MASTER EN SCIENCES INFORMATIQUES

Les logiciels espions

Bottes, Jean-Luc

Award date:
2006

Facultés Universitaires Notre-Dame de la Paix, Namur
Institut d'Informatique.
Année académique 2005-2006

Les logiciels espions

Jean-Luc Bottes

Mémoire présenté en vue de l'obtention du grade de Licencié en Informatique

« Seul un ordinateur éteint, enfermé dans un coffre-fort et enterré six pieds sous terre dans un endroit tenu secret peut être considéré comme sécurisé, et encore »
Bruce Schneier

Résumé et liste de mots clés

Résumé :

Les logiciels espions, connus sous le nom de "Spywares", sont des parasites qui ont constitué un phénomène d'une ampleur considérable ces dernières années.

Ces espions ont fait beaucoup parler d'eux dans la presse et sur Internet, de manière catastrophique ou minimaliste, les avis sont très partagés.

Mythe ou réalité, risque réel ou simple désagrément, l'ouvrage fait un état des lieux objectif en étudiant le phénomène d'un point de vue purement technique.

Il se penche essentiellement sur les logiciels espions à finalités commerciales et tente de mettre en garde l'utilisateur face au risque encouru en sa qualité d'internaute.

Une démonstration expérimentale met en évidence la complexité du problème.

Mots clés :

Logiciels espions, spyware, Gator, adware, Spybot, vie privée

---

Abstract:

Spywares are parasites that have been subject to a considerable proliferation over the last few years.

Although these spy programs have been much talked about in the press and in the media, opinions are divided as to their impact: either damaging and intrusive or negligible and annoying.

This is an investigation studying this area from a purely technical standpoint, concentrating on the spywares for commercial gain and outlining certain areas that current and future users of the Internet are at risk.

The scenarios described here illustrate the global complexity of the problem.

Keywords:

Spyware, Gator, adware, Spybot, privacy

Avant-propos

Mon expérience professionnelle a débuté dans le domaine du marketing direct. Celle-ci m'a amené à exploiter des profils d'abonnés à un magazine gratuit à des fins d'actions publicitaires. Ceci se passait au début des années 90.

Mon intérêt pour les spywares s'est éveillé suite à une présentation de Jean-Marc Dinant, doctorant aux Facultés de l'Université de Namur, sur le thème de la vie privée sur Internet. Il m'a fait prendre conscience du parallélisme de la situation. En effet, c'était exactement la même démarche que celle utilisée par les logiciels espions et adwares d'aujourd'hui.

Mon intérêt s'est naturellement porté sur le l'exploitation des données privées à des fins commerciales.

Je remercie Monsieur Ramaekers d'avoir fait le suivi et la relecture de mon travail, ainsi que Jean-Marc Dinant pour ses remarques judicieuses sur les choix du laboratoire.

Je pense également à Sophie et Luc qui m'ont encouragé et aidé tout au long de cette aventure, merci à eux.

Je n'oublie pas tous ceux qui ont cru en moi et m'ont soutenu.

Table des matières

Table des figures

Glossaire

ActiveX
ActiveX est une technologie de Microsoft, successeur de l'OLE (Object Linking and Embedding), qui permet l'exécution de programmes à l'intérieur d'autres programmes.

Adserver
Adserver est la contraction de Advertising Server, serveur de publicités. Ces sont des serveurs Internet gérés par des régies publicitaires spécialisées.

ADSL (Asymmetric Digital Subscriber Line)
L'ADSL, dont la traduction officielle est « raccordement numérique asymétrique » (RNA)

Adware
Voir *Publiciel*

AIM (AOL Instant Messaging)
AIM est le système de messagerie instantanée de America OnLine.

Backdoor
Voir *Porte dérobée*

Banner
Voir *Bannière*

Bannière
Une bannière est un encart publicitaire qui peut prendre différentes formes et tailles (incrustée sur une page web ou dans une application).

BHO (Browser Helper Objects)
Un BHO est un petit programme qui ajoute des fonctionnalités à Internet Explorer, des barres d'outils additionnelles affichées dans Internet Explorer par exemple.

Bot
Les bots, dérivés de robots, désignent tout programme s'exécutant de manière automatique sur un poste. Ils deviennent malveillants lorsque le programme s'installe sans l'accord de l'internaute et livre des informations sur la machine sur laquelle il s'est installé.

Chat
Le chat est un mot anglais désignant le bavardage, la conversation. Le chat est supporté par des outils de messagerie instantanée ou des canaux de discussion.

Cheval de Troie
Le cheval de Troie (ou troyen, en anglais « Trojan ») est un programme qui contient des fonctions cachées pouvant s'exécuter à l'insu de l'utilisateur.

CLSID (Class Identifier)
Le CSLID est un identificateur unique pour un ActiveX qu'on peut trouver dans la base de registre de Windows.

COM (Component Object Model)
Le Component Object Model, aussi connu sous le nom de ActiveX, est un composant logiciel (comme les DLL) créé par Microsoft. Il est utilisé pour permettre le dialogue inter-programmes. Ce format est le successeur de l'OLE.

Cookie
Un cookie est un petit fichier de texte enregistré et lu par un navigateur à la demande d'un site Web.

Crawler
Un robot d'indexation (en anglais « web crawler » ou « web spider ») est un logiciel qui explore automatiquement le web. Il est généralement conçu pour collecter les ressources indexées par un moteur de recherche

Dialer
voir *Numéroteur*

DLL (Dynamic Link Library)
Une DLL est une bibliothèque logicielle, un ensemble de routines regroupées pour réaliser un groupe de tâches du même domaine. Ce format de librairie est spécifique à Windows.

DMCA (Digital Millenium Copyright Act)
Le DMCA est une loi américaine. Le but de ce texte est de fournir un moyen de lutte contre les violations du droit d'auteur. Il vise à établir une législation de la propriété intellectuelle adaptée à l'ère numérique.

DNS (Domain Name System)
Le DNS est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.

DOS (Denial of Service)
En français « Déni de Service », une attaque par DOS vise à rendre un système ou une application informatique incapable de répondre aux requêtes des utilisateurs.

Enregistreurs de frappe au clavier
Les enregistreurs de frappe au clavier (en anglais « keylogger »), qui peuvent être matériels ou logiciels, ont pour fonction d'enregistrer furtivement absolument tout ce qu'un utilisateur tape sur un clavier d'ordinateur.

Error Reporting tool
voir *Outil de rapport d'erreur*

FAI (Fournisseur d'Accès Internet)
C'est par l'intermédiaire d'un FAI qu'un utilisateur se connecte sur le réseau Internet. L'équivalant en anglais est « ISP ».

Fenêtre surgissante
Une fenêtre surgissante est une fenêtre informatique qui s'affiche au dessus de la fenêtre de navigation normale lorsqu'on navigue sur internet, souvent pour afficher un message publicitaire.

Firewall
voir *Pare-feu*

Foistware
Le terme anglais « foistware » désigne tout programme non sollicité qui s'installe conjointement à une application, dont il est généralement difficile de se défaire.

Freeware
Voir *Graticiel*

FTP (File Transfert Protocol)
FTP est un protocole de transfert de fichier.

GUID (Globally Unique Identifier)
Le GUID est un nombre unique de 128 bits qui est produit par Windows ou par tout autre application Windows afin d'identifier un composant spécifique, une application, un fichier, un enregistrement de base de données et/ou un utilisateur.

