machine, il faut procéder à sa suppression à l'aide d'un outil prévu à cet effet.

3.2 Protection matérielle

La mise en place d'une protection logicielle, demande la configuration de toutes les machines à protéger. Dans une entreprise comprenant plusieurs centaines de postes de travail, cette tâche devient très vite longue et encombrante.

On optera alors pour une protection matérielle, ce qui permettra de n'avoir à configurer que l'équipement protecteur lui-même.

Nous allons ici nous concentrer sur la création de règles pour un Blue Coat ProxySG 400, disponible avec le logiciel SGOS 3.2.3.3.

3.2.1 Création de règles pour le Blue Coat ProxySG 400[10]

En prenant comme référence les méthodes de défense mises en œuvre au §3.1 et le document [TBICS], il convient tout d'abord de définir les objectifs à atteindre, afin de créer les règles nécessaires.

Nous allons donc configurer le proxy, de manière à :

- Bloquer les sites de *spywares*
- Bloquer les installations de *spywares*
- Logger toute activité réseau liée aux *spywares*
- Informer les utilisateurs de la présence d'un *spyware* sur leur machine

Les règles seront écrites en langage CPL (*Content Policy Language*), propre à Blue Coat. Les codes CPL présentés ci-après ne sont qu'un échantillon du code complet se trouvant en annexe A6.

Tout d'abord nous allons créer une liste de sites de confiance (*Trusted Sites*), fonctionnant sur le modèle de liste blanche, qui ne seront pas soumis aux règles qui vont suivre. La déclaration des sites se fait comme suit :

```
define url.domain condition trusted_domains
      bluecoat.com
      microsoft.com
      unige.ch
      windowsupdate.com
end

define subnet IP_Interne
      10.1.0.0/16
end

define condition trusted_sites
      condition = trusted_domains
      url.address = IP_Interne
end
```

[10] http://www.bluecoat.com/products/sg400/index.html

Nous définissons donc comme sites de confiance tous ceux contenus dans `trusted_domains`, ainsi que les adresses IP internes.

Puis nous définissons les catégories de site pour lesquels nous ne voulons pas télécharger le contenu actif ou les exécutables. Cette partie est donc basée sur un modèle liste noire. Le code CPL est comme suit :

```
define condition exe_blocks
      category="Nudity"
      category="Adult Content"
      category="Sex"
      category="Non-Traditional Religions and Occult and Folklore"
      category="Proxy Avoidance"
      category="Search Engines and Portals"
      category="Illegal or Questionable"
      category="Tasteless"
      category="Advertisements"
      category="Instant Messaging"
      category="Pay-to-Surf"
      category="Peer-to-Peer File Sharing"
      category="Dynamic Content"
      category="Network Errors"
      category="Uncategorized"
      category="none"
end

define condition active_content_blocks
      condition=exe_blocks
      category="Personal Web Sites"
      category="Hacking"
      category="Mp3 and Audio Download Services"
      category="Gambling"
      category="Games"
      category="Violence"
      category="Drugs"
      category="Militancy and Extremist"
      category="Racism and Hate"
end
```

Les catégories situées dans `exe_blocks` seront interdites de télécharger des fichiers exécutables ainsi que du contenu actif, celles situées dans `active_content_blocks` seront uniquement interdites de télécharger du contenu actif.

3.2.1 Bloquer les sites de *spywares*

Cette partie a pour but de détecter toute communication d'un *spyware* avec son serveur, ainsi que toute tentative d'installation à travers un site *spyware* connu.

Nous utilisons pour cela une base de données répertoriant un grand nombre de sites internet et les classant par catégories. Nous choisissons ici, d'utiliser la base de données Websense[11], qui répertorie plus de 13 millions de sites, divisés en plus de 90 catégories. La liste des catégories se trouve en annexe A5

[11] http://www.websense.com/global/en/ProductsServices/MasterDatabase/

Nous pouvons ensuite définir la condition indiquant qu'un *spyware* communique avec son serveur, comme :

```
define condition phone_home
      category="Security PG"
end
```

Et la règle correspondante :

```
<Proxy Spyware_PhoneHome>
      Condition=phone_home \
      FORCE_DENY("Requête bloquée car spyware $(quot)phoning
home$(quot). Veuillez consulter votre ingénieur système.")
```

Lorsqu'une requête a lieu à partir ou en direction d'un site faisant partie de la catégorie « Security PG », la condition phone_home est vraie et l'action FORCE_DENY est exécutée, ce qui fait que la page internet sera remplacé par le message ci-dessus.

3.2.2 Bloquer les installations de *spywares*

Comme expliqué au §2.2, un des moyens les plus utilisés pour installer des *spywares* sur une machine est l'utilisation de la technologie ActiveX. Il nous faut donc supprimer les « *drive-by installs* », nous allons pour cela interdire le téléchargement de tout composant ActiveX.

Pour cela nous créons 2 conditions, une se basant sur l'extension et l'autre sur le type de contenu :

```
define condition active_content_extensions
      url.extension=cab
      url.extension=ocx
      response.x_header.Content-Disposition = "\.(cab|ocx)($|[^a-z0-
9])"
end

define condition active_content_type
      response.header.Content-Type="application/cab"
      response.header.Content-Type="application/x-compress"
      response.header.Content-Type="application/x-compressed"
      response.header.Content-Type="zz-application/zz-winassoc-cab"
      response.header.Content-Type="application/x-cab-compressed"
      response.header.Content-Type="application/(x-|)java[^s]"
end
```

Et la règle correspondante :

```
<Proxy ActiveContent_Executable_control> condition=!trusted_sites \

      condition=active_content_blocks
      condition=active_content_extensions \
      FORCE_DENY("Requête bloquée car spyware $(quot)Drive-by
Install$(quot) reconnue par active_content_extensions")
      condition=active_content_type \
      FORCE_DENY("Requête bloquée car spyware $(quot)Drive-by
Install$(quot) reconnue par active_content_type")
```

Cette règle nous dit que toute réponse provenant d'un site ne se trouvant pas dans la liste de confiance et étant interdit de télécharger du contenu actif est refusée si :

- L'extension du fichier est définie dans `active_content_extensions`
- Le type de fichier est défini dans `active_content_type`

3.2.3 Logger toute activité réseau liée aux *spywares*

Tout trafic anormal sur le réseau doit être *loggé*, de manière à permettre à l'ingénieur système de repérer quels sont les machines infectées et ainsi procéder à la désinfection (§4).

Nous allons donc *logger* tout trafic concernant les *spywares* , nous créons pour cela 4 *logs* nommés :

- `Drive_by_install_denied` : contenant toutes les occurrences de tentative d'installation de *spywares* par la méthode « *drive-by install* »
- `Executable_file_denied` : contenant toutes les occurrences pour lesquelles le téléchargement d'un exécutable a été refusé
- `Phone_home_detected` : contenant les occurrences détectées lors du contact d'un *spyware* avec son serveur
- `Risky_tags_striped` : contenant les balises dangereuses supprimées

La création des *logs* ne peut se faire par code CPL, elle doit donc être effectuée avant de programmer les règles sur le proxy, à travers l'interface web, sous `Configuration -> Access logging -> Logs`.

L'ajout d'un élément dans un *log* se fera en insérant l'appel du *log* en tant qu'action voulue à l'endroit désiré. Reprenons la règle définie en §3.2.1 pour illustrer ceci :

```
<Proxy Spyware_PhoneHome>
      Condition = phone_home \
      FORCE_DENY("Requête bloquée car spyware $(quot)phoning
home$(quot). Veuillez consulter votre ingénieur système.")\
      access_log(phone_home_detected)
```

Lorsqu'une communication entre un *spyware* et son serveur a lieu, le message de refus s'affiche et une nouvelle entrée est crée dans le *log* phone_home_detected.

Les *logs* peuvent ensuite être téléchargés périodiquement sur un serveur ftp, de manière à pouvoir les consulter par la suite.

3.2.4 Informer les utilisateurs

Une fois le trafic *spyware* détecté il peut être intéressant d'alerter l'utilisateur, pour qu'il puisse remettre sa machine en état ou pour qu'il demande à l'ingénieur système de le faire. Lors d'un refus, le message s'affichera sur la fenêtre courante, si le trafic n'est pas visible à l'écran, l'utilisation d'une nouvelle fenêtre graphique affichant un message est la meilleure solution.

L'affichage de cette fenêtre se fait en effectuant l'appel suivant :

```
action.user_alert(yes)
```

Cette action est utilisée dans la règle *Spyware*_PhoneHome codée dans le code complet en annexe A6.

3.2.5 Installation des règles sur le proxy

Une fois le code CPL terminé, il faut l'insérer dans le proxy. Pour cela nous utiliserons l'interface web qui se présente comme suit :

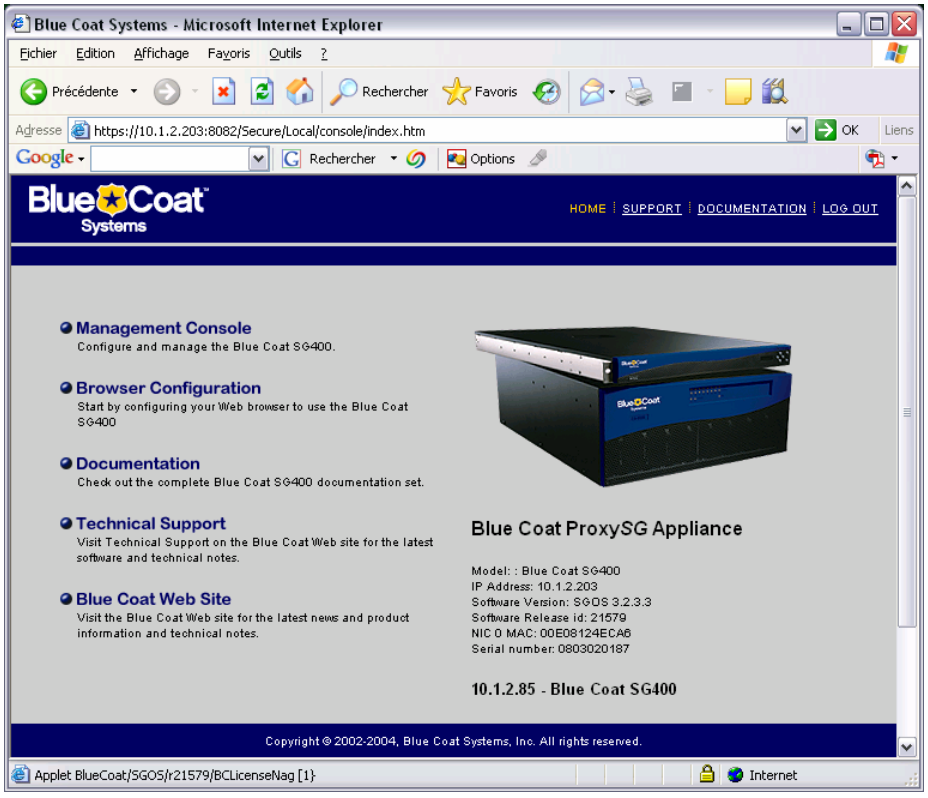


Fig. 26 - Blue Coat - Page d'accueil

En cliquant sur « Management Console », nous arrivons sur la page de configuration du proxy. Sur cette page cliquer sur « Policy », puis sur « Policy Files ».

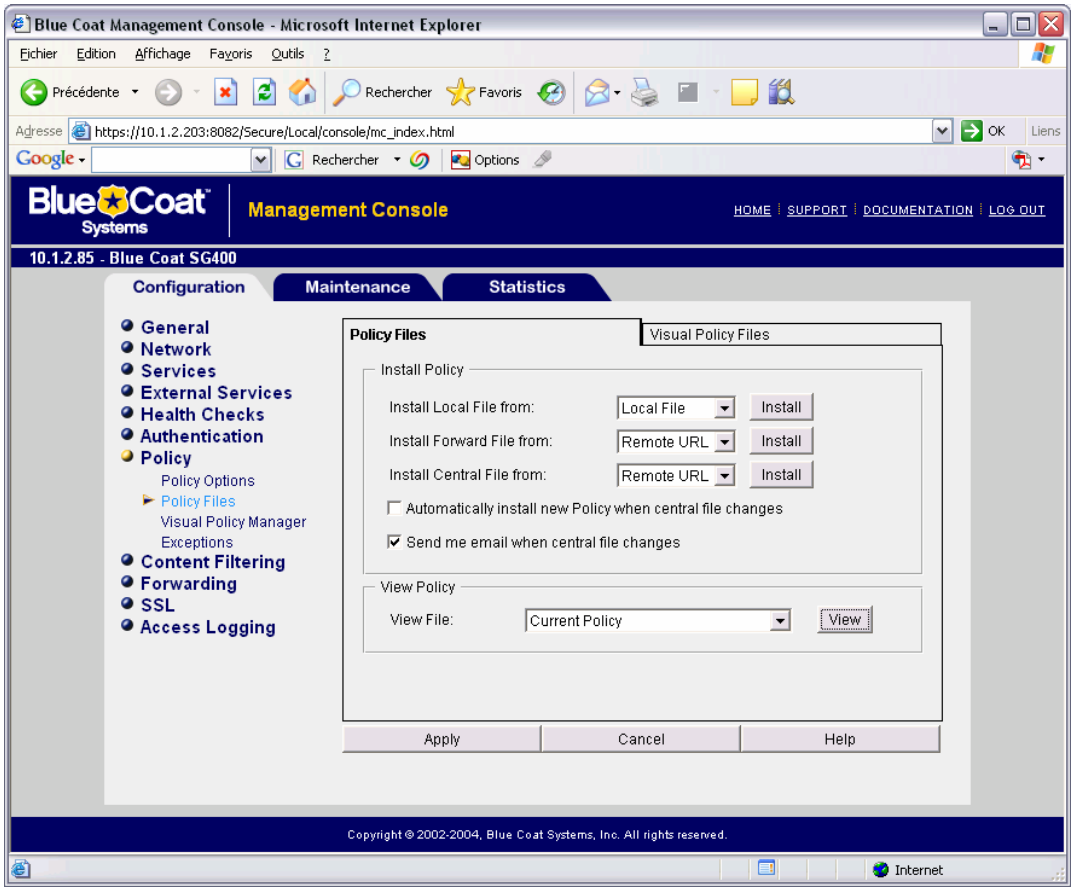


Fig. 27 - Blue Coat - Insertion du code CPL

Sur cette fenêtre, choisir « Local File » dans « Install Local File From : » et cliquer sur « Install ». Naviguer ensuite jusqu'au fichier contenant le code et l'ajouter. Une fenêtre s'affichera alors indiquant comment c'est passé l'insertion du code dans le proxy (*errors, warnings*, …).