Hijacker
voir *Pirate de navigateur*

HTML (HyperText Markup Language)
Le HTML est le langage de codage d'un document hypertexte.

HTTP (HyperText Tranfer Protocol)
Le HTTP est un protocole qui permet le transfert de documents de type hypertexte.

ICQ
ICQ est le système de messagerie instantanée crée par la firme Mirabilis, ensuite achetée par America On Line.

IMAP (Internet Message Access Protocol)
IMAP est un protocole utilisé par les serveurs de messagerie électronique

IRC (Internet Relay Chat)
L'IRC (en français « discussion relayée par Internet »), c'est un protocole de communication par Internet, prédécesseur des systèmes de messagerie instantanée.

ISP (Internet Service Provider)
Voir *FAI.*

Javascript
JavaScript est un langage de programmation utilisé principalement dans les navigateurs Web. De type interprété, c'est un des langages de script parmi les plus répandus, il est directement inclus dans le code de la page HTML.

Keylogger
Voir *Enregistreurs de frappe au clavier*

Kill bit
Le Kill bit est une technique de blocage d'installation d'ActiveX basée sur des listes de CSLID.

MAC (Media Access Control)
Une adresse MAC est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire et utilisé pour attribuer mondialement une adresse unique.

Malware
Voir *Programme nuisible*

Mouchard
Le mouchard est un autre nom désignant un logiciel espion.

Numéroteur
Le numéroteur (en anglais « dialer ») est un programme qui se connecte seul à Internet en utilisant un modem connecté à une ligne téléphonique. La connexion se fait généralement sur des sites à taux de facturation élevés.

OLE (Object Linking and Embedding)
OLE est un mécanisme qui permet de créer ou d'éditer des documents contenant des objets de diverses applications.

Outil de rapport d'erreur
L'outil de rapport d'erreurs est une routine incluse dans un programme qui permet de transmettre une collection de données techniques à une équipe de développement ou de maintenance en cas d'erreur fatale du programme à des fins de débogage.

Pare-feu
Le pare-feu (en anglais « Firewall ») et un dispositif logiciel ou matériel qui filtre les données sur un réseau informatique.

Partagiciel
Un partagiciel (en anglais « shareware ») est un logiciel propriétaire, protégé par le droit d'auteur, dont l'usage peut être limité dans le temps ou dans les fonctionnalités, à moins d'en rétribuer l'auteur.

PDA (Personal Directory Assistant)
Il s'agit d'un petit boîtier de la taille d'une calculatrice, qui tient dans la main, abritant une architecture informatique et doté d'un écran tactile et parfois d'un clavier incorporé avec des petites touches. Le PDA est utilisé principalement pour ses fonctions d'agenda, de répertoire téléphonique et de bloc-notes, mais les avancées technologiques ont permis de lui adjoindre des fonctionnalités multimédia.

PDF (Portable Document Format)
PDF est un format de fichier informatique créé par Adobe Systems. C'est un format ouvert dont les spécifications sont publiques et utilisables librement, dérivé du format PostScript.

Peer-to-peer
Voir *Poste à poste*

Pirate de navigateur
Un pirate de navigateur est un petit programme ou une entrée dans le registre qui est responsable du changement des pages de démarrage et de recherche d'Internet Explorer.

Pop over
Le pop-under est une forme de fenêtre intruse qui s'impose en avant-plan.

Pop under
Le pop-under est une forme de fenêtre intruse qui s'ouvre en arrière-plan.

POP3 (Post Office Protocol Version 3)
POP3 est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique.

Pop-up
Voir *fenêtre surgissante*

Porte dérobée
Une porte dérobée (en anglais « backdoor ») est un programme qui permet à un intrus d'accéder à l'ordinateur d'un utilisateur aussi longtemps qu'il est connecté à l'internet. C'est une sorte de télécommande, généralement très complète qui donne accès à tous les fichiers et ressources de l'ordinateur.

Poste à poste
Poste à poste (en anglais « Peer-to-Peer »), souvent abrégée P2P désigne un modèle de réseau informatique dont les éléments (les nœuds) ne jouent pas exclusivement les rôles de client ou de serveur mais fonctionnent des deux façons, en étant à la fois clients et serveurs des autres nœuds de ces réseaux, contrairement aux systèmes de type client-serveur.

Pourriel
Le pourriel (en anglais « spam ») désigne les communications électroniques massives, notamment de courrier électronique, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes.

Publiciel
Un publiciel (en anglais « adware », de « ad supported software ») est un programme propriétaire gratuit dont le créateur conserve les droits d'auteur, mais ne réclame aucune redevance pour son utilisation. Celui-ci reçoit une compensation car le logiciel est financé par la publicité qu'il affiche.

Référant
Le référent (en anglais « referrer ») est l'URL de la page contenant le lien dynamique qui a été suivi. Le référent fait partie de l'entête de la requête HTTP envoyée par le navigateur au serveur web.

Referrer
Voir *Référant*

Reniffleurs
Les renifleurs (en anglais « sniffer ») sont des logiciels qui affichent, impriment ou stockent en fichier pour analyse ultérieure l'exact contenu, caractère par caractère, de chaque paquet de données qui sort ou entre, ainsi que l'adresse IP du destinataire.

Rootkit
Un rootkit est un programme permettant à un pirate de maintenir dans le temps un accès frauduleux à un système informatique. Un rootkit utilise des faiblesses du système d'exploitation ou d'un programme ayant des droits particuliers pour, en fin de compte, lancer un shell ou ligne de commande ayant les droits de l'administrateur.

Scriptlet
Le scriptlet est un composant logiciel répondant aux spécifications du HTML dynamique, constitué d'un fichier contenant un modèle de page Web ainsi que les composants ActiveX et les directives permettant aux concepteurs de créer facilement des pages Web ou des éléments de pages Web.

Shareware
Voir *Partagiciel*

Smart-link
Les smart-links sont des hyperliens, généralement commerciaux, ajoutés sur certains mots d'une page web.

Smart-tags
Les smart-tags sont des smart-links que Microsoft a d'abord implémenté dans Internet Explorer de la version beta de Windows XP, ensuite abandonné (ou plutôt mis en suspend) dans les versions qui ont suivi suite à un tollé du public.

SMTP (Simple Mail Transfer Protocol)
Le SMTP est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.

Snapshot
Un snapshot est une capture d'écran, une photo logique de l'affichage à l'écran d'un utilisateur à un moment donné.

Sniffer
Voir *Reniffleur*

Spam
Voir *Pourriel*

Spider
Voir *Crawler*

Traçage
Le traçage est une technique qui consiste à enregistrer les actions prises par un utilisateur. C'est par exemple l'enregistrement des adresses des sites web visités.

Tracking
Voir *Traçage*

Trojan
Voir *Cheval de Troie*

URL (Uniform Resource Locator)
L'URL est une chaîne de caractères utilisée pour identifier les ressources dans le World Wide Web : document HTML, image, son ... Elle est informellement appelée une adresse Web.

Ver
Un ver informatique (en anglais « worm ») est un logiciel malveillant qui se reproduit sur des ordinateurs à l'aide d'un réseau informatique comme l'Internet et qui, contrairement à un virus, n'a pas besoin d'un programme hôte pour se reproduire.

Virus
Un virus informatique est un logiciel malveillant écrit dans le but de se dupliquer sur d'autres ordinateurs en infectant des programmes et documents. Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté.

Wabbit
Un wabbit est un type de logiciel malveillant qui s'auto-réplique. Contrairement aux virus, il n'infecte pas les programmes ni les documents et contrairement aux vers, il ne se propage pas par les réseaux.

Web bug
Un Web-Bug est un mouchard caché dans une micro-image invisible dans une page web ou un e-mail.

Whois
Whois est un service de recherche fourni par les Registres Internet régionaux ou bien les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine.

Worm
Voir *Vers*

Introduction

« Imaginez que quelqu'un vous suive constamment dans le moindre de vos déplacements, note vos moindres faits et gestes durant vos promenades, les personnes rencontrées, relève vos courses ou les vitrines que vous avez regardé, épie votre courrier, vos conversations, les livres feuilletés, les fiches médicales et de santé consultées, la nature des biens de consommation et des produits financiers sur lesquels vous vous êtes arrêté, le genre des sites religieux, philosophiques ou pornographiques parcourus, et vos mots de passe et revende ces informations... Est-ce que vous accepteriez cela ? Est-ce parce que l'espion est immatériel qu'il devient "fréquentable" ? »[1]

Cette citation de Pierre Pinard, auteur d'un site Web dédié à la sécurité et la protection de la vie privée, correspond à un point de vue journalistique du phénomène des logiciels espions. Ce ton accrocheur n'est pas innocent et trouve tout son sens dans la manière dont l'opinion publique réagit à la situation.

On trouve effectivement des avis partagés en la matière. Deux tendances à risque se dégagent rapidement. D'une part, on trouve les utilisateurs mal informés qui se croient immunisés. D'autre part, il y a ceux qui banalisent le phénomène « spyware » en se disant qu'il y en a partout et que c'est la moindre de leurs préoccupations. Ces derniers estiment que le spyware est un simple désagrément publicitaire, un juste prix à payer pour pouvoir utiliser du logiciel gratuit.

Ce mémoire traite de l'étude des logiciels espions par une observation et une analyse d'un point de vue purement technique, sans prendre parti sur le côté émotionnel ou sociologique de ce phénomène.

En mariant un exposé technique et une démonstration par études de cas, l'ouvrage a pour but de sensibiliser le lecteur aux risques réellement encourus, celui-ci étant directement lié à son comportement en sa qualité d'internaute. Il est donc primordial d'amener l'utilisateur à une réflexion fondée sur une connaissance élémentaire qui servira à l'évaluation du risque.

L'attitude des utilisateurs n'est pas la seule mesure anti-spyware, il existe plusieurs outils qui supportent cette démarche de contre-espionnage. Ces outils se basent sur des principes techniques des plus simples aux plus complexes, celles-ci étant présentées dans ce travail.

Les démonstrations confrontent le lecteur à des situations vécues par une majorité d'internautes et dont certains éléments, jusqu'à alors anodins pour les néophytes, prennent une signification et des implications que j'espère dignes d'intérêts.

[1] Pierre Pinard, Spyware, définition, http://assiste.free.fr/assiste.com.html?http://assiste.free.fr/p/internet_attaques/spyware.php

Chapitre 1 Etude théorique

1.1 Définition et généralités

1.1.1 Définition

Un logiciel espion, en anglais « spyware », est un programme ou un sous-programme qui s'installe sur l'ordinateur d'un utilisateur[2] sans sa permission éclairée. Ce programme, difficile ou impossible à désinstaller, est conçu dans le but de transmettre des données personnelles[3] ou des informations relatives à l'activité de l'utilisateur à son insu ou sans son consentement.[4]

Le terme « Spyware » est un acronyme anglais venant de « Spy » (espion / espionne en anglais) et « ware » qui désigne une classe de logiciels[5]. La traduction française de Logiciel Espion a donné également Espiogiciel[6], on l'appelle également plus simplement « espion » ou « mouchard ».

1.1.2 Qui est concerné ?

Toute personne accédant à Internet est susceptible d'être un jour confronté à un logiciel espion.

Il est difficile de connaître avec précision le nombre d'utilisateurs affectés, car le spyware s'exécute généralement avec discrétion et dans l'ignorance totale du propriétaire de l'ordinateur. Et même s'ils connaissent sa présence, beaucoup ne le voient pas comme une menace, tout au plus comme un vague inconvénient. Ils ne prennent donc aucune mesure pour s'en débarrasser et n'avertissent pas leur administrateur réseau. [ZAT01]

Des études tentent de déterminer une approximation du nombre d'ordinateurs infectés par un logiciel espion et ceux-ci s'accordent sur des résultats de l'ordre de 80% à 90%[7].

Dans l'esprit populaire, certains utilisateurs s'imaginent qu'ils ne risquent rien tant qu'ils ne visitent pas de sites douteux tels que les sites pornographiques ou des sites de pirates. Il n'en est rien. Ce type de sites est certes un vecteur important de propagation des logiciels espion mais bien d'autres sites dits « convenables » y contribuent également.

1.1.3 Méthodes d'introduction

Les spywares sont souvent présents dans des logiciels distribués gratuitement (connus sous le nom de « graticiels » en français et « freeware » en anglais), ou des partagiciels (« shareware »), afin de rentabiliser leur développement[8]. Le logiciel espion est installé conjointement au logiciel ou est intégré dans le logiciel.

Le canal de distribution le plus répandu actuellement fait appel à une technologie applicable au navigateur de Microsoft Internet Explorer exclusivement. Elle se fait au travers de fenêtres non sollicitées apparaissant en

---

[2] Un « utilisateur » tel que représenté dans cet ouvrage représente la victime potentielle d'un logiciel espion. Cette notion a son importance selon que l'on se place comme victime, distributeur ou concepteur d'un logiciel espion. Ces différents points de vue seront abordés plus loin. L'utilisateur « victime » est le profil exploité dans la majeure partie de l'ouvrage.

[3] La notion de « données à caractère personnel » fait l'objet de débats juridiques qui sont hors propos dans cet ouvrage.

[4] Edward Felten et Alex Halderman, du département informatique de l'université de Princeton, dans une publication de IEEE Security & Privacy donnent la définition suivante :
« The term 'Spyware' applies to software that's installed without the user's informed consent, is difficult or impossible to uninstall, and transmits information about the user's activities without notice or consent ».[IEE06]

[5] Par exemple : freeware (logiciel gratuit), shareware (partagiciel), cardware (l'auteur désire recevoir une carte de visite ou une carte postale pour le logiciel qu'il a développé), etc.

[6] Espiogiciel est parfois erronément orthographié Espiongiciel

[7] Selon une étude menée par Dell Corp. Du 17-19 septembre 2004, 90% des ordinateurs Windows sont infectés par un spyware ; selon l'étude de National Cyber Security Alliance et America Online du 25 octobre 2004, 80% des ordinateurs domestiques sont infectés par un spyware et 80% des détenteurs de systèmes infectés l'ignorent.[ALA01]

[8] Le graticiel est totalement gratuit, le partagiciel correspond généralement à une version d'évaluation pour laquelle une rétribution est demandée par l'auteur afin de continuer à l'utiliser en toute légalité ou encore afin de profiter de l'entièreté des fonctionnalités lorsque la version d'évaluation est bridée. Il ne faut pas confondre les graticiels avec des logiciels libres (« open software ») dont le code source est accessible, qui sont dépourvus de logiciel espion.

premier plan du navigateur d'un utilisateur lors d'une simple visite sur des pages d'un site web. Cette fenêtre l'invite à cliquer sur un bouton qui démarrera le téléchargement et l'installation du logiciel espion. L'utilisateur n'est bien sûr pas averti ni parfois même conscient que le fait de cliquer sur le bouton proposé aura de telles conséquences.