Les règles en utilisation peuvent être consultées en cliquant sur « View ». L'utilisateur peut toujours ajouter de nouvelles règles, soit en éditant le code CPL, soit en utilisant le « Visual Policy Manager ».

Il suffit ensuite d'insérer le proxy entre les machines à protéger et la connexion internet ou de rediriger le trafic réseau vers le proxy sous `Propriétés de Internet -> Connexions -> Paramètres réseau`, et en configurant l'adresse et le port du serveur proxy

4 Détection / suppression de *spywares*

10 jours d'étude

Pour procéder au test des différents logiciels de suppression de *spywares*, une machine a été infectée avec plusieurs *spywares*, dont CoolWebSearch, BonziBuddy, ISTBar ou encore Ezula. Nous essayerons ensuite de la désinfecter avec les outils proposés.

Toutes les analyses se feront en mode sans échec de manière à n'avoir aucun processus *spyware* qui soit lancé et ainsi faciliter la suppression.

De plus le mode administrateur est recommandé, pour permettre la suppression de toutes les clés de registres et de tous les fichiers. En mode utilisateur, certains *spywares* (presque tous) ne sont pas supprimés correctement car l'accès à certaines clés de la base de registre est interdit (`HKLM`).

Une démonstration du manque d'efficacité lors de l'utilisation en mode utilisateur se trouve sur le CD sous `Tests infection\02 - machine infectée à fond\05 - Spybot - Search&Destroy\en_user.gif`.

Il faudra cependant veiller à effectuer les mises à jour des signatures des *spywares* en mode normal, de manière à avoir accès à internet.

Le système infecté se présente comme suit :

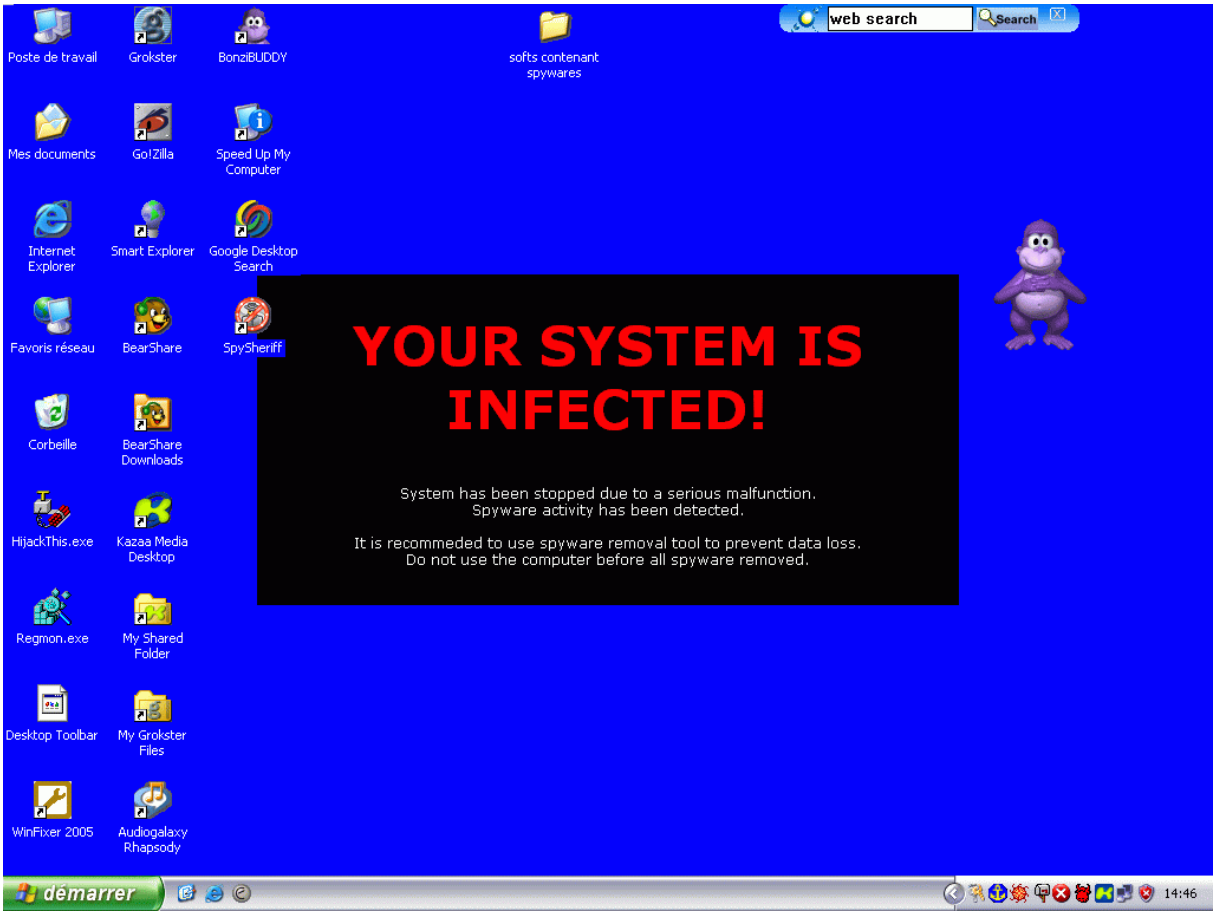


Fig. 28 - Système infecté

Certains utilisateurs auront déjà remarqué la présence de BonziBuddy, qui est un *spyware* très connu et caractérisé par la présence d'un singe à l'écran.

4.1 Analyse orientée forensique

L'analyse forensique permet de détecter les *malwares* installés sur la machine, sans l'utilisation d'outils spécialisés dans la suppression de *spywares* présentés à partir du §4.2. Cette analyse se fera en mode normal, de manière à détecter les processus des *malwares* qui sont lancés, et avec les droits administrateur, de manière à avoir accès à toutes les fonctionnalités de l'outil HijackThis.

La recherche dans la base de registre est la principale forme utilisée ici. Pour cela, nous utilisons le logiciel ARM mentionné en annexe A3.4.

Cette analyse du registre pourrait très bien se faire sans sauvegarde avant infection, c'est d'ailleurs ce qui arrive normalement. Cependant, dans le but de diminuer le nombre de valeurs à vérifier, nous procéderons à la comparaison des 2 sauvegardes et n'aurons ainsi qu'à analyser les valeurs ajoutées par les processus d'installation des *spywares*.

Nous comparons donc la base de registre infectée à la référence et analysons les différences.

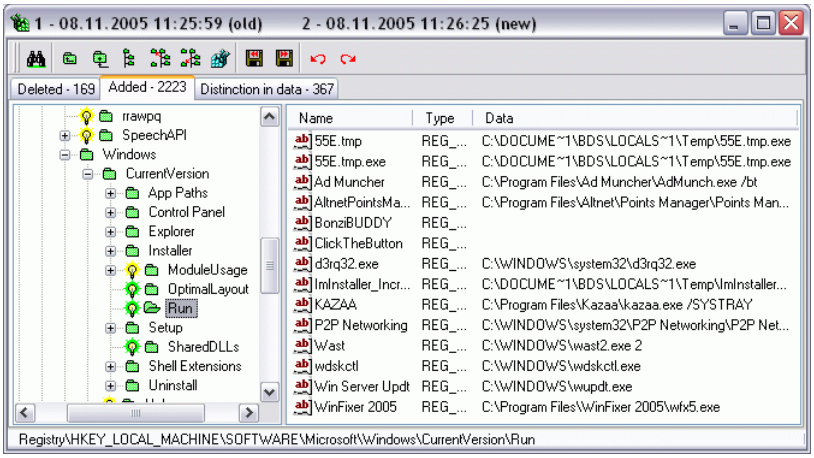


Fig. 29 - Modifications dans `HKLM\SOFTWARE\Microsoft\Windows\...\Run`

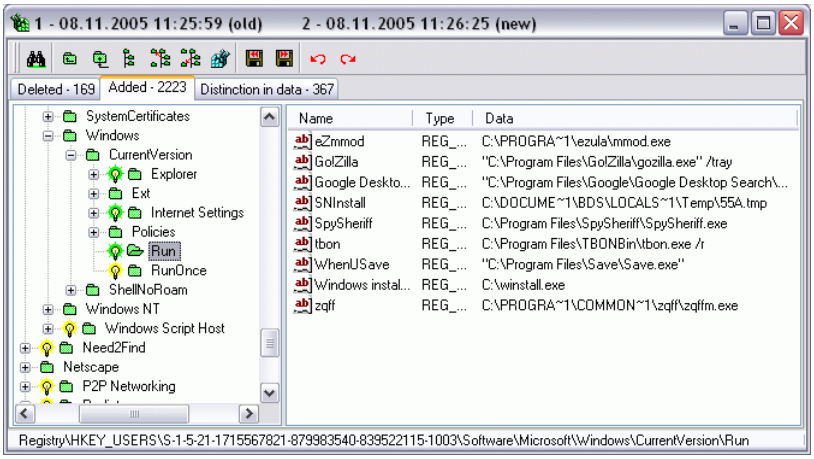


Fig. 30 - Modifications dans `HKCU\{Id_Administrateur}\Software\Microsoft\Windows\...\Run`

Les différentes valeurs sont comparées aux bases de référence [CASTLE] et [PROCLIB].

Valeurs ajoutées dans les clés Run	Exécutable	Catégorie	Nom de la menace	Statut
55E.tmp	55E.tmp.exe	*Malware*	SpySheriff / *Spyware*No	Indésirable
55E.tmp.exe	55E.tmp.exe	*Malware*	SpySheriff / *Spyware*No	Indésirable
Ad Muncher	AdMunch.exe	*Pop-up blocker*	-	Utile
AltnetPointsManager	Points Manager.exe	*Adware*	Altnet	Indésirable
BonziBUDDY	Inconnu	*Spyware*	BonziBuddy	Indésirable
ClickTheButton	Inconnu	*Adware*	BonziBuddy	Indésirable
d3rq32.exe	d3rq32.exe	Inconnue	Trojan.Agent.bi	Indésirable
ImInstaller_IncrediMail	incredimail_install .exe	*Email program / adware*	IncrediMail	Selon choix utilisateur / indésirable
KAZAA	kazaa.exe	*adware / foistware*	Kazaa	Selon choix utilisateur / indésirable
P2P Networking	P2P Networking.exe	*P2P program / adware*	Kazaa	Selon choix utilisateur / indésirable
Wast	wast2.exe	*Adware*	Grokster	Indésirable
wdskctl	wdskctl.exe	*Adware*	IEPlugin	Indésirable
Win Server Updt	wupdt.exe	*Adware*	IEPlugin	Indésirable
WinFixer 2005	wfx5.exe	*Foistware*	WinFixer	Indésirable
eZmmod	mmod.exe	*Adware*	eZula	Indésirable
Go!Zilla	gozilla.exe	*Adware*	Go!Zilla	Selon choix utilisateur / indésirable
Google Desktop Search	GoogleDesktop.exe	*Search application*	-	Utile
SNInstall	55A.tmp	*Malware*	SpySheriff / *Spyware*No	Indésirable
SpySheriff	SpySheriff.exe	*Malware*	SpySheriff / *Spyware*No	Indésirable
tbon	tbon.exe	*Adware*	BestOffers	Indésirable
WhenUSave	Save.exe	*Adware*	WhenU	Indésirable
Windows installer	winstall.exe	*Malware*	SpySheriff / *Spyware*No	Indésirable
zqff	zqffm.exe	Inconnu	CoolWebSearch	Indésirable

Fig. 31 - Valeurs ajoutées dans les clés Run du registre

Après analyse des clés Run du registre, nous détectons 15 menaces installées sur la machine. Il nous reste maintenant à détecter les *malwares* qui ne se lancent pas au démarrage.