Une autre source de distribution est celle des fichiers exécutables joints aux courriers électroniques non sollicités. L'utilisateur qui ouvre le fichier attaché au message déclenche l'exécution de l'installation du logiciel espion.

Via Internet encore, en installant des greffons de navigateur comme par exemple une barre d'outils liée à un moteur de recherche.

Voici d'autres exemples de canaux de distribution :

- de nombreux économiseurs d'écran disponibles gratuitement au téléchargement,
- de nombreux accélérateurs de téléchargement, par exemple: Gozilla[9] et GetRight[10],
- des logiciels d'échange de fichiers (peer to peer) tels que Kazaa[11] et eMule[12],
- certains programmes de messagerie instantanée,
- certains programmes d'installation de pilotes de périphériques,
- la majorité des sites pornographiques et sites pirates (« crack », « warez »).

1.1.4 Objectif

Il faut distinguer deux types de logiciels espions : les logiciels espions à fins commerciales et les logiciels d'espionnage et de surveillance.

Le premier type est distribué à tout visiteur et dont on ne connait généralement pas l'identité. Dans cette catégorie, celui à qui profite le logiciel espion tente d'établir un profil d'utilisateur en étudiant son comportement, et accessoirement déterminer son identité. On y trouve tous les outils de traçage (en anglais « tracking ») et de profilage (en anglais « profiling »).

Le second type comprend toute une collection de logiciels d'espionnage et de surveillance d'un utilisateur a priori connu. Ils sont utilisés dans le cadre d'un véritable espionnage en violation du respect de la vie privée et de la législation. Ce type de logiciel ne fait pas l'objet principal de cette étude. Ce sujet y est abordé mais les recherches sont axées sur les logiciels espions de la première catégorie.

Le type de logiciel espion le plus répandu et plus alarmant est bien sur la première catégorie car tout internaute peut en être victime à tout moment. Le but est, en théorie, essentiellement commercial. Un spyware ne cherche pas spécifiquement à identifier l'utilisateur nominativement, mais à le cibler, qualifier, profiler, voire de profiler chaque utilisateur de l'ordinateur, identifié avec un nom de compte lors du « login », ou par diverses techniques de reconnaissance comme la vitesse de frappe au clavier, l'orthographe, le vocabulaire, etc.

« En réalité, par divers recoupements, l'identification devient personnelle avec des éléments plus concrets tels que le nom, l'adresse, le numéro de téléphone, les adresses e-mail, les numéros de comptes et mots de passe. La liste est longue, elle s'étend sur des informations plus orientées telles que le numéro de sécurité sociale, les polices d'assurances, les troubles et maladies, la religion, l'âge et le sexe, la sexualité, les sites et pages visités, le temps passé sur chaque page, les questions posées sur des forums de discussions, les mots-clés utilisés etc. ...

Tout ceci en secret et, lorsque l'utilisateur en prend conscience, contre son gré car il n'y a aucun moyen pour lui de l'empêcher, il est généralement trop tard pour réagir. Tout cela, prétendument, pour seulement permettre de déterminer ses centres d'intérêts[13], donc son profil de consommateur, afin de mieux cibler les publicités qui lui sont envoyées. »[PIN05]

---

[9] Go! Zilla (http://www.gozilla.com)

[10] GetRight (http://www.getright.com)

[11] Kazaa (http://www.kazaa.com)

[12] eMule (http://www.emule.fr)

[13] Exemples de ciblage, par centres d'intérêt : automobile, cinéma et spectacle, équipement électroménager, hi-fi / vidéo / télévision / informatique, sport, jeux et consoles, produits pour enfants, emploi et carrière, tourisme et voyage, ...

1.1.5 Justification

Les éditeurs de logiciels espions, ainsi que leurs distributeurs et autres exploitants (éditeurs de partagiciels, régies publicitaires, etc.) tentent de justifier ou de rassurer les utilisateurs sur l'usage des logiciels espion en évoquant différents principes :

- l'anonymat des informations,
- l'insignifiance des informations collectées,
- le modèle économique des entreprises présentes sur la toile.

Les informations collectées sont prétendument traitées uniquement de manière agrégée, garantissant par conséquent un anonymat des informations. Cette prétention s'avère être complètement fausse. Le traitement agrégé des données se fait sur base d'informations généralement nominatives, directement ou indirectement. Et quand bien même il n'y aurait pas de nom de personne physique derrière une information, il existe au moins un identifiant qui permet un autre type d'exploitation : le traçage et, par extension, le profilage.

Affirmer que l'information prélevée est insignifiante est une réponse simpliste qui ne peut contenter que les naïfs. Il est clair qu'on ne met pas en œuvre des moyens énormes, tant financiers que matériels pour ne prélever que des informations insignifiantes. Les enjeux économiques sont bien au-delà de ce qu'on laisse paraître.

Sous le prétexte que le modèle économique de l'Internet réclame une gratuité de services, on trouve une justification de l'usage de logiciels espions afin de rémunérer et de financer les divers intervenants humains et matériels du service en ligne.

1.2 Logiciels espions et virus

Il n'est pas rare qu'on confonde logiciel espion et virus. Les différences sont effectivement subtiles. Tous deux sont considérés comme logiciels malveillants (en anglais « malware »[14]) : non sollicités, intrusifs et potentiellement destructeurs. Tous deux ont la capacité de saisir et de détruire de l'information, ainsi que celle de ruiner les performances d'un système.

Les virus et les logiciels espions sont propagés par le biais des visites de pages Web et les téléchargements, ainsi que les fichiers attachés aux courriels. Tout deux peuvent attaquer un système par différents vecteurs.

On peut distinguer un virus d'un logiciel espion par l'étude du comportement de ceux-ci. Un virus cherche à contaminer un ordinateur, se répliquer, et finalement infecter le plus d'ordinateurs possibles, le plus rapidement possible. Lorsqu'un virus a infecté un ordinateur, ce code malicieux essaie de trouver tous les moyens mis à sa disposition pour se propager. Par exemple : l'envoi de courriel à partir d'un carnet d'adresse Outlook. De plus en plus, un virus ne se contentera pas de la messagerie pour assurer sa propagation, mais essaiera plusieurs vecteurs de propagation. Il exploitera les services tels que le partage de fichiers, telnet, FTP, les messageries instantanées et tout autre programme de communication.

Par contre, le logiciel espion essaie de rester en place, il adopte un comportement typiquement parasitaire. Dans le monde de l'espionnage, le logiciel espion peut se comparer à une taupe, qui évitera toute activité pouvant lui faire perdre sa couverture. Le logiciel espion prend l'apparence d'une application ordinaire ou vient se loger dans une librairie dynamique (DLL) ou dans une entrée de la base de registre dont l'utilisateur moyen ne connaît rien, afin de collecter les informations en toute discrétion.

Une autre distinction peut se faire de par leurs objectifs, ou plus précisément par les objectifs de l'auteur du logiciel malveillant. De nombreux virus sont écrits par des programmeurs qui ne cherchent qu'à se distinguer parmi leurs pairs et à faire un pied de nez aux éditeurs d'anti-virus et aux administrateurs réseaux. Les virus sont écrits pour supplanter les virus précédents et montrer jusqu'où peuvent être poussées les limites dans ce domaine de programmation.

Les logiciels espions soutirent d'un ordinateur hôte toutes informations financièrement exploitables, et cela aussi longtemps qu'ils peuvent rester sur l'hôte. Le logiciel espion se contente de résider sur un ordinateur et d'enregistrer toutes les activités de l'utilisateur. Il peut éventuellement l'influencer par l'intermédiaire de fenêtres publicitaires, de substitution du moteur de recherche ou par le changement de la page de démarrage. Les logiciels

[14] Le terme malware provient de l'anglais : « MALicious softWARE ». Il désigne tout logiciel malveillant, appelé également « code malicieux », qui a pour but de nuire à un système informatique, de traquer et surveiller les utilisateurs. On retrouve sous cette dénomination les virus, chevaux de Troie, les logiciels espions et autres logiciels indésirables.

espions drainent les ressources de l'ordinateur (usage du processeur) et en réduisent les performances générales. Mais quoi qu'il en soit, restent invariablement sur l'ordinateur hôte.

Enfin, on peut comparer les virus aux logiciels espions à travers leurs intentions malicieuses. Les virus sont en général intentionnellement destructeurs. Les logiciels espions quant à eux ont besoin de l'ordinateur hôte pour survivre et adoptent par conséquent un comportement non destructeur, sauf dans le cas où on tente de le désinstaller. De nombreux paquetages d'installation de logiciels espions sont résistants à la suppression : on peut les désinstaller pour les voir réapparaître au prochain redémarrage de l'ordinateur. D'autres modifient un ou plusieurs composants critiques du système d'exploitation de sorte à rendre le système inutilisable si on les désinstalle partiellement. [PIS05]

1.3 Logiciels espions et publiciels

A la base, un publiciel (en anglais « adware ») est un programme qui affiche des publicités. L'adware seul ne porte pas atteinte à la vie privée ni à la sécurité du système sur lequel il est installé.

Le logiciel espion est souvent confondu avec le publiciel. De fait, la différence tient à une légère nuance. Si ce programme ne fait qu'afficher de la publicité, c'est alors un adware. Par contre s'il envoie de l'information à un tiers sans avoir demandé le consentement de l'utilisateur, c'est un spyware. [ADW05]

Cela signifie qu'un programme peut être à la fois un spyware et un adware. Il est important de souligner que les adwares ne sont pas forcément des spywares et que la majorité de ceux-ci n'affichent pas systématiquement de la publicité comme des adwares. [ADW05]

L'adware est considéré comme une alternative légale offerte aux consommateurs qui ne veulent pas payer de droits d'utilisation de logiciels. Des programmes, jeux ou logiciels utilitaires peuvent être conçus et distribués sous la forme de graticiels (en anglais « freeware »). Il arrive parfois que des freewares soient volontairement limités dans les fonctionnalités jusqu'à ce qu'on s'acquitte des frais d'enregistrement. Actuellement, de nombreux freewares sont délivrés sous une forme « sponsorisée » jusqu'au paiement des frais d'enregistrement. L'entièreté des fonctionnalités est activée mais des publicités du sponsor sont affichées durant l'utilisation du logiciel. Les publicités sont généralement présentées sous forme d'encart dans une petite section de l'interface ou de fenêtre de type « pop-up ». A la fermeture du programme, les publicités liées au programme sont sensées disparaître. Ce mécanisme permet à l'utilisateur de tester le programme avant de l'acheter et de permettre la suppression des publicités moyennant une clé d'enregistrement. [BEA04]

1.4 Les logiciels d'espionnage et de surveillance

Les logiciels d'espionnage et de surveillance utilisent des techniques d'acquisition de données similaires à celles employées par les logiciels espions exploités par les publicistes et agences de marketing à des fins essentiellement commerciales. Le but poursuivi par ce type de logiciel espion est un espionnage plus personnalisé. La cible n'est pas le grand public mais une personne ou un organisme spécifique.

Différents éditeurs tels que Spy Arsenal[15] et E Spy Software[16] proposent des produits d'espionnage qui implémentent, par exemple, les fonctionnalités suivantes :

- l'enregistrement de tout ce qui est frappé au clavier (y compris : mots de passe, texte effacé etc.),
- l'enregistrement de toutes les informations passant sur un réseau via les pages web (HTTP), le transfert de fichiers (FTP) et le courrier entrant et sortant (SMTP, IMAP, POP3),
- l'enregistrement de l'environnement sonore d'un ordinateur par l'intermédiaire du microphone,
- l'enregistrement des conversations téléphoniques lorsque la ligne passe par un modem relié à l'ordinateur,
- l'enregistrement de tous les messages entrants et sortants via les canaux de discussion (IRC),
- la capture d'une photo de l'écran d'un utilisateur à intervalles régulier,
- l'enregistrement des conversations via les systèmes de messagerie instantanée (ICQ[17], AIM[18]).

---

[15] Spy Arsenal (http://www.spyarsenal.com)

[16] E Spy Software (http://www.e-spy-software.com)

[17] ICQ est l'outil créé par Mirabilis Ltd en 1996, ensuite racheté par America On Line en juin 1998 (http://www.icq.com)

[18] AIM est l'acronyme de AOL Instant Messaging, le système de messagerie instantanée d'America on Line (http://www.aim.com)

La cible et l'argument de vente de ce type de produit sont complètement différents de ceux conçus à des fins de marketing et de profilage sur les internautes. Ils sont généralement présentés comme produits de surveillance :

- pour protéger ses enfants des gens mal intentionnés avec qui ils pourraient avoir des contacts sur Internet,
- pour surveiller son conjoint car on soupçonne une liaison extraconjugale,
- pour surveiller les employés d'une entreprise afin d'utiliser l'infrastructure de l'entreprise « de manière optimale ».

1.5 Critères de classification

1.5.1 Visibilité

Certains spywares collectent des données sur leurs utilisateurs et interagissent de manière visible avec eux sous la forme :

- d'affichage de bannières publicitaires ciblées,
- d'apparition de fenêtres pop-up et leurs variantes,
- d'une modification du contenu des sites web visités afin par exemple d'y ajouter des liens commerciaux dits « liens intelligents » (en anglais « smart links »),
- d'envoi de courrier électronique non sollicité (« spam »[19]) ou de courrier papier (dans ce cas la visibilité est différée).

C'est la forme de spyware la plus répandue actuellement, il s'agit notamment des spywares de type « adware ».

Les bannières publicitaires sont des incrustations dans les pages des sites Web ou dans la fenêtre d'exécution d'un programme.

Le pop-up est le terme générique désignant une fenêtre indépendante qui apparaît inopinément sur l'écran de l'utilisateur à la manière d'un « Post-It », généralement dans le but d'afficher une publicité. En français, on utilise parfois le terme « fenêtre surgissante » pour désigner un pop-up.