L'outil HijackThis devrait nous apporter quelques éléments de plus.

```
Logfile of HijackThis v1.99.1
Scan saved at 14:15:01, on 09.11.2005
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)

Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\WINDOWS\system32\mstz32.exe
C:\WINDOWS\Explorer.EXE
C:\Program Files\VMware\VMware Tools\VMwareService.exe
C:\Program Files\VMware\VMware Tools\VMwareTray.exe
C:\Program Files\VMware\VMware Tools\VMwareUser.exe
C:\WINDOWS\wdskctl.exe
C:\Program Files\WinFixer 2005\wfx5.exe
C:\Program Files\Ad Muncher\AdMunch.exe
C:\WINDOWS\system32\P2P Networking\P2P Networking.exe
C:\Program Files\Altnet\Points Manager\Points Manager.exe
C:\WINDOWS\system32\wscntfy.exe
C:\PROGRA~1\Altnet\DOWNLO~1\asm.exe
C:\WINDOWS\system32\d3rq32.exe
C:\DOCUME~1\BDS\LOCALS~1\Temp\55E.tmp.exe
C:\PROGRA~1\COMMON~1\zqff\zqffm.exe
C:\PROGRA~1\ezula\mmod.exe
C:\Program Files\Save\Save.exe
C:\Program Files\TBONBin\tbon.exe
C:\Program Files\Google\Google Desktop Search\GoogleDesktop.exe
C:\winstall.exe
C:\Program Files\SpySheriff\SpySheriff.exe
C:\Program Files\GetRight\getright.exe
C:\Program Files\Go!Zilla\gozilla.exe
C:\Program Files\BonziBUDDY\BonziBDY.EXE
C:\Program Files\MailAlert\MailAlert.exe
C:\Program Files\GetRight\getright.exe
C:\WINDOWS\msagent\AgentSvr.exe
C:\PROGRA~1\COMMON~1\zqff\zqffa.exe
C:\WINDOWS\system32\wuauclt.exe
C:\Program Files\Google\Google Desktop Search\GoogleDesktopIndex.exe
C:\Program Files\Google\Google Desktop Search\GoogleDesktopCrawl.exe
C:\PROGRA~1\COMMON~1\zqff\zqffl.exe
C:\Documents and Settings\BDS\Bureau\HijackThis.exe
C:\WINDOWS\system32\wpabaln.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =
http://if.searchcentrix.com/sidecat.jsp?p=98567&appid=21&id=10361010121
34
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =
res://C:\WINDOWS\system32\iiytk.dll/sp.html#28129
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
about:blank
```

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = res://C:\WINDOWS\system32\iiytk.dll/sp.html#28129
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar = res://C:\WINDOWS\system32\iiytk.dll/sp.html#28129
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = res://C:\WINDOWS\system32\iiytk.dll/sp.html#28129
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant = http://if.searchcentrix.com/sidecat.jsp?p=98567&appid=21&id=1036101012134
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch = http://search.ieplugin.com/search.htm
R1 - HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) = http://search.ieplugin.com/q.cgi?q=%s
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName = Liens
R3 - Default URLSearchHook is missing
O2 - BHO: Class - {2ABA8EC8-43E6-7C24-9568-068569082C70} - C:\WINDOWS\system32\javafk.dll
O2 - BHO: bho2gr Class - {31FF080D-12A3-439A-A2EF-4BA95A3148E8} - C:\Program Files\GetRight\xx2gr.dll
O2 - BHO: Need2Find Bar BHO - {4D1C4E81-A32A-416b-BCDB-33B3EF3617D3} - C:\Program Files\Need2Find\bar\1.bin\ND2FNBAR.DLL
O2 - BHO: InstaFinderK - {4E7BD74F-2B8D-469E-90F0-F66AB581A933} - C:\PROGRA~1\INSTAF~1\INSTAF~1.DLL
O2 - BHO: GSIM - {4E7BD74F-2B8D-469E-DFF7-EC6BF4D5FA7D} - C:\WINDOWS\gsim.dll
O2 - BHO: RXResultTracker Class - {59879FA4-4790-461c-A1CC-4EC4DE4CA483} - C:\PROGRA~1\RXTOOL~1\sfcont.dll
O2 - BHO: Intelligent Explorer - {69135BDE-5FDC-4B61-98AA-82AD2091BCCC} - C:\WINDOWS\systb.dll
O2 - BHO: Class - {8A371204-086A-4507-80FF-D00747F0E100} - C:\WINDOWS\ipxy.dll
O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} - c:\program files\google\googletoolbar2.dll
O2 - BHO: IEHlprObj Class - {CD4C3CF0-4B15-11D1-ABED-709549C10000} - C:\Program Files\Go!Zilla\GoIEHlp.dll
O3 - Toolbar: Intelligent Explorer - {69135BDE-5FDC-4B61-98AA-82AD2091BCCC} - C:\WINDOWS\systb.dll
O3 - Toolbar: RX Toolbar - {25D8BACF-3DE2-4B48-AE22-D659B8D835B0} - C:\Program Files\RXToolBar\RXToolBar.dll
O3 - Toolbar: &Google - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - c:\program files\google\googletoolbar2.dll
O4 - HKLM\..\Run: [VMware Tools] C:\Program Files\VMware\VMware Tools\VMwareTray.exe
O4 - HKLM\..\Run: [VMware User Process] C:\Program Files\VMware\VMware Tools\VMwareUser.exe
O4 - HKLM\..\Run: [Win Server Updt] C:\WINDOWS\wupdt.exe
O4 - HKLM\..\Run: [winsync] C:\WINDOWS\system32\sspk4l.exe reg_run
O4 - HKLM\..\Run: [wdskctl] C:\WINDOWS\wdskctl.exe
O4 - HKLM\..\Run: [WinFixer 2005] C:\Program Files\WinFixer 2005\wfx5.exe
O4 - HKLM\..\Run: [Ad Muncher] C:\Program Files\Ad Muncher\AdMunch.exe /bt
O4 - HKLM\..\Run: [P2P Networking] C:\WINDOWS\system32\P2P Networking\P2P Networking.exe /AUTOSTART
O4 - HKLM\..\Run: [KAZAA] C:\Program Files\Kazaa\kazaa.exe /SYSTRAY
O4 - HKLM\..\Run: [AltnetPointsManager] C:\Program Files\Altnet\Points Manager\Points Manager.exe -s
O4 - HKLM\..\Run: [Wast] C:\WINDOWS\wast2.exe 2

O4 - HKLM\..\Run: [ImInstaller_IncrediMail]
C:\DOCUME~1\BDS\LOCALS~1\Temp\ImInstaller\IncrediMail\incredimail_insta
ll.exe -startup -product IncrediMail
O4 - HKLM\..\Run: [d3rq32.exe] C:\WINDOWS\system32\d3rq32.exe
O4 - HKLM\..\Run: [55E.tmp] C:\DOCUME~1\BDS\LOCALS~1\Temp\55E.tmp.exe
O4 - HKLM\..\Run: [55E.tmp.exe]
C:\DOCUME~1\BDS\LOCALS~1\Temp\55E.tmp.exe
O4 - HKCU\..\Run: [zqff] C:\PROGRA~1\COMMON~1\zqff\zqffm.exe
O4 - HKCU\..\Run: [eZmmod] C:\PROGRA~1\ezula\mmod.exe
O4 - HKCU\..\Run: [WhenUSave] "C:\Program Files\Save\Save.exe"
O4 - HKCU\..\Run: [tbon] C:\Program Files\TBONBin\tbon.exe /r
O4 - HKCU\..\Run: [Google Desktop Search] "C:\Program
Files\Google\Google Desktop Search\GoogleDesktop.exe" /startup
O4 - HKCU\..\Run: [Go!Zilla] "C:\Program Files\Go!Zilla\gozilla.exe"
/tray
O4 - HKCU\..\Run: [Windows installer] C:\winstall.exe
O4 - HKCU\..\Run: [SNInstall] C:\DOCUME~1\BDS\LOCALS~1\Temp\55A.tmp
O4 - HKCU\..\Run: [SpySheriff] C:\Program
Files\SpySheriff\SpySheriff.exe
O4 - Startup: BonziBUDDY.lnk = C:\Program Files\BonziBUDDY\BonziBDY.EXE
O4 - Startup: MailAlert.lnk = C:\Program Files\MailAlert\MailAlert.exe
O4 - Global Startup: AnchorNet Agent.lnk = C:\Program
Files\AnchorNet\anchor.exe
O4 - Global Startup: GetRight - Tray Icon.lnk = C:\Program
Files\GetRight\getright.exe
O4 - Global Startup: Go!Zilla.lnk = C:\Program
Files\Go!Zilla\gozilla.exe
O8 - Extra context menu item: &Google Search - res://c:\program
files\google\GoogleToolbar2.dll/cmsearch.html
O8 - Extra context menu item: &Search -
http://ko.bar.need2find.com/KO/menusearch.html?p=KO
O8 - Extra context menu item: &Translate English Word -
res://c:\program files\google\GoogleToolbar2.dll/cmwordtrans.html
O8 - Extra context menu item: Backward Links - res://c:\program
files\google\GoogleToolbar2.dll/cmbacklinks.html
O8 - Extra context menu item: Cached Snapshot of Page -
res://c:\program files\google\GoogleToolbar2.dll/cmcache.html
O8 - Extra context menu item: Download with GetRight - C:\Program
Files\GetRight\GRdownload.htm
O8 - Extra context menu item: Download with Go!Zilla -
file://C:\Program Files\Go!Zilla\download-with-gozilla.html
O8 - Extra context menu item: Open with GetRight Browser - C:\Program
Files\GetRight\GRbrowse.htm
O8 - Extra context menu item: Similar Pages - res://c:\program
files\google\GoogleToolbar2.dll/cmsimilar.html
O8 - Extra context menu item: Translate Page into English -
res://c:\program files\google\GoogleToolbar2.dll/cmtrans.html
O9 - Extra button: (no name) - {9E248641-0E24-4DDB-9A1F-705087832AD6} -
C:\WINDOWS\system32\wuauclt.dll
O9 - Extra 'Tools' menuitem: Java - {9E248641-0E24-4DDB-9A1F-
705087832AD6} - C:\WINDOWS\system32\wuauclt.dll
O9 - Extra button: (no name) - {A80F2DB2-80A9-4834-8F5A-4AB70F4EF4C3} -
C:\WINDOWS\systb.dll
O9 - Extra 'Tools' menuitem: IMI - {A80F2DB2-80A9-4834-8F5A-
4AB70F4EF4C3} - C:\WINDOWS\systb.dll
O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} -
C:\Program Files\Messenger\msmsgs.exe
O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-
BB9E-00C04F795683} - C:\Program Files\Messenger\msmsgs.exe
O16 - DPF: {1D6711C8-7154-40BB-8380-3DEA45B69CBF} (Web P2P Installer) -

```
O16 - DPF: {42F2C9BA-614F-47C0-B3E3-ECFD34EED658} (Installer Class) -
http://www.ysbweb.com/ist/softwares/v4.0/ysb_regular.cab
O16 - DPF: {4E7BD74F-2B8D-469E-DFF7-EC6BF4D5FA7D} (GSIM) -
http://config.grandstreetinteractive.com/toolbar/test/gsim.cab
O16 - DPF: {666E4D35-E955-11D0-A707-000000521958} -
http://www.ieplugin.com/webplugin.cab
O16 - DPF: {7C559105-9ECF-42B8-B3F7-832E75EDD959} (Installer Class) -
http://www.tbcode.com/ist/softwares/v4.0/0006_cracks.cab
O17 - HKLM\System\CCS\Services\Tcpip\..\{D5967F0E-E436-49D2-8335-
7F59DA95F3CE}: NameServer = 10.1.1.10
O20 - Winlogon Notify: style32 - C:\WINDOWS\
O23 - Service: Network Security Service (NSS) ( 11Fßä #·ºÄÖ`I) -
Unknown owner - C:\WINDOWS\system32\mstz32.exe
O23 - Service: Remote Packet Capture Protocol v.0 (experimental)
(rpcapd) - Unknown owner - %ProgramFiles%\WinPcap\rpcapd.exe" -d -f
"%ProgramFiles%\WinPcap\rpcapd.ini (file missing)
O23 - Service: VMware Tools Service (VMTools) - VMware, Inc. -
C:\Program Files\VMware\VMware Tools\VMwareService.exe
```

Fig. 32 - Log HijackThis après infection complète

Nous procédons à l'analyse de chaque ligne du log, à l'aide de [HIJACK], [CASTLE], [PROCLIB] ou de Process Explorer. Les lignes qui nous intéressent sont en **gras**, les autres étant soit utilisées par le système d'exploitation, soit légitimes.

Regardons tout d'abord les processus en cours :

- **C:\WINDOWS\system32\mstz32.exe**. D'après les recherches effectuées sur Google, ce processus semble être le **trojan TrojanDownloader.Agent.bq**
- **C:\WINDOWS\wdskctl.exe**, a déjà été défini auparavant comme l'***adware*** **IEPlugin**
- **C:\Program Files\WinFixer 2005\wfx5.exe**, est le ***foistware*** **WinFixer**
- **C:\WINDOWS\system32\P2P Networking\P2P Networking.exe**, voir Fig. 31
- **C:\Program Files\Altnet\Points Manager\Points Manager.exe,** voir Fig. 31
- **C:\PROGRA~1\Altnet\DOWNLO~1\asm.exe**, est l'***adware*** **Altnet**
- **C:\WINDOWS\system32\d3rq32.exe**, correspond au **trojan Trojan.Agent.bi**
- **C:\DOCUME~1\BDS\LOCALS~1\Temp\55E.tmp.exe**, voir Fig. 31
- **C:\PROGRA~1\COMMON~1\zqff\zqffm.exe**, voir Fig. 31
- **C:\PROGRA~1\ezula\mmod.exe**, voir Fig. 31
- **C:\Program Files\Save\Save.exe**, voir Fig. 31
- **C:\Program Files\TBONBin\tbon.exe**, voir Fig. 31
- **C:\winstall.exe**, voir Fig. 31
- **C:\Program Files\SpySheriff\SpySheriff.exe**, voir Fig. 31

- **C:\Program Files\GetRight\getright.exe**, est un gestionnaire de téléchargements, la version gratuite est aussi un ***spyware***

- **C:\Program Files\Go!Zilla\gozilla.exe**, voir Fig. 31

- **C:\Program Files\BonziBUDDY\BonziBDY.EXE** est le ***spyware*** **BonziBuddy**

- **C:\Program Files\MailAlert\MailAlert.exe** n'est pas reconnu comme un *spyware*, cependant il n'est pas nécessaire au fonctionnement correct de la machine

- **C:\PROGRA~1\COMMON~1\zqff\zqffa.exe** et **zqffl.exe** sont lancés par **zqffm.exe** (voir Fig. 31) et ne sont connus de personne car ils possèdent un nom aléatoire. Ils sont donc une **menace**

Regardons maintenant les paramètres spécifiques à HijackThis :

- **R0, R1** : Les pages de recherche de IE ont été déviées par l'***adware*** **SearchCentrix** et **IEPlugin**

- **O2** : quelques BHOs ont été ajoutés par l'***adware*** **CoolWebSearch, GetRight, Need2Find/MySearch, l'*adware* InstaFinder, l'*hijacker* GrandStreet/SearchCentrix, l'*adware* RXToolbar, l'*adware* IEPlugin et Go!Zilla**

- **O3** : ainsi que quelques barres d'outils installées par les ***adwares*** **IEPlugin et RXToolbar**

- **O4** : **BonziBuddy**, **MailAlert, le *spyware* AnchorNet, GetRight et Go!Zilla** sont situés dans le dossier « Démarrage ». Pour les autres c.f. Fig. 31

- **O8** : éléments ajoutés au menu contextuel par **Need2Find/MySearch, GetRight et Go!Zilla**

- **O9** : ainsi que quelques boutons et menus supplémentaires à la barre principale d'IE par l'***adware*** **IEPlugin**

- **O16** : les contrôles ActiveX téléchargés ayant permis l'installation de certains *spywares* se trouvent à ce point

- **O23** : le **trojan TrojanDownloader.Agent.bq** a ajouté un service et démarre donc au démarrage de la machine en tant que tel

L'analyse de ce log nous a permis de détecter quelques *malwares* de plus, nous arrivons à un décompte de 22 familles de menaces réelles réparties comme suit :

- Altnet
- AnchorNet
- BestOffers
- BonziBuddy
- CoolWebSearch
- eZula
- Getright
- Go!Zilla
- Grokster
- IEPlugin
- IncrediMail
- InstaFinder
- Kazaa
- MailAlert
- Need2Find/MySearch
- RXToolbar
- WhenU
- SearchCentrix
- SpySheriff / *Spyware*No
- Trojan.Agent.bi
- TrojanDownloader.Agent.bq.
- WinFixer

Certaines de ces menaces peuvent être supprimées en utilisant l'utilitaire Ajout/Suppression de programmes de Windows, d'autres par contre nécessiterons une suppression manuelle ayant recours à des sites spécialisés et à des forums tels [SPYWAR] ou [SPYREM].

4.2 Lavasoft Ad-Aware SE Personal Edition 1.06r1[12]

Lavasoft est une des premières compagnies à avoir mis au point un logiciel de combat contre les *spywares*. De plus, de part sa gratuité, Ad-Aware est très fortement implanté en tant que logiciel anti*spywares*. Ce qui oblige presque à tester son efficacité.

Il existe plusieurs versions de ce logiciel, presque toutes payantes. Nous avons choisi de tester la version libre, disponible sur le site Download.com[13]. Certaines fonctionnalités de seront pas disponibles.

Une fois l'installation terminée, il suffit de lancer le raccourci pointant sur l'exécutable. Au prime abord, l'interface de Ad-Aware paraît très instinctive, ce qui simplifie l'utilisation.

Fig. 33 - Ad-Aware - Écran d'accueil

La première chose à faire est de procéder à la mise à jour des signatures. Il suffit, pour cela, de cliquer sur « Status » puis sur « Check for updates now » et finalement sur « Connect » sur la fenêtre qui s'ouvre.

[12] http://www.lavasoft.com/
[13] http://www.download.com/Ad-Aware-SE-Personal-Edition/3000-8022_4-10399602.html?tag=lst-0-2

4.2.1 Suppression à posteriori

Une fois la mise à jour terminée, nous pouvons procéder à l'analyse des fichiers. Cliquons pour cela sur « Scan now », choisissons « Perform full system scan », de manière à effectuer une analyse complète du système (y compris les fichiers archives), et activons les 2 options en bas de la fenêtre (permettant de détecter les risques de niveau bas). Un click sur « Next » lancera alors l'analyse.

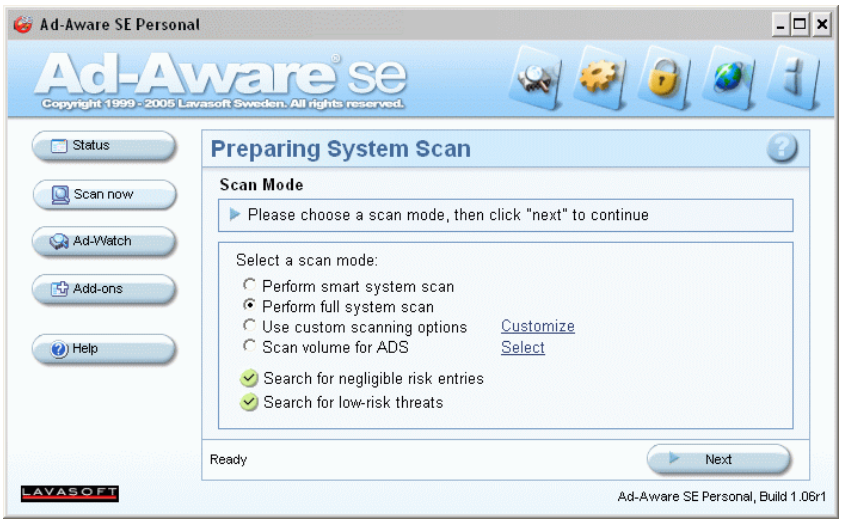


Fig. 34 - Ad-Aware - Réglages d'analyse

Une fois l'analyse terminée, un résumé s'affiche, indiquant le nombre d'objets critiques trouvés. Ainsi que les processus, les modules, les clés et les valeurs de registre, les fichiers et les dossiers identifiés.

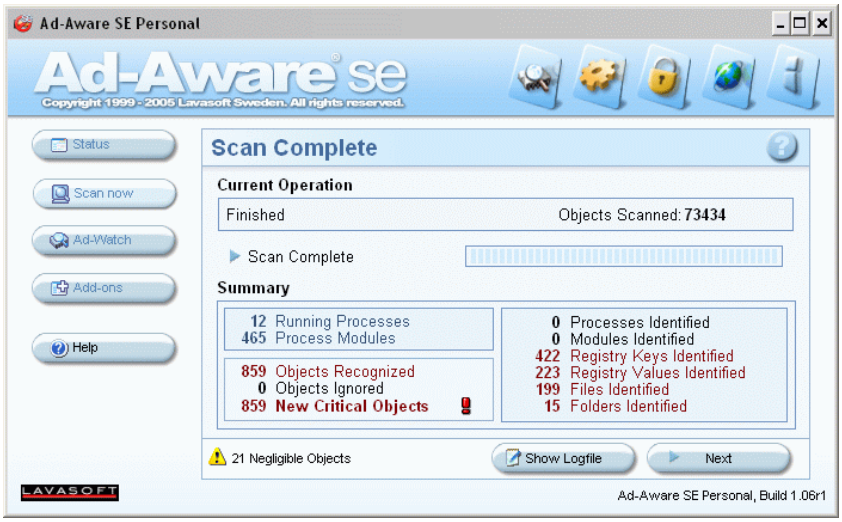


Fig. 35 - Ad-Aware - Résumé de la 1ère analyse

En cliquant sur « Next », le détail de l'analyse s'affiche. Nous pouvons alors sélectionner les éléments à supprimer.

Fig. 36 - Ad-Aware - Détails de la 1ère analyse

Nous voyons ici, que 23 familles de *spywares* ont été détectées. La liste complète se trouve sur le CD sous `Tests infection\02 - machine infectée à fond\03 - Ad-Aware\2c_log1_ad-aware.TXT`.

Nous sélectionnons les familles à supprimer (toutes excepté *MRU List*) et cliquons sur « Next ». Les *MRU List* (*Most Recently Used List*) sont des objets contenant la liste des derniers fichiers, clés de registre ou applications utilisées, ils ne sont pas dangereux et n'ont donc pas besoin d'être effacés.

Le logiciel procède alors à la suppression des éléments sélectionnés.

Logiquement, si la suppression a été faite correctement, Ad-Aware ne devrait plus détecter de *spywares* sur la même machine. Nous décidons alors de redémarrer la machine et de procéder à une nouvelle analyse, toujours en mode sans échec.

Fig. 37 - Ad-Aware - Détails de la 2ème analyse

À notre grande surprise, quelques objets appartement aux familles des *spywares* détectées auparavant sont toujours là. Cependant, nous constatons qu'il n'y a plus que 9 *spywares* présents sur la machine.

Nous décidons alors de supprimer les objets critiques et de procéder à une nouvelle analyse, après redémarrage.

Cette fois-ci aucun *spyware* n'est détecté par Ad-Aware.

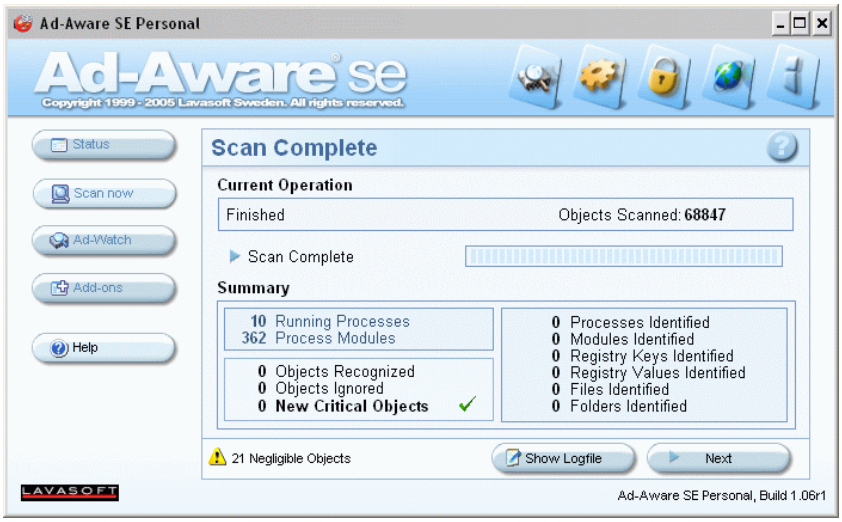


Fig. 38 - Ad-Aware - Détails de la 3ème analyse

Lorsqu'une nouvelle session est ouverte en mode normal. Certains logiciels nous indiquent qu'un module indispensable à leur fonctionnement a été supprimé. Il convient, dans ce cas, de désinstaller complètement l'application et d'opter pour une version payante ou pour un autre logiciel ayant les mêmes fonctionnalités.

De plus, quelques logiciels ayant installé les *spywares* sont toujours sur la machine. Il se peut alors que ces derniers aient, à nouveau, été installés.

Une nouvelle analyse, en mode sans échec permet de confirmer ceci.

Fig. 39 - Ad-Aware – Détails de la 4ème analyse

Nous en déduisons que les *spywares* ont de nouveau été installés, car les logiciels responsables de leur mise en route se sont lancés au démarrage. C'est un gros défaut de Ad-Aware, il ne supprime pas complètement certaines menaces détectées et permet donc qu'elles soient réinstallées lors du redémarrage.

4.2.2 Agent temps réel

L'agent temps réel disponible avec Ad-Aware n'est disponible que sur la version payante et n'a donc pas été étudié.

4.3 Microsoft Anti*Spyware* Beta 1 v1.0.615[14]

Due à l'augmentation considérable des *spywares* ces dernières années, Microsoft a jugé important de développer un logiciel anti*spyware* (ou plutôt de racheter un logiciel à l'éditeur Giant[15]). Ce logiciel est encore en version beta, cependant selon ZDNet[16], Microsoft a annoncé qu'il demeurera gratuit même lors de sa publication officielle.

L'interface d'Anti*Spyware* se présente comme suit, comme Ad-Aware, un résumé est affiché lors du lancement de l'application.

Fig. 40 - Microsoft Anti*Spyware* - Écran d'accueil

Il faut ensuite procéder à la mise à jour de la base de données des signatures, en cliquant sur « File », puis sur « Check for updates… ». La base de données de ce logiciel répertorie, en ce moment, plus de 100'000 menaces.

[14] http://www.microsoft.com/athome/security/*spyware*/software/default.mspx
[15] http://www.giantcompany.com/default.htm
[16] http://www.zdnet.fr/actualites/internet/0,39020774,39206950,00.htm

4.3.1 Suppression à posteriori

Une fois cette opération effectuée, nous allons procéder à une analyse complète du système. Pour cela, cliquons sur « Scan options », puis sélectionnons « Run a full system scan » et sélectionner tous les éléments. Enfin cliquons sur « Run Scan Now ».

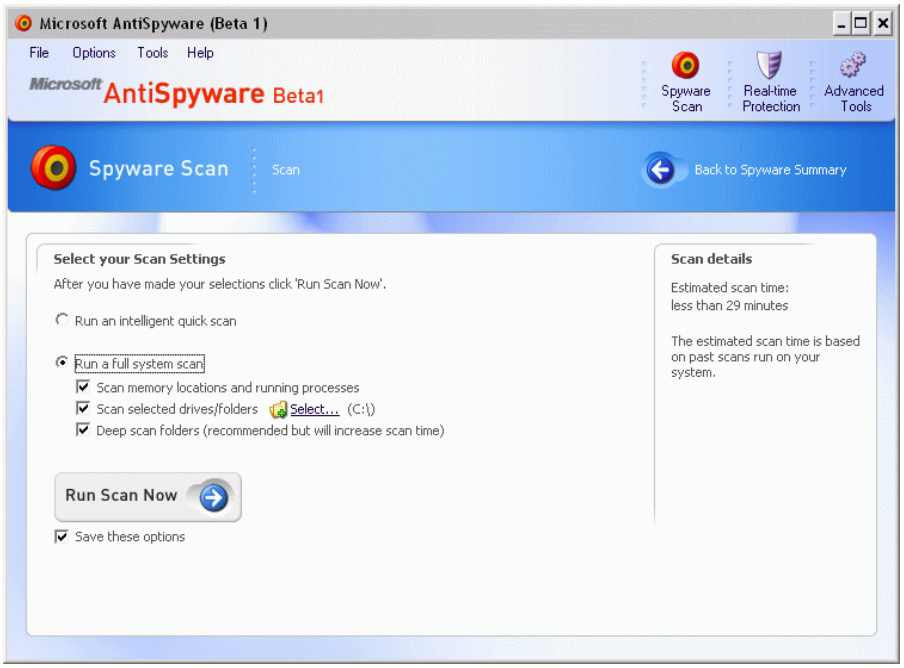


Fig. 41 - Microsoft Anti*Spyware* - Réglages d'analyse

Une fois l'analyse terminée, un résumé des menaces détectées s'affiche.