Ceux-ci se déclinent en différentes variantes :

- pop over (pop-up s'affichant au premier plan, par dessus la page de navigation courante de l'utilisateur),
- pop under (forme un peu moins agressive de pop-up, qui vient s'afficher en arrière plan et qui n'est généralement visible que lorsque l'utilisateur quitte le site qu'il était en train de visiter),
- interstitiel (format de page publicitaire qui occupe l'écran durant l'intervalle de temps où un utilisateur quitte une page de navigation et l'affichage de la page suivante),
- superstitiel (forme d'interstitiel lourd de type multimédia),
- popup slider (forme d'objet "volant" qui se place au dessus des pages visitées).

Les spywares, appelés « mouchards » agissent en toute discrétion et ont pour objectif la collecte et l'envoi d'informations. Ces spywares s'efforcent généralement de ne montrer aucun signe d'activité (invisible dans la liste des programmes actifs, la barre des tâches et le système).

La surveillance et la réutilisation éventuelle des données collectées se font à l'insu des utilisateurs, généralement dans un but statistique ou marketing, de débogage ou de maintenance technique, voire de cyber-surveillance. L'existence de ces mouchards est délibérément cachée aux utilisateurs [JUD02].

1.5.2 Constitution logicielle

Une deuxième classification peut se faire sur base de la constitution logicielle du spyware. En effet, un spyware peut être intégré, externalisé, ou prendre une autre forme (script internes ou externes, locaux ou distants).

Les espions sont, la plupart du temps, la conjonction de plusieurs techniques simultanées qui coopèrent. Par exemple, les cookies ne sont pas des bouts de programme mais participent activement au processus d'espionnage qui utilise des rapprochements entre diverses données pour qu'elles deviennent nominatives et s'affinent.

[19] Les Français utilisent également les termes « polluriel » ou « pourriel » pour désigner le spam.

Les spywares espionnent. Il n'est pas nécessaire d'être connecté au Net pour qu'ils agissent, ils peuvent stocker l'information et la délivrer dès qu'une connexion est établie.

Les spywares utilisent une combinaison de différentes formes de programmation. L'une d'entre elles est le script sur le serveur d'un site visité qui permet de connaître certaines informations sur le visiteur et sa connexion (vitesse, navigateur et version, système d'exploitation et version, écran et résolution).

Les formes les plus abouties des spywares, sont les programmes à part entière implantés sur les ordinateurs. Il n'y a pas de limites à leur pouvoir d'investigation.

Spyware intégré

Le spyware intégré (ou interne) est une simple routine incluse dans le code d'un programme ayant une fonction propre, pour lui donner en plus la possibilité de collecter et de transmettre via internet des informations sur ses utilisateurs. Ce type de programmation suppose que l'éditeur du logiciel hôte est totalement complice ou est carrément et simultanément l'auteur des espions. Les logiciels concernés sont par exemple Gator, New.net[20], SaveNow, TopText, Alexa ou Webhancer[21].

Le spyware et le programme associé ne font qu'un et s'installent donc simultanément sur l'ordinateur de l'utilisateur.

Le terme anglais « foistware » désigne tout programme non sollicité qui s'installe conjointement à une application, dont il est généralement difficile de se défaire. Les américains utilisent une expression qui caractérise bien ce type de programme : « Everything-installs-it-can't-get-rid-of-it ». En français, tout ce qui s'installe et dont on ne peut se débarrasser. Ils arrivent à la manière d'un cheval de Troie, en plusieurs fragments logiciels, de sorte qu'en les supprimant un à un, ils parviennent quand même à réinfecter le système.[BOL01]

Exemple d'Alexa

Un bel exemple se retrouve dans le navigateur le plus utilisé à travers le monde : Microsoft Internet Explorer. Depuis la version 5, Internet Explorer est lié à Alexa, une société qui édite un spyware du même nom. Une entrée d'un des menus renvoi l'utilisateur vers une page en ligne de Microsoft, et c'est cette page qui redirige vers le moteur de recherche d'Alexa. Il est présenté comme un outil de recherche dans un des menus de la barre d'outils d'Internet Explorer. Celui-ci collecte et transmet les adresses de site web consultés à son serveur à des fins de marketing.

Figure 1 : Afficher les liens apparentés

Microsoft reste assez discret sur l'existence de cet espion. En consultant les dispositions légales à propos de cette fonctionnalité sur la barre d'outils, on peut trouver sur le site de Microsoft le texte suivant [MIC03].

> **Show Related Links**
>
> The Show Related Links functionality in Internet Explorer is provided by Alexa. If you would like to find Web pages similar to the Web page you are currently viewing, click the **Tools** menu, and then click **Show Related Links.** When you do so, the Web address of the page you are viewing is sent to an Alexa server which returns a list of potentially similar links in the Search Companion area. This information is not sent to Microsoft. If you do not wish to send the address of the Web page you are currently viewing to Alexa, do not click **Show Related Links**.

[20] New.Net est une librairie d'extension de navigateur (« IE plugin DLL »). Une fois installé, le logiciel tourne silencieusement au démarrage (vie Rundll32) grâce à une entrée placée dans la base de registre de Windows. Ce plugin s'apparente plus à une extension du système d'exploitation vu la manière dont il s'intègre à la configuration du réseau (socket Windows), de telle sorte que toutes les requêtes DNS passent par ce plugin.

[21] WebHancer prétend mesurer les performances des connexions sur tout le réseau. Il installe des clés dans la base de registre de Windows au niveau des sockets de telle sorte que toute connexion internet soit interrompue si jamais on essaie de supprimer cet espion.

Par ce paragraphe, on informe les utilisateurs que la fonctionnalité « Afficher les liens apparentés » est fournie par la société Alexa. On informe enfin qu'il ne faut pas utiliser cet outil si on ne veut pas que les adresses des sites Web visités actuellement ne soient transmises à la société tierce Alexa.

Il est intéressant de noter que le spyware Alexa est également intégré au navigateur de Netscape dès la version 4.0.6. La fonctionnalité sous Nescape s'intitule « What's Related ».

Spyware externalisé

Le spyware externalisé est une application autonome dialoguant avec le logiciel qui lui est associé, et pour le compte duquel elle se charge de collecter et de transmettre les informations sur ses utilisateurs.

Ces spywares sont conçus par des régies publicitaires ou des sociétés spécialisées comme Radiate, Cydoor, Conducent, Onflow ou Web3000, avec lesquelles les éditeurs de logiciels passent des accords. Le spyware de Cydoor est par exemple associé au logiciel peer-to-peer KaZaA, et s'installe séparément mais en même temps que lui.