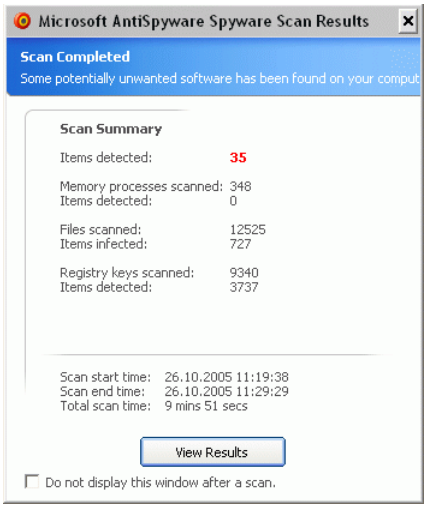


Fig. 42 - Microsoft Anti*Spyware* - Résumé de la 1ère analyse

Nous pouvons, dans la fenêtre qui suit, choisir l'action à mener pour chaque menace détectée. La liste complète des menaces détectées se trouve sur le CD sous `Tests infection\02 - machine infectée à fond\04 - Microsoft AntiSpyware\2c_log1_microsoft.txt`.

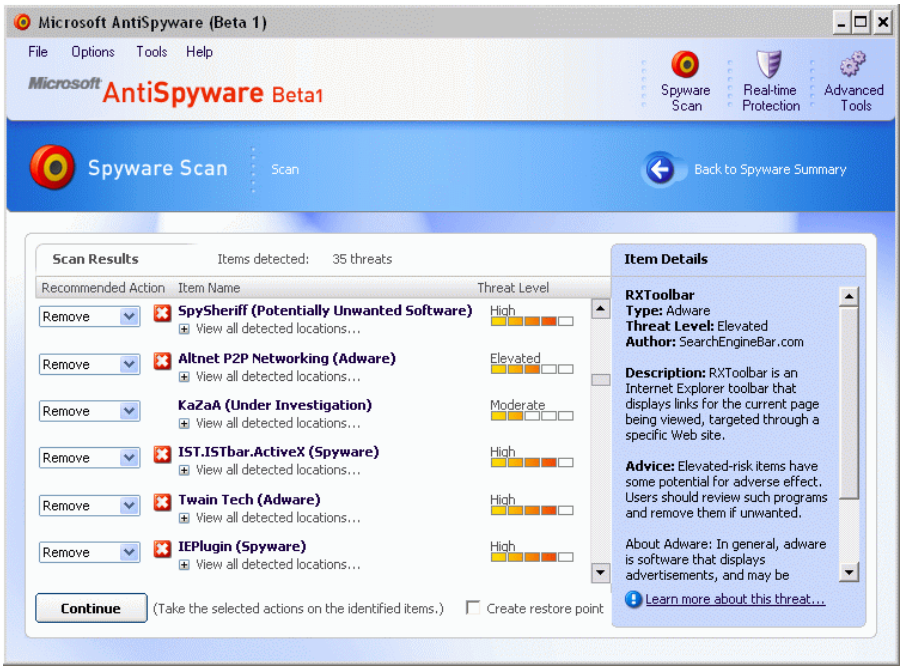


Fig. 43 - Microsoft Anti*Spyware* - Détails de la 1ère analyse

Nous choisissons ici de supprimer toutes les menaces. Puis nous redémarrons la machine en mode normal, de manière à voir si les *spywares* se sont réinstallés. Nous retournons en mode sans échec et refaisons une analyse.

La nouvelle analyse ne détecte plus que 2 menaces. Nous choisissons à nouveau de les supprimer et d'effectuer une nouvelle analyse. Celle-ci ne détecte plus aucun *spyware*.

4.3.2 Agent temps réel

Le module de protection en temps réel de ce logiciel est divisé en 3 sous-catégories :

- **Les agents internet** : protègent contre les applications modifiant les paramètres de connexion internet
- **Les agents système** : protègent contre les menaces modifiant les paramètres système, tels les permissions ou les services
- **Les agents application** : protègent contre les menaces installant, modifiant ou effaçant les logiciels installés, tels modifiant les paramètres d'IE, le téléchargement d'ActiveX ou l'ajout de nouveaux programmes à la liste de démarrage automatique

Les différents composants des agents peuvent être configurés selon le choix de l'utilisateur, de manière à permettre, par exemple, l'ajout de barre d'outils au navigateur.

Les messages affichés sont de 3 types différents. Les modifications acceptées par défaut sont affichées en vert. Celles demandant l'accord de l'utilisateur, mais ne présentant pas un grand danger, sont affichées en bleu, ce sont les avertissements. Celles étant dangereuses sont affichées en rouge, ce sont les alertes.

Fig. 44 - Microsoft Anti*Spyware* - Avertissement

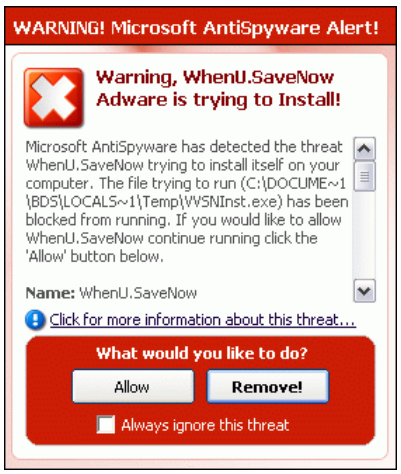


Fig. 45 - Microsoft Anti*Spyware* - Alerte

L'utilisateur peut ensuite choisir d'autoriser ou pas l'installation ou la modification demandée.

Une analyse périodique de certaines clés de registre (notamment les services et les paramètres IE) a lieu environ toutes les 20 secondes.

L'agent temps réel détectant toute installation de *spywares* connus et toute tentative de modification illégitime d'un paramètre système, le système ne sera infecté que si l'utilisateur l'autorise.

De nombreuses autres options sont disponibles, elles sont résumées dans la Fig. 52.

4.4 Spybot - Search&Destroy 1.4[17]

Développé par Safer Networking Ltd., Spybot - Search&Destroy (S&D) est un logiciel anti*spyware* gratuit, reconnu par certains comme un des meilleurs outils anti*spywares*.

Lors du lancement de l'application, cliquer sur « Mode », puis sur « Mode avancé », de manière à voir toutes les options disponibles. L'interface de S&D se présente alors comme suit :

Fig. 46 - Spybot - S&D - Écran d'accueil

Pour procéder à la mise à jour des signatures, cliquer sur « MAJ », puis sur « Recherche de mise à jour » et enfin sur « Télécharger les mises à jour ».

La liste des menaces reconnues peut être consultée dans les réglages de Spybot, sous « Modules additionnels » et « Ignorer : Produits ». En ce moment, environ 30000 menaces sont répertoriées. Un aperçu de la liste se trouve sur le CD sous `Tests infection\02 - machine infectée à fond\05 - Spybot - Search&Destroy\liste_menaces_reconnues_spybot.txt`.

[17] http://www.safer-networking.org/fr/spybotsd/index.html

4.4.1 Suppression à posteriori

Effectuons maintenant une analyse du système. Pour cela cliquons sur « Search & Destroy), puis sur « Vérifier tout ».

Une fois l'analyse terminée, 32 *spywares* ont été trouvés. La liste complète se trouve sur le CD sous `Tests infection\02 - machine infectée à fond\05 - Spybot - Search&Destroy\1b_log1_s&d.txt`.

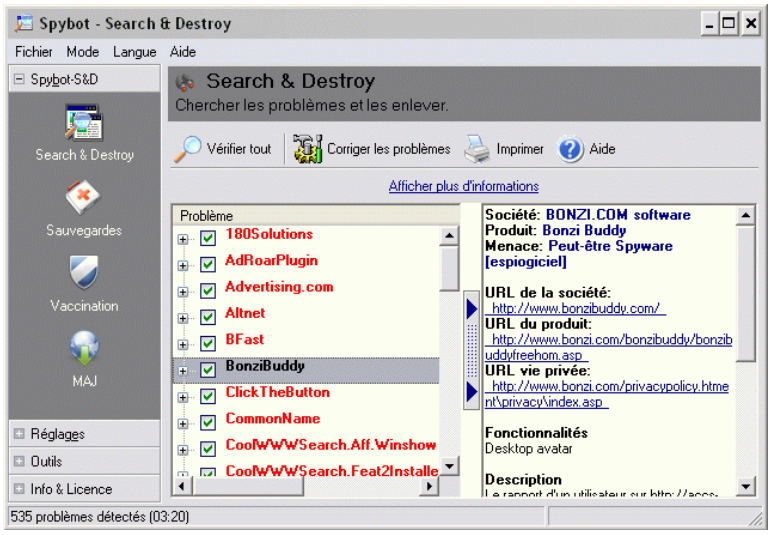


Fig. 47 - Spybot - S&D - Détails de la 1ère analyse

Nous choisissons de corriger tous les problèmes.

Lors de la suppression, certaines menaces n'ont pas pu être supprimées, il nous propose alors de les supprimer au démarrage de la machine.

Une fois la machine redémarrée, nous procédons à une nouvelle analyse.

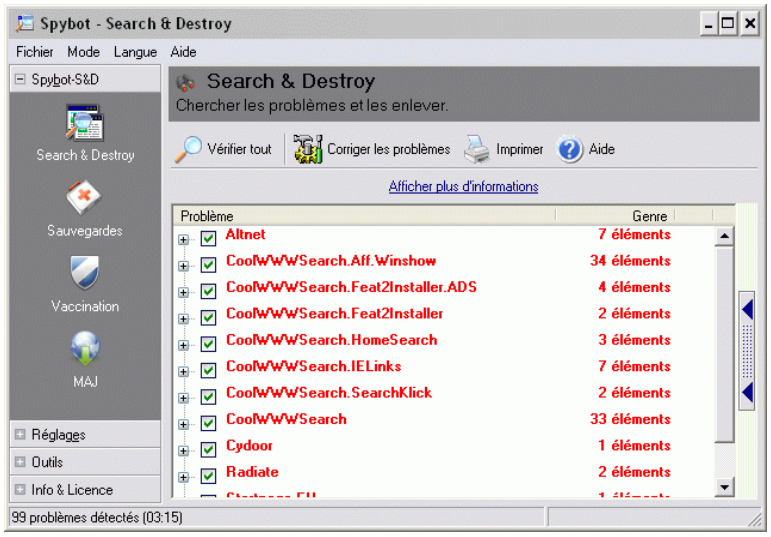


Fig. 48 - Spybot - S&D - Détails de la 2ème analyse

6 familles de *spywares* sont alors détectées. Les *spywares* se sont réinstallés lors du redémarrage en mode normal. Nous procédons de nouveau à la correction des problèmes et effectuons une nouvelle analyse.

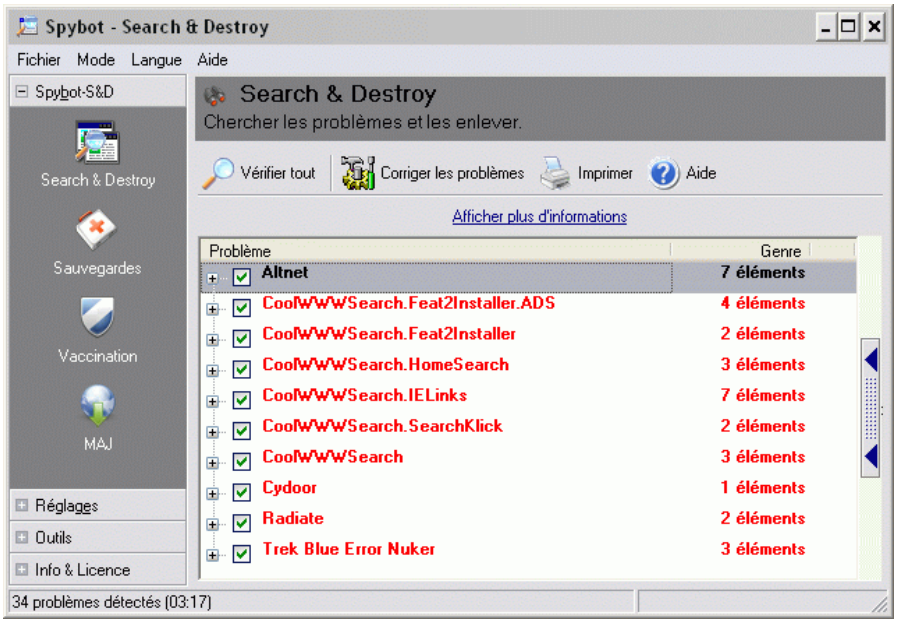


Fig. 49 - Spybot - S&D - Détails de la 3ème analyse

Nous nous apercevons que nous avons encore 5 menaces sur la machine. De plus, lors de la suppression, CoolWWWSearch.Feat2Installer n'a pas été complètement supprimé. On peut donc en déduire que c'est le responsable de la réapparition des autres éléments de la famille CoolWWWSearch.

4.4.2 Agent temps réel

La fonction de protection temps réel de Spybot – Search&Destroy est divisée en 2 modules appelés résidents :

- Le résident « SDHelper » : bloqueur de téléchargements nuisibles pour IE
- Le résident « TeaTimer » : protège les réglages système fondamentaux

Chaque fois qu'un réglage système important est modifié, une fenêtre s'affiche invitant l'utilisateur à prendre une décision.

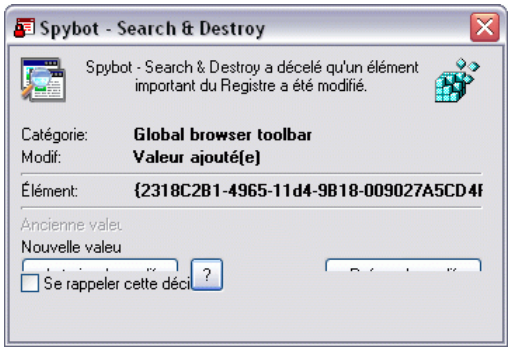


Fig. 50 - Spybot - S&D - Avertissement

L'utilisateur peut ensuite choisir d'autoriser ou pas l'installation ou la modification demandée. On remarque un *bug* lors de l'affichage de la fenêtre invitant l'utilisateur à autoriser ou pas, il convient de préciser que le bouton de droite permet de refuser, et celui de gauche autorise.

Une analyse périodique de certaines clés de registre (notamment les paramètres IE et les associations de fichiers) a lieu environ toutes les secondes.