Exemple de KaZaA

Kazaa serait placé en tête des «menaces spywares», selon l'éditeur américain de solutions de sécurité Computer Associates. Autrement dit, le logiciel d'échange de fichiers "peer-to-peer" serait aujourd'hui le programme intrusif le plus souvent téléchargé sur un ordinateur.[ILL04]

La version 3.0 de Kazaa, est disponible au téléchargement depuis le 22 novembre 2004. Une semaine après la mise en ligne, Kazaa 3.0 a été téléchargé plus d'un million de fois dans le monde, selon son éditeur. Un chiffre à relativiser toutefois car le succès de Kazaa semble suivre une courbe descendante, concurrencé par des alternatives moins intrusives: eMule, eDonkey, BitTorrent, et autre WinMX.[ILL04]

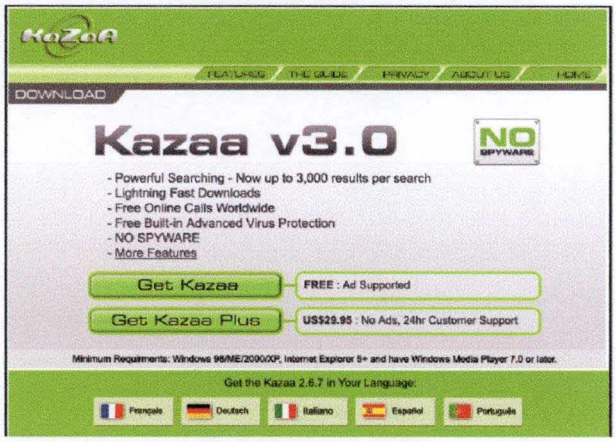
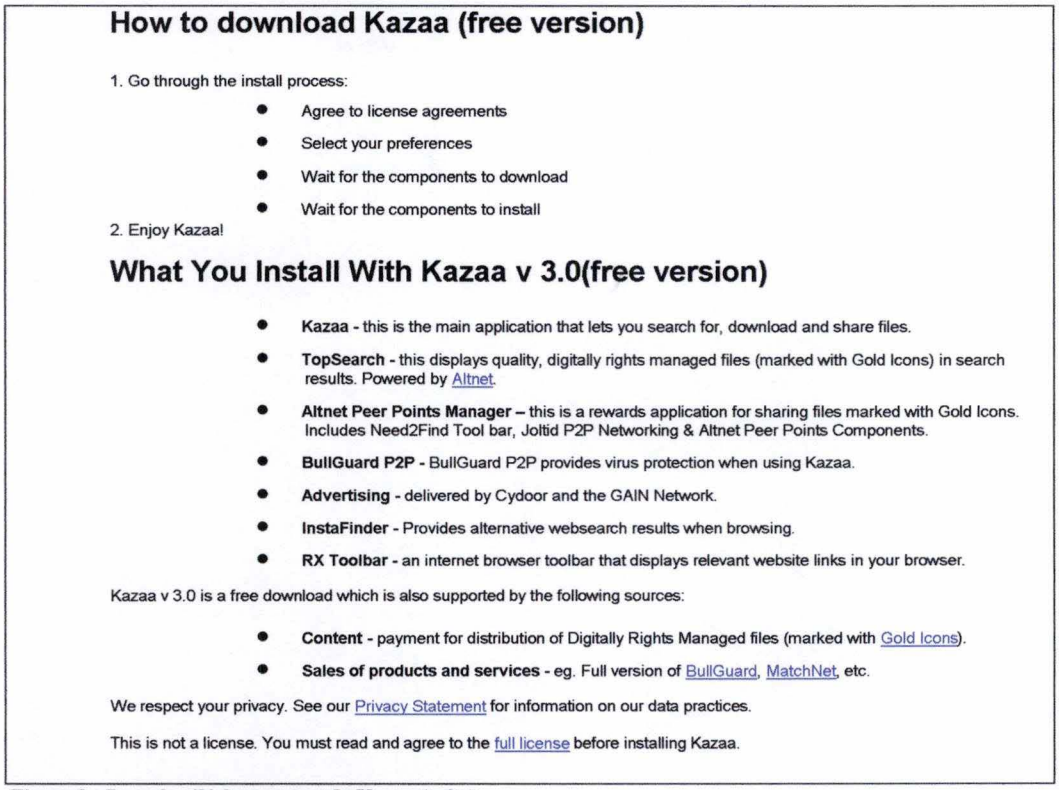


Figure 2 : Page de téléchargement de Kazaa[22]

La suite de la page est explicite quant à ce qui est réellement installé en même temps que l'outil de transfert de fichiers Kazaa[23].

[22] Kazaa (http://www.kazaa.com)

[23] L'illustration est en anglais car la version française est relative à la version 2.6.7 et ne contient pas la même information sur les installations annexes à Kazaa 3.0, bien que ceux-ci soient tout aussi présents dans cette version antérieure.



How to download Kazaa (free version)

1. Go through the install process:
   - Agree to license agreements
   - Select your preferences
   - Wait for the components to download
   - Wait for the components to install
2. Enjoy Kazaa!

What You Install With Kazaa v 3.0(free version)

- **Kazaa** - this is the main application that lets you search for, download and share files.
- **TopSearch** - this displays quality, digitally rights managed files (marked with Gold Icons) in search results. Powered by Altnet.
- **Altnet Peer Points Manager** – this is a rewards application for sharing files marked with Gold Icons. Includes Need2Find Tool bar, Joltid P2P Networking & Altnet Peer Points Components.
- **BullGuard P2P** - BullGuard P2P provides virus protection when using Kazaa.
- **Advertising** - delivered by Cydoor and the GAIN Network.
- **InstaFinder** - Provides alternative websearch results when browsing.
- **RX Toolbar** - an internet browser toolbar that displays relevant website links in your browser.

Kazaa v 3.0 is a free download which is also supported by the following sources:

- **Content** - payment for distribution of Digitally Rights Managed files (marked with Gold Icons).
- **Sales of products and services** - eg. Full version of BullGuard, MatchNet, etc.

We respect your privacy. See our Privacy Statement for information on our data practices.

This is not a license. You must read and agree to the full license before installing Kazaa.

Figure 3 : Page de téléchargement de Kazaa (suite)

La page de téléchargement arbore la bannière du « No spyware », cependant en étant un peu plus attentif au texte, en lisant la rubrique «Sharman Networks Privacy Statement », on peut lire un paragraphe « Publicité par un tiers », relatif aux partenaires commerciaux, notamment Cydoor et GAIN Network[24], nous informant que ces partenaires ont l'accès à certaines informations sur les utilisateurs. Il s'agit de programmes conçus pour afficher des pop-ups publicitaires en fonction des habitudes de navigation de l'utilisateur.

Sharman Networks se décharge de toute responsabilité en invoquant le paragraphe suivant : "Nous partageons des informations démographiques globales avec nos partenaires et annonceurs. Ces informations ne permettent, en aucune manière, une identification personnelle des utilisateurs. [...] Si vous vous connectez au site Web d'un tiers, ce dernier peut collecter directement certaines informations auprès de vous. Dans ce cas, consultez sa politique de confidentialité pour connaître l'utilisation de ces informations. Nous ne portons aucune responsabilité sur les conduites et pratiques des tiers. »[25]

1.6 Sources d'information et techniques d'acquisition

Les spywares mettent en œuvres différents moyens techniques en vue de collecter de l'information sur l'utilisateur. Outre les techniques d'espionnage nécessaires à la capture d'informations, certaines de celles-ci sont disponibles à tout instant ou sont fournies directement par l'utilisateur sans que celui-ci ne soit conscient de l'usage qui en sera fait. On y retrouve par exemple l'information entrée lors des procédures d'enregistrement en ligne des licences de logiciels, lors de leur téléchargement, leur installation ou au premier démarrage.