4.5 Récapitulatif des caractéristiques

Après comparaison, entre eux, des résultats obtenus, nous arrivons à la conclusion que certaines menaces ne sont pas nommées de la même façon selon le logiciel utilisé.

Une comparaison manuelle a donc été effectuée, il en ressort que le nombre de menaces effectives est :

- Analyse orientée forensique : 22 menaces
- Lavasoft Ad-Aware SE Personal Edition 1.06r1 : 20 menaces
- Microsoft Anti*Spyware* Beta 1 v1.0.615 : 21 menaces
- Spybot - Search&Destroy 1.4 : 19 menaces

Le groupement de ces familles de menaces se trouve en annexe A4.

Le nombre de menaces détectées lors de l'analyse forensique sera pris comme référence pour le calcul de l'efficacité dans le tableau ci-dessous.

Performances	**Lavasoft Ad-Aware SE Personal Edition 1.06r1**	**Microsoft Anti*Spyware* Beta 1**	**Spybot – Search&Destroy**
Menaces détectées	20	21	19
Menaces supprimées	12	21	15
Durée moyenne d'analyse	~ 4 min.	~ 9 min. 50 s.	~ 3 min. 20 s.
Efficacité après 3 analyses	55 %	95 %	68 %
Autres	Capacité de suppression non optimale	• Bonne base de signatures • Suppression optimale	Pas la possibilité de choisir l'action de réparation à entreprendre

Fig. 51 - Outils de suppression - Tableau des performances

Propriétés	Lavasoft Ad-Aware SE Personal Edition 1.06r1	Microsoft Anti*Spyware* Beta 1	Spybot – Search&Destroy
Réparation après redémarrage	Oui	Non	Oui
Protection temps réel	Payant	Oui	Oui
Ignore list	Oui	Oui	Oui
Possibilité de restauration	Oui	Oui	Oui
Caractéristiques des *spywares*	Non	Oui	Oui
Planificateur d'analyse	Non	Oui	Oui
Autres	• Restauration des pages par défaut IE	• *Spynet community* : protection immédiate contre les nouvelles menaces • Outil d'exploration système : démarrage du système, Activex téléchargés, BHOs, barre d'outils, réglages IE, … • Analyseur de fichiers • Restauration des pages du navigateur • Effaceur de traces : *cookies*, … • Rapport de *spywares* suspectés	• Détection de traceurs (module additionnel) • Effaceur de sécurité : effacement définitif des fichiers • Ajustements IE : réglages cachés d'IE • Incohérences du registre • Démarrage du système

Fig. 52 - Outils de suppression - Tableau des propriétés

Ces quelques outils permettent de supprimer la plus part des *spywares* connus.

Cependant, l'utilisation conjointe de 2 de ces logiciels est vivement conseillée, car nous avons remarqué les différences de performances entre eux. Le choix le plus adéquat est d'utiliser Microsoft Anti*Spyware* avec Spybot – Search&Destroy, qui offrent aussi une protection en temps réel.

Si toutefois après utilisation de ces produits, il vous semble qu'il reste des programmes suspects. Il faudra alors procéder à une suppression manuelle en utilisant une liste de référence tel [CASTLE] ou [PROCLIB] et un utilitaire tel Autoruns de Sysinternals[18] pour détecter les programmes et services lancés au démarrage. Pour quelques *malwares* plus tenaces, il faudra même recourir au démarrage en ligne de commandes, afin d'effacer les fichiers requis, et à l'aide sur des forums spécialisés tel [SPYWAR] ou [SPYREM].

[18] http://www.sysinternals.com/Utilities/Autoruns.html

Conclusion

Tout au long de ce travail de diplôme il m'a été permis de constater la difficulté de travailler sur un poste de travail infecté de *spywares*, tant au niveau des performances de la machine, qui sont sévèrement diminuées, ainsi qu'au niveau de la gêne que ces logiciels causent à l'utilisateur, notamment par l'affichage de publicité.

Après avoir étudié et compris le fonctionnement de quelques-unes des méthodes d'infection utilisées par les *spywares*, il m'a été demandé d'étudier les différentes possibilités de protection de la machine.

Une approche logicielle à été développée, en définissant les bons réglages à appliquer au système d'exploitation ainsi qu'au navigateur internet et l'utilisation de logiciels tierce partie, tels les agents de protection temps réel, afin d'éviter l'infection de la machine. Une approche matérielle a ensuite été abordée, en utilisant un proxy Blue Coat. En tenant compte du fait qu'elle est avant tout ciblée pour les entreprises, elle permet d'être plus sélectif au niveau des informations à bloquer et donc de minimiser les risques d'infection. Une fois les 2 approches effectuées, il convient de rehausser que, pour un utilisateur particulier l'approche logicielle est plus adaptée car elle n'implique pas l'achat de nouveau matériel et permet d'utiliser presque toutes les fonctionnalités web existantes. Cependant, en ce qui concerne les entreprises, cette approche n'est pas du tout réaliste car elle implique la reconfiguration de tous les postes de travail du parc informatique, quand on sait que la plus part des entreprises actuelles possèdent plusieurs centaines, voire milliers de machines, cela devient très « lourd » à mettre en place. On optera dans ce cas pour la variante matérielle.

Si malgré toutes ces précautions prises, une infection a tout de même lieu, il faudra recourir à l'utilisation de logiciels de suppression adéquats ou procéder à la remise en état de la machine à l'aide d'un système de *ghost* ou à la réinstallation du système d'exploitation.

En résumé, ce travail de diplôme m'a permis de me rendre compte de la problématique liée aux *spywares* et d'en étudier les remèdes.

Certains points peuvent faire l'objet d'une étude postérieure plus approfondie, notamment les méthodes d'installations liées aux failles de sécurité du navigateur et du SE ainsi que d'autres logiciels (Office, …), le développement d'un *spyware* utilisant plusieurs de ces failles pourrait même faire l'objet d'un projet.

DE SOUSA Bruno

Références

[ACDNL] *ActiveX Control Downloading*
http://www.softlookup.com/tutorial/ActiveX/index17.asp

[ACVB6] Travail de diplôme : Visual Basic 6 & technologie ActiveX – Frédéric Comte – Ecole D'Ingénieurs d'Yverdon – Session 2001
http://activex.developpez.com

[BENED1] *Spyware installation methods*
http://www.benedelman.org/*spyware*/installations/
http://www.benedelman.org/news/041105-1.html

[BLEEPIN] Site de nouvelles informatiques, forums, définitions, tutoriaux
http://www.bleepingcomputer.com/

[CASTLE] Liste de programmes et BHO connus
http://castlecops.com/StartupList.html
http://castlecops.com/CLSID.html

[CERT] *Results of the security in ActiveX workshop*
http://www.cert.org/reports/activeX_report.pdf

[CHECKL] *Windows XP Security Checklist*
http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm

[HIJACK] *HijackThis log tutorial*
http://www.*spyware*info.com/~merijn/htlogtutorial.html
http://www.zebulon.fr/articles/HijackThis.php

[MSDNO] Contrôles ActiveX sur internet
http://msdn.microsoft.com/library/fre/default.asp?url=/library/FRE/vccore/html/_core_internet_first_steps.3a_.activex_controls.asp

[PREVENT] *What you can do about spyware and other unwanted software*
http://www.microsoft.com/athome/security/*spyware*/*spyware*prevent.mspx

[PROCLIB] Liste de processus connus
http://www.processlibrary.com/

[SECUS] *Spywares* : ces logiciels à votre écoute
http://www.secuser.com/dossiers/*spywares*_generalites.htm

[SPYREM] *Remove Adware & Spyware*
http://www.spyany.com/program/remove_adware_*spyware*_index.html
http://www.trendmicro.com/vinfo/grayware/default.asp

[SPYWAR] Forum spécialisé dans la lutte contre les *spywares*
http://www.*spyware*warrior.com/index.php

[TBICS] *ProxySG/ProxyAV TechBrief – Identifying & Controlling Spyware*
http://www.bluecoat.com/downloads/support/BCS_tb_controlling_*spyware*.pdf
http://download.bluecoat.com/LA/asCPL/*spyware*-WebSense.txt

Table des figures

Annexes

6 jours d'étude

A1. Environnement de travail

Pour ce travail de diplôme, nous avons besoin de travailler sur un environnement qui nous permette de remettre la machine dans un état propre quand il est jugé nécessaire, nous nous sommes donc tournés vers le choix de travailler sur une machine avec le logiciel VMware Workstation[19].

VMware Workstation est un puissant logiciel d'émulation de postes de travail, utilisé dans l'industrie pour le développement et le test d'applications. Il est installé sur une machine physique hôte, qui possède déjà un système d'exploitation.

Il permet de créer des machines virtuelles et d'y installer, par la suite, un système d'exploitation basé x86, tels Windows, Linux[20] ou encore Solaris[21].

Ces machines virtuelles se comportent exactement comme des machines physiques indépendantes. Les différentes interfaces de la machine hôte sont utilisées par les différentes machines virtuelles. L'annexe A2 apporte la justification de ce propos.

Les principaux avantages d'utiliser une machine virtuelle plutôt qu'une machine physique sont :

- Réduction des coûts matériels
- Diminution du temps d'installation de la machine
- Machine toujours propre, possibilité de restaurer une version antérieure de la machine virtuelle avec le système de *snapshots* (image instantanée du disque dur)
- Environnement *sandbox* (bac à sable). Les actions potentiellement dangereuses pour la machine, n'affecterons que la machine virtuelle et non la machine hôte

Pour toutes ces raisons, nous utiliserons un environnement VMware pour effectuer tous les tests par la suite.

Caractéristiques des machines	**Machine hôte**	**Machine virtuelle**
Processeur (Hz)	2.8 G	2.8 G
Mémoire RAM (Bytes)	1 G	748 M
Système d'exploitation	Windows XP SP2 - Mis à jour	Windows XP SP2 - De base
Navigateur internet	Internet Explorer 6 - Mis à jour	Internet Explorer 6 – De base

Les tests seront effectués en mode administrateur et utilisateur.

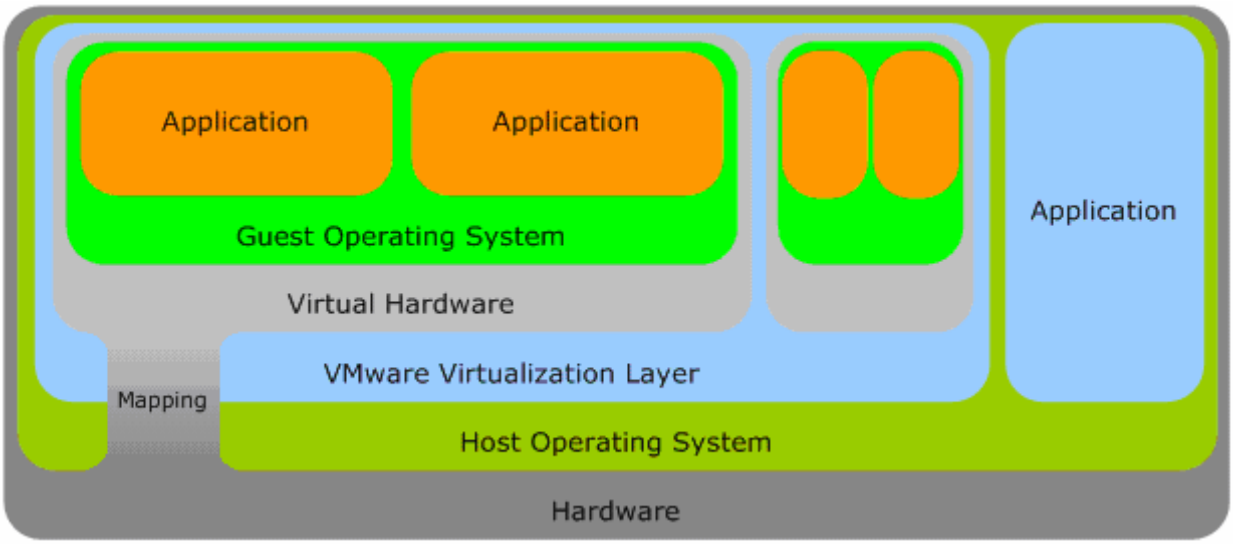
[19] http://www.vmware.com/products/ws/
[20] http://www.linux.org/
[21] http://www.sun.com/software/solaris/

A2. Indépendance des machines virtuelles VMware Workstation 5

Comme dit précédemment, l'environnement de travail utilisé pour ce projet a été choisi de manière à pouvoir remettre la machine dans un état propre à n'importe quel moment, nous avons pour cela choisi de travailler sur une plateforme VMware.

L'indépendance des machines virtuelles est donc essentielle, de manière à ne pas infecter la machine hôte lors des tests réalisés sur la machine virtuelle.

L'architecture VMware Workstation se présente comme suit :

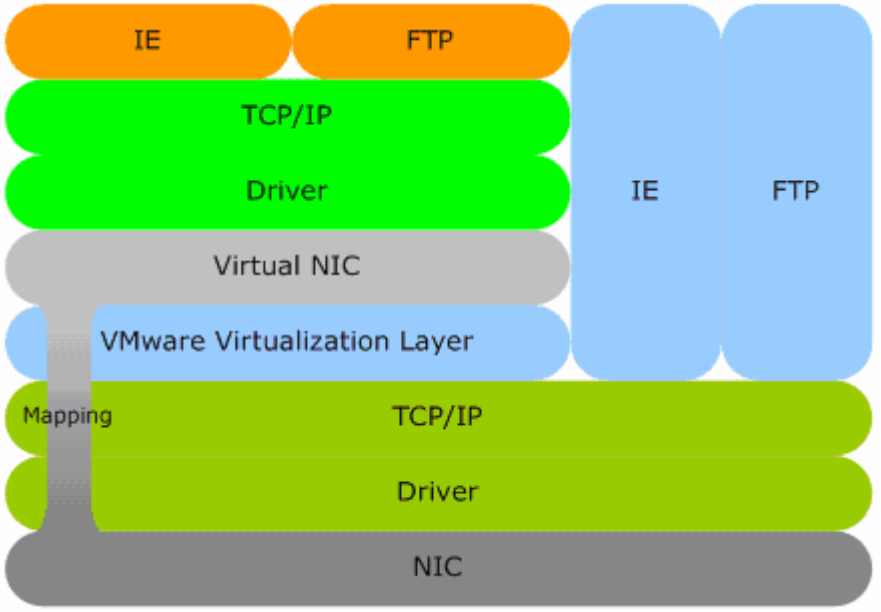


Nous remarquons que VMware est traité comme une application à part entière, la couche de virtualisation de VMware se charge d'effectuer le *mapping* du matériel physique en matériel virtuel.

En ce qui concerne les ressources mémoire et processeur, lors de la création de la machine virtuelle, l'utilisateur a la possibilité de définir la quantité de mémoire RAM à utiliser pour sa machine virtuelle. Une zone mémoire de cette taille sera alors réservée pour l'exécution de VMware et ne sera utilisée par aucune autre application. En ce qui concerne l'utilisation du processeur, comme VMware est considéré par le SE hôte comme une application à part entière, le processeur est partagé avec les autres applications, selon le besoin.

Pour les autres ressources matérielles, un *mapping* est effectué entre le matériel physique et le matériel virtuel.

Prenons le cas particulier d'une carte réseau NIC (*Network Interface Card*) :



Nous observons que le fonctionnement de la NIC physique, nécessite l'installation d'un pilote sur le SE. Une application, sur la machine hôte, ayant recours au réseau, utilisera alors le NIC physique, le driver et les paramètres TCP/IP du SE hôte.

Une application, sur la machine virtuelle, ayant recours au réseau, utilisera quant à elle le NIC virtuel, le driver et les paramètres TCP/IP du SE invité. Le NIC virtuel est réalisé par un *mapping* du NIC physique, ce qui veut dire que c'est comme si on avait une deuxième interface réseau indépendante.

Il convient d'effectuer quelques tests simples, de manière à démontrer cette affirmation.

Nous allons pour cela régler le TTL (*TimeToLive*) des paquets TCP/IP de la machine virtuelle à 10 et laisser celui de la machine hôte à la valeur par défaut (128). Nous procéderons ensuite à la capture des paquets et analyserons les valeurs de TTL obtenues.

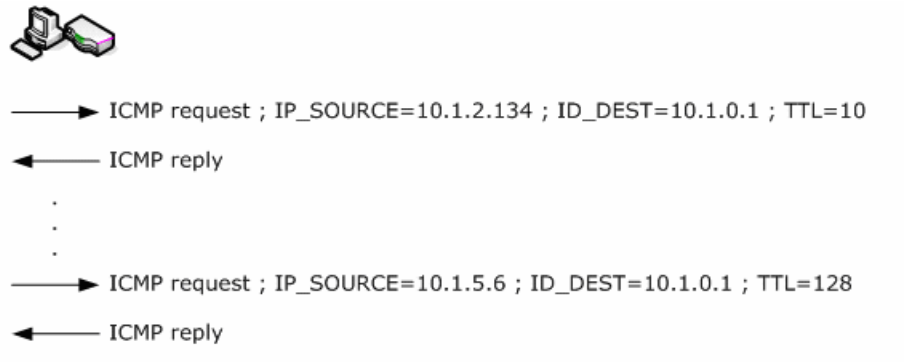
Les paramètres des machines sont :

- IP_NIC = 10.1.5.6
- IP_DEFAULT_GATEWAY_NIC : 10.1.0.1
- IP_VIRTUAL_NIC = 10.1.2.134
- IP_ DEFAULT_GATEWAY_VIRTUAL_NIC : 10.1.0.1

Nous modifions ensuite la valeur par défaut du TTL de la machine invitée, en ajoutant la clé suivante dans le registre invité :

- Clé : `[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]`
- Nom de la valeur : `DefaultTTL`
- Type : `REG_DWORD` (Valeur `DWORD`)
- Données de la valeur : 10 ou 0xA

Nous procédons ensuite à l'émission d'un *ping*, en provenance de la machine hôte et de la machine virtuelle, en direction de la passerelle par défaut :




```
No.  Time       Source         Destination    Protocol Info
1    0.000000   10.1.2.134     10.1.0.1       ICMP Echo (ping) request

Frame 1 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Vmware_f1:e5:08 (00:0c:29:f1:e5:08), Dst:
3com_b7:2e:60 (00:01:02:b7:2e:60)
Internet Protocol, Src: 10.1.2.134 (10.1.2.134), Dst: 10.1.0.1
(10.1.0.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0x016c (364)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 10
    Protocol: ICMP (0x01)
    Header checksum: 0x98cd [correct]
    Source: 10.1.2.134 (10.1.2.134)
    Destination: 10.1.0.1 (10.1.0.1)
Internet Control Message Protocol

No.  Time       Source         Destination    Protocol Info
2    0.001061   10.1.0.1       10.1.2.134     ICMP Echo (ping) reply

Frame 2 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 3com_b7:2e:60 (00:01:02:b7:2e:60), Dst:
Vmware_f1:e5:08 (00:0c:29:f1:e5:08)
Internet Protocol, Src: 10.1.0.1 (10.1.0.1), Dst: 10.1.2.134
(10.1.2.134)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0xeaa2 (60066)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
    Header checksum: 0xba95 [correct]
    Source: 10.1.0.1 (10.1.0.1)
    Destination: 10.1.2.134 (10.1.2.134)
Internet Control Message Protocol

...
```

```
No.  Time       Source         Destination    Protocol Info
9    11.243832  10.1.5.6       10.1.0.1       ICMP Echo (ping) request

Frame 9 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: WwPcbaTe_8d:59:45 (00:0f:1f:8d:59:45), Dst:
3com_b7:2e:60 (00:01:02:b7:2e:60)
Internet Protocol, Src: 10.1.5.6 (10.1.5.6), Dst: 10.1.0.1 (10.1.0.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0x0aec (2796)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (0x01)
    Header checksum: 0x16cd [correct]
    Source: 10.1.5.6 (10.1.5.6)
    Destination: 10.1.0.1 (10.1.0.1)
Internet Control Message Protocol

No.  Time       Source         Destination    Protocol Info
10   11.244422  10.1.0.1       10.1.5.6       ICMP Echo (ping) reply

Frame 10 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 3com_b7:2e:60 (00:01:02:b7:2e:60), Dst:
WwPcbaTe_8d:59:45 (00:0f:1f:8d:59:45)
Internet Protocol, Src: 10.1.0.1 (10.1.0.1), Dst: 10.1.5.6 (10.1.5.6)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0xf3a2 (62370)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
    Header checksum: 0xaf15 [correct]
    Source: 10.1.0.1 (10.1.0.1)
    Destination: 10.1.5.6 (10.1.5.6)
Internet Control Message Protocol

...
```

Nous remarquons que les paquets ICMP envoyés par la machine virtuelle possèdent un TTL=10, alors que ceux envoyés par la machine hôte possèdent un TTL=128 (par défaut).

Tout paramètre modifié exclusivement sur la machine hôte ou virtuelle, ne modifie en rien l'autre machine. Nous voyons donc bien l'indépendance entre les 2 machines. Il faut aussi remarquer que les différentes machines virtuelles sont, elles aussi, complètement indépendantes entre elles. De plus, le système d'exploitation invité peut être différent de celui installé sur la machine hôte, ce qui confirme qu'il ne doit y avoir aucun lien entre les paramètres d'un système et de l'autre.

A3. Outils d'analyse

A3.1 HijackThis 1.99.1[22]

HijackThis est un utilitaire reconnu dans le combat des *spywares* et autres *malwares*, orienté IE. Il peut cependant aussi servir lorsque d'autres navigateurs sont utilisés. Il analyse toutes les clés de registre appelées au démarrage de Windows ainsi que toutes les clés relatives à IE. Il nous informe aussi des processus lancés au moment de l'analyse.

Chaque ligne du log commence par un nom de section :

- **R - *Registry, StartPage / SearchPage changes***
  - **R0** - *Changed registry value*
  - **R1** - *Created registry value*
  - **R2** - *Created registry key*
  - **R3** - *Created extra registry value where only one should be*
- **F - *IniFiles, autoloading entries***
  - **F0** - *Changed inifile value*
  - **F1** - *Created inifile value*
  - **F2** - *Changed inifile value, mapped to Registry*
  - **F3** - *Created inifile value, mapped to Registry*
- **N - *Netscape / Mozilla StartPage / SearchPage changes***
  - **N1** - *Change in prefs.js of Netscape 4.x*
  - **N2** - *Change in prefs.js of Netscape 6*
  - **N3** - *Change in prefs.js of Netscape 7*
  - **N4** - *Change in prefs.js of Mozilla*
- **O - *Other, several sections which represent :***
  - **O1** - *Hijack of auto.search.msn.com with Hosts file*
  - **O2** - *Enumeration of existing MSIE BHO's*
  - **O3** - *Enumeration of existing MSIE toolbars*
  - **O4** - *Enumeration of suspicious autoloading Registry entries*
  - **O5** - *Blocking of loading Internet Options in Control Panel*
  - **O6** - *Disabling of 'Internet Options' Main tab with Policies*
  - **O7** - *Disabling of Regedit with Policies*
  - **O8** - *Extra MSIE context menu items*
  - **O9** - *Extra 'Tools' menuitems and buttons*
  - **O10** - *Breaking of Internet access by New.Net or WebHancer*
  - **O11** - *Extra options in MSIE 'Advanced' settings tab*
  - **O12** - *MSIE plugins for file extensions or MIME types*
  - **O13** - *Hijack of default URL prefixes*
  - **O14** - *Changing of IERESET.INF*
  - **O15** - *Trusted Zone Autoadd*
  - **O16** - *Download Program Files item*
  - **O17** - *Domain hijack*
  - **O18** - *Enumeration of existing protocols and filters*
  - **O19** - *User stylesheet hijack*
  - **O20** - *AppInit_DLLs autorun Registry value, Winlogon Notify Registry keys*

[22] http://www.*spyware*info.com/~merijn/htlogtutorial.html

- **021** - *ShellServiceObjectDelayLoad (SSODL) autorun Registry key*
- **022** - *SharedTaskScheduler autorun Registry key*
- **023** - *Enumeration of NT Services*

Fig. 53 - Noms de sections HijackThis

De plus, nous avons aussi la possibilité de « corriger » les clés dont les valeurs nous semblent erronées. La correction se fait soit par *reset*, soit par effacement de la clé. Il est utile lorsque la suppression à l'aide d'un des logiciels présentés en §4.2, §4.3 et §4.4 n'a pas été optimale.

Les droits administrateur sont requis de manière à avoir accès au fichier HOSTS ainsi que pour pouvoir effectuer la correction des valeurs, car il y aura modification dans la clé `HKLM` de la base de registre. Le fichier détaillant les clés de registre accédées par cet outil se trouve sur le CD sous `Tests infection\02 - machine infectée à fond\02 – HijackThis\acces_registre_hijackthis_regmon.LOG`.

A3.2 Ethereal 0.10.12[23]

Ethereal est un logiciel de capture de paquets sur le réseau. Il nous sera très utile pour comprendre les échanges HTTP qui ont lieu entre les *spywares* et leurs serveurs et analyser les données transmises.

Il nous faut, pour cela, être en mode administrateur de manière à pouvoir utiliser les librairies de capture de paquets.

A3.3 Regmon 7.02 de Sysinternals[24]

Regmon est un utilitaire de surveillance de la base de registre. Il affiche tous les programmes accédant à la base et toutes les clés accédées et/ou modifiées, en pseudo temps réel.

Il nous servira à comprendre le mécanisme des différents outils utilisés et le comportement de certains *spywares*. Notamment, il nous permettra d'observer quelles clés de registre ont pu être modifiées ou pas selon les droits que l'utilisateur possède sur la machine.

Nous remarquerons qu'un utilisateur sans droits administrateur, peut tout de même modifier toutes les valeurs se trouvant sous `HKEY_CURRENT_USER` (`HKCU`), il ne peut cependant pas modifier les valeurs sous `HKEY_LOCAL_MACHINE` (`HKLM`).

A3.4 Active Registry Monitor 1.38 de SmartLine[25]

ARM est un utilitaire permettant de comparer 2 bases de registre Windows.

L'utilisation de ce logiciel implique que l'utilisateur possède les droits de débogage, ce qui interdit son utilisation en mode utilisateur.

[23] http://www.ethereal.com
[24] http://www.sysinternals.com/Utilities/Regmon.html
[25] http://www.protect-me.com/arm

La version disponible pour le téléchargement nécessite l'installation du logiciel. Cependant, une fois le logiciel installé, l'exécutable peut être utilisé tout seul, c'est-à-dire qu'il peut, par exemple, être placé sur un CD-ROM ou autre support et utilisé tel quel. Il faudra dans ce cas définir la base de données à utiliser manuellement.

ARM permet d'importer une sauvegarde du registre créée avec Regedit, mais il est aussi capable d'en créer une.

Une fois la base de référence importée, nous pouvons effectuer une analyse de l'état actuel du registre et ainsi déterminer les différences entre les 2.

Cet utilitaire sera très utile pour l'analyse de type forensique, nous pourrons ainsi comparer les 2 sauvegardes et en déduire les modifications effectuées par les *malwares* installés.

A3.5 Process Explorer 9.25 de Sysinternals[26]

L'affichage de Process Explorer est divisé en 2 parties. La partie supérieure nous montre les processus en cours actuellement, alors que la partie inférieure nous montre soit les DLL utilisées par le processus sélectionné, soit les *handles* ouverts par ce processus.

Nous l'utiliserons pour déterminer avec quel processus (*spyware*) un exécutable inconnu communique.

[26] http://www.sysinternals.com/Utilities/ProcessExplorer.html

A4. Groupement des familles de menaces

Ad-Aware :

AltnetBDE(TAC index:4):66 total references
Aureate(TAC index:5):2 total references
BonziBuddy(TAC index:7):145 total references
BrilliantDigital(TAC index:6):3 total references
CoolWebSearch(TAC index:10):32 total references
Cydoor(TAC index:7):18 total references
DyFuCA(TAC index:3):3 total references
EzuLa(TAC index:6):193 total references
GROKSTER <- BroadCastPC(TAC index:7):12 total references" = Twaintech
IEPlugin <- ImIServer IEPlugin(TAC index:5):49 total references
Instafinder(TAC index:4):18 total references
istbar(TAC index:7):8 total references
Other(TAC index:5):3 total references
Possible Browser Hijack attempt(TAC index:3):20 total references
RXToolbar(TAC index:5):26 total references
Searchcentrix <- Visicom Media(TAC index:3):7 total references
Spysheriff <- *Spyware*No(TAC index:7):45 total references
webnexus <- VX2(TAC index:10):2 total references
WhenU(TAC index:3):60 total references
WinFixer(TAC index:3):126 total references

Windows Anti*Spyware* :

Altnet
Aureate
BonziBUDDY
Bonzibuddy <- ClickTheButton
coolwebsearch <- TargetSaver
coolwebsearch <- Travelling Salesman (zqff) = targetsaver
Cydoor
eZula.TopText
Go!Zilla Software Bundler
Grokster Software Bundler
IEPlugin
InstaFinder
IST.ISTbar
KaZaA
RXToolbar
SearchCentrix
SpySheriff
Twain Tech
Web P2P Installer
Webnexus
WhenU.SaveNow
Winfixer
WurldMedia

Spybot :

Altnet <- MyWay.MyBar:
Altnet:
Aureate <- Radiate:
bonzibuddy <- ClickTheButton:

```
BonziBuddy:
coolwebsearch <- Targetsaver:
coolwebsearch <- Trek Blue Error Nuker:
CoolWWWSearch:
Cydoor:
DyFuCA:
eZula HotText:
grokster <- AdRoarPlugin: twain tech
Grokster.Topsearch:
IE Plugin:
instafinder <- CommonName:
instafinder <- InstaFink:
IST <- ISearchTech.ISTactiveX:
Spy Sheriff:
spysheriff <- Smitfraud-C.:
SearchCentric <- VisiCom.SearchCentric:
web p2p installer <- Sumom.A:
Web-Nexus:
WhenU.SaveNow:
WinFixer:
WurldMedia:
```

A5. Catégories Websense

```
Categories defined by Websense:
    Adult Material
        Nudity
        Adult Content
        Sex
        Sex Education
        Lingerie and Swimsuit
    Business and Economy
        Financial Data and Services
    Education
        Cultural Institutions
        Educational Institutions
        Educational Materials
        Reference Materials
    Government
        Military
        Political Organizations
    News and Media
        Alternative Journals
    Religion
        Non-Traditional Religions and Occult and Folklore
        Traditional Religions
    Society and Lifestyles
        Restaurants and Dining
        Gay or Lesbian or Bisexual Interest
        Personals and Dating
        Alcohol and Tobacco
        Hobbies
        Personal Web Sites
    Special Events
    Information Technology
        URL Translation Sites
        Proxy Avoidance
        Search Engines and Portals
        Web Hosting
        Hacking
        Computer Security
    Abortion
        Pro-Choice
        Pro-Life
    Advocacy Groups
    Entertainment
        MP3 and Audio Download Services
    Gambling
    Games
    Illegal or Questionable
    Job Search
    Shopping
        Internet Auctions
        Real Estate
    Sports
        Sport Hunting and Gun Clubs
    Tasteless
    Travel
    Vehicles
    Violence
    Weapons
```

```
    Drugs
        Prescribed Medications
        Supplements and Unregulated Compounds
        Abused Drugs
        Marijuana
    Militancy and Extremist
    Racism and Hate
    Health
    User-Defined
    Internet Communication
        Web-based Email
        Web Chat
    Productivity PG
        Advertisements
        Online Brokerage and Trading
        Instant Messaging
        Freeware and Software Download
        Pay-to-Surf
        Message Boards and Clubs
    Bandwidth PG
        Internet Telephony
        Streaming Media
        Personal Network Storage and Backup
        Internet Radio and TV
        Peer-to-Peer File Sharing
    Social Organizations
        Service and Philanthropic Organizations
        Social and Affiliation Organizations
        Professional and Worker Organizations
    Security PG
        Malicious Web Sites
        Spyware
        Phishing and Other Frauds
        Keyloggers
    Miscellaneous
        Images (Media)
        Image Servers
        Private IP Addresses
        Content Delivery Networks
        Dynamic Content
        Network Errors
        Uncategorized
        File Download Servers

Categories defined by System:
    none
    unavailable
        unlicensed
```

A6. Code CPL pour configuration du Blue Coat ProxySG 400

```
; 1 - Bloquer les sites de spywares
;-----------------------------------------------------------------------
---------
;
;  Cette partie a pour but de détecter toute communication d'un spyware
avec son
;  serveur, ainsi que toute tentative d'installation à travers un site
spyware
;  connu, en utilisant les catégories et en loggant les événements

<Proxy Spyware_PhoneHome>
      ; tout trafic en direction ou provenant d'un site spyware est
refusé
      ; et la page s'affichant indique le message ci-dessous
      Condition=phone_home \
      http.response.code=(200..599) \
      access_log(phone_home_detected) \
      FORCE_DENY("Requête bloquée car spyware $(quot)phoning
home$(quot). Veuillez consulter votre ingénieur système.")

      ; trafic non refusé car certains spywares modifient tous les
headers du
      ; trafic même si ce n'est pas le leur, l'utilisateur est
néanmoins averti
      ; par une fenêtre d'alerte
      condition=spyware_request \
      http.response.code=(200..599) \
      access_log(phone_home_detected) \
      action.user_alert(yes)


; 2 - Bloquer les installations de spywares
;-----------------------------------------------------------------------
---------
;
;  1. L'extension du fichier ou le type du contenu est du contenu actif
;     -> Refuser
;  2. L'extension du fichier ou le type du contenu est un exécutable
;     et la categorie n'est pas autorisée à utiliser les exécutables
;     -> Refuser
;  3. Page web ne faisant pas partie des sites de confiance ->
supprimer les
;     balises dangereuses

<Proxy ActiveContent_Executable_control> condition=!trusted_sites \
                              condition=active_content_blocks
      ; 1a.
      condition=active_content_extensions \
      FORCE_DENY("Requête bloquée car spyware $(quot)Drive-by
Install$(quot) reconnue par active_content_extensions")    \
      access_log(drive_by_install_denied)
      ; 1b.
      condition=active_content_type \
      FORCE_DENY("Requête bloquée car spyware $(quot)Drive-by
Install$(quot) reconnue par active_content_type")    \
      access_log(drive_by_install_denied)
      ; 2a.
```

```
      condition=exe_blocks    \
      condition=exe_extensions \
      FORCE_DENY("Requête bloquée car téléchargement de fichier
exécutable dangereux.") \
      access_log(executable_file_denied)
      ; 2b.
      condition=exe_blocks    \
      condition=exe_content_type \
      FORCE_DENY("Requête bloquée car téléchargement de fichier
exécutable dangereux.") \
      access_log(executable_file_denied)
      ; 3.
      condition=webpage action.StripActiveContent(yes) \
      access_log(risky_tags_striped)
      ; 3.
      ;condition=webpage action.StripRiskyContent(yes) \
      ;access_log(risky_tags_striped)


;  Sites de confiance - liste blanche
;-------------------------------------------------------------------
---------
;
;  Les sites dans cette liste ne sont pas soumis aux règles précédentes

define url.domain condition trusted_domains
      bluecoat.com
      microsoft.com
      unige.ch
      windowsupdate.com
end

define subnet IP_Interne
      10.1.0.0/16
end

define condition trusted_sites
      ;category="Additional_Spyware_Trusted_Sites"
      condition=trusted_domains
      url.address=IP_Interne
end

; Création d'un catégorie permettant à l'utilisateur d'ajouter des
sites de
; confiance
define category Additional_Spyware_Trusted_Sites
end

;  Filtrage sur les catégories Websense
;-------------------------------------------------------------------
---------
;  Sites pour lesquels les exécutables sont refusés

define condition exe_blocks
      category="Nudity"
      category="Adult Content"
      category="Sex"
      category="Non-Traditional Religions and Occult and Folklore"
      category="Proxy Avoidance"
      category="Search Engines and Portals"
      category="Illegal or Questionable"
```

```
      category="Tasteless"
      category="Advertisements"
      category="Instant Messaging"
      category="Pay-to-Surf"
      category="Peer-to-Peer File Sharing"
      category="Dynamic Content"
      category="Network Errors"
      category="Uncategorized"
      category="none"
end

;  Sites pour lesquels le contenu actif est refusé
define condition active_content_blocks
      ; les exe_blocks ne peuvent pas nonplus afficher du contenu actif
      condition=exe_blocks
      ; catégories pour lesquelles les exécutables sont acceptés mais
pas le
      ; contenu actif
      category="Personal Web Sites"
      category="Hacking"
      category="Mp3 and Audio Download Services"
      category="Gambling"
      category="Games"
      category="Violence"
      category="Drugs"
      category="Militancy and Extremist"
      category="Racism and Hate"
end

define condition phone_home
      category="Security PG"
end



;  Active-Content patterns
;-------------------------------------------------------------------------
---------

;  Extensions de contenu actif
define condition active_content_extensions
      url.extension=cab
      url.extension=ocx
      ; recherche dans les Content-Disposition headers
      response.x_header.Content-Disposition="\.(cab|ocx)($|[^a-z0-9])"
end

;  Extensions exécutables
define condition exe_extensions
      url.extension=ace
      url.extension=ani
      url.extension=bat
      url.extension=chm
      url.extension=class
      url.extension=cmd
      url.extension=com
      url.extension=cpl
      url.extension=dll
      url.extension=exe
      url.extension=hlp
```

```
      url.extension=hta
      url.extension=jar
      url.extension=msi
      url.extension=pif
      url.extension=rar
      url.extension=reg
      url.extension=scr
      url.extension=vb
      url.extension=vbs
      url.extension=wsc
      url.extension=wsf
      url.extension=wsh
      url.extension=zip
      ; recherche dans les Content-Disposition headers
      response.x_header.Content-
Disposition="\.(ace|ani|bat|chm|class|cmd|com|cpl|dll|exe|hlp|hta|jar|m
si|pif|rar|reg|scr|vb|vbs|wsc|wsf|wsh|zip)($|[^a-z0-9])"
end

;  Types MIME de contenu actif
define condition active_content_type
      response.header.Content-Type="application/cab"
      response.header.Content-Type="application/x-compress"
      response.header.Content-Type="application/x-compressed"
      response.header.Content-Type="zz-application/zz-winassoc-cab"
      response.header.Content-Type="application/x-cab-compressed"
      response.header.Content-Type="application/(x-|)java[^s]"
end

;  Types MIME des exécutables
define condition exe_content_type
      response.header.Content-Type="application/octet-stream"
      response.header.Content-Type="application/x-msdownload"
      response.header.Content-Type="application/x-msdos-program"
end


;  Spyware Agent Patterns
;-------------------------------------------------------------------------
---------

define condition spyware_request
      request.header.User-Agent="Gator|FunWebProducts|BigBadProducts"
      request.header.User-Agent="ISEARCHTECH|IOKernel|MyWay"
      request.header.User-Agent="\.exe\|1, 0, 0,|3a|404search"
      request.header.User-Agent="Apropos|Browser Adv|Bundle"
      request.header.User-Agent="EnvoloAutoUpdater|ESB{|ezula"
      request.header.User-Agent="FunWebSearch"
      request.header.User-Agent="Godzilla|HelperH|Hotbar"
      request.header.User-Agent="iefeatsl|IST"
      request.header.User-Agent="istsvc|Kontiki|mez"
      request.header.User-Agent="MGS-Internal-Web-Manager|MyApp"
      request.header.User-Agent="ML"
      request.header.User-Agent="KHTML"
      request.header.User-
Agent="MyTotalSearch|MyTotalSearchSearchAssistant"
      request.header.User-
Agent="MyWebSearch|MyWebSearchSearchAssistant|NSISDL"
      request.header.User-Agent="OSSProxy|Peer Points
Manager|PeerEnabler"
      request.header.User-Agent="SAH Agent|searchengine2000\.com"
```

```
      request.header.User-Agent="Secret
Agent|sureseeker\.com|Sidesearch"
      request.header.User-Agent="SideStep Client|SurferPlugin|TIBS
Loader"
      request.header.User-Agent="TIBSBrowser|Topconvertingagent|TSA/"
      request.header.User-Agent="UCmore|Visicom Toolbar|Wildtangent"
      request.header.User-Agent="Wildtangent Kernel|Wise"
end


;  Suppression des balises
;-------------------------------------------------------------------------
---------

;  Suppression du contenu actif
define active_content transform_StripActiveContent
      tag_replace object <<EOT
            Contenu actif supprimé (object)
      EOT
end

;  Suppression des balises dangereuses
define active_content transform_Strip_Risky_Tags
      tag_replace object <<EOT
            Contenu dangereux supprimé (object).
      EOT
      tag_replace script <<EOT
            Contenu dangereux supprimé (script).
      EOT
      tag_replace embed <<EOT
            Contenu dangereux supprimé (embed).
      EOT
      tag_replace applet <<EOT
            Contenu dangereux supprimé (applet).
      EOT
end

define action StripActiveContent
      transform transform_StripActiveContent
end

define action StripRiskyContent
      transform transform_Strip_Risky_Tags
end

; Condition pour ne supprimmer que dans les pages html
define condition webpage
      client.protocol=http
      response.header.Content-Type="text/html"
end



; Affichage d'un avertissement


define javascript user_alert
prolog <<ABC123
{
      alert( "Alerte de sécurité\n\n"+
```

```
            "Une communication avec un serveur spyware a été
détectée.\n"+
            "Il se pourrait que vôtre machine soit infectée.\n"+
            "Veuillez consulter votre ingénieur système."
      );
}
ABC123
end

define action user_alert
      transform user_alert
end
```