1.6.1 Bavardage de navigateurs

Pour consulter les pages Web, un internaute utilise un programme de navigation sur l'Internet que l'on appelle communément « navigateur ». Il est possible d'utiliser divers navigateurs car ceux-ci suivent un protocole commun : le protocole HTTP (« HyperText Transfer Protocol »). Ce protocole permet le transfert de pages qui suivent un format commun : le HTML (« HyperText Markup Language »). HTML est un langage de description de page de type « Hypertexte », ce qui signifie que ce document peut contenir des liens vers d'autres documents, des images, des fichiers ou tout autre objet supporté par le langage HTML. HTTP est donc le protocole qui permet

[24] GAIN Network (Gator Advertising and Information Network) désigne un ensemble de canaux de diffusion de publicité comportementale produits par la société Claria (anciennement Gator)

[25] Sharman Networks, Déclaration de confidentialité, http://www.kazaa.com/fr/privacy/privacy.htm (janvier 2005)

de transmettre des documents au format HTML. Les éléments qui composent un document HTML peuvent provenir du site Internet qui héberge le document, aussi bien que n'importe quel autre site référencé dans la page visitée. Il se peut par exemple qu'un site d'informations en Belgique affiche des images qui se trouvent à Hong-Kong ou à New-York, tout en donnant l'impression à l'internaute qu'il ne sort pas du site belge qu'il a choisi de visiter. Il est donc clair que l'internaute est amené à son insu à se connecter sur les tous les serveurs desquels le navigateur doit rapatrier de l'information pour constituer le document HTML. Notons qu'une image peut très bien être invisible aux yeux de l'internaute et servir de cette manière au transfert d'informations entre le navigateur et un site distant.

Les liens contenus dans un document HTML sont appelés hyperliens (en anglais « HyperLink »). Un hyperlien ne nécessite pas forcément une action volontaire de l'utilisateur pour être activé, il peut très bien l'être automatiquement à son insu.

Lors de la consultation de documents, les navigateurs sont bavards : ils échangent des informations communes incluses dans l'entête du protocole HTTP. Tous les navigateurs (Microsoft Internet Explorer, Netscape, Opera etc.) fournissent au site visité des informations sur le pays et la langue, l'environnement informatique, et, surtout, le référent, c'est-à-dire la page d'où on vient.

Si on analyse de plus près les informations contenues dans l'entête HTTP, nous pouvons décrire les champs suivants :

Accept-language	La plupart des navigateurs sont configurés pour accepter les pages Web rédigés dans une certaine langue. Le code de langue comprend souvent de l'information non seulement sur la langue supposée de l'utilisateur mais également sur le pays, par exemple « fr_BE » pour un francophone de Belgique. Ce paramètre peut bien évidemment être changé par l'utilisateur.
User-agent	Le paramètre « User-agent » transporte l'information relative à la marque et la version du navigateur ainsi que de l'environnement dans lequel il tourne. L'information sur l'environnement peut être très complète. Il est possible par exemple de déterminer que le système d'exploitation est Windows XP et même quel niveau de correctif.
Referrer	Le référent (en anglais « referrer ») contient l'adresse du site qui a amené l'internaute à la page qu'il visite actuellement, a condition d'y avoir accédé par l'intermédiaire d'un hyperlien. Il n'y a donc aucune information si l'utilisateur a entré l'adresse complète de la page dans l'adresse de destination du navigateur.
Cookies	Lorsqu'un navigateur reçoit des paramètres de type « cookies », ça lui permet d'écrire un petit texte localement et le lier à la page visitée. De cette façon, à chaque visite de ce même site, le cookie peut servir de petite mémoire que le serveur peut utiliser pour lire ou écrire des informations chez ce même internaute. Les cookies sont décrits dans le paragraphe suivant.

Une illustration de ces informations d'entête HTTP est présentée un peu plus loin dans le cadre de la navigation guidée par l'intermédiaire des moteurs de recherche de pages Web.

1.6.2 Les cookies

Les cookies sont des petits fichiers d'informations (au format texte) enregistrés sur un ordinateur par le navigateur à la demande d'un site Web. Un cookie est un fichier d'information, il ne peut donc pas contenir de virus. Il permet d'attribuer un profil ou une qualité, au moins pendant la durée de la navigation sur le site, ou plus longtemps, voire indéfiniment.

Au départ, l'objectif est de faciliter la consultation et la navigation sur un site web. Cependant, dans certains cas, ils peuvent servir à espionner (en enregistrant les sites visités, les données des formulaires remplis, etc.) ou à pirater un compte sur un site Web (en volant les cookies d'authentification).

Mais les cookies ne représentent pas forcément un risque, d'abord parce qu'un cookie enregistré par un site ne peut pas être lu par un autre. Ensuite l'espionnage et surtout le piratage ne peuvent exister que sous certaines conditions. Enfin les cookies ne contiennent pas toujours des données confidentielles[26].

[26] Par exemple le site de mesure d'audience estat.com enregistre le comportement d'un visiteur totalement anonymement, sans aucun danger pour sa vie privée. Ce cookie contient un numéro identifiant de l'ordinateur, numéro spécifique au site visité, qui ne sert qu'à produire des statistiques d'audience utiles au webmaster pour améliorer le contenu et la présentation du site

La durée de vie des cookies est fixée par le site, mais les options du navigateur permettent de définir leur durée de vie. Il existe deux types de cookies :

- les cookies de session étant supprimés automatiquement à la fermeture du navigateur, ou désactivés par le site émetteur,
- les cookies persistants ayant une durée plus grande, fixée unilatéralement par la personne qui l'a programmé. Ces cookies sont indépendants de l'adresse IP : ils « marquent » une machine et non une connexion, de sorte que même si l'adresse IP change entre deux connexions, le cookie fait le lien de l'une à l'autre, sauf s'il est physiquement détruit par l'utilisateur. [VER01]

Les cookies peuvent contenir toute information que le site Web juge utile, par exemple :

- le pseudonyme et le mot de passe pour poster des messages sur un forum sans devoir s'identifier plusieurs fois,
- un numéro de session pour conserver le contenu d'un caddie virtuel d'un rayon à l'autre, sur un site de commerce,
- un numéro identifiant l'ordinateur d'un visiteur pour l'identifier en lieu et place de son compte ou pour du tracking (traçage). Une telle information est spécifique au site qui l'a créé : il n'existe pas d'identifiant universel dans un cookie,
- des informations saisies par l'utilisateur (un formulaire de profil personnel, numéro de carte bancaire, des options de présentation, ...),
- des informations automatiques (la manière de naviguer dans le site, ...).

La lisibilité – ou pour être précis l'absence de lisibilité – des cookies est souvent montrée du doigt. Elle résulte de deux phénomènes. D'une part, les concepteurs de logiciels de navigation réalisent leurs produits d'une manière telle que le contrôle sur les cookies est rendu très difficile. Ces logiciels sont livrés avec une configuration par défaut qui accepte les cookies de manière automatique et invisible. D'autre part, à supposer que le contrôle soit activé, la compréhension des informations n'est pas aisée. [VER01]

Les cookies d'authentification

Les cookies d'authentification sont des cookies de session identifiant chaque abonné d'un service Web, qu'il s'agisse du pseudonyme et du mot de passe, ou d'un numéro valable seulement pendant la durée d'une session sur le service, c'est à dire jusqu'à la déconnection du site. Un cookie enregistré par un site ne peut être lu par un autre, mais un programme pirate peut voler les cookies d'un abonné au service sous certaines conditions. Par exemple dans un forum autorisant l'enregistrement de programme en JavaScript[27], un pirate peut rédiger un message en introduisant un programme malveillant qui récupère les cookies d'identification du lecteur. Quant un autre abonné lit le message, avec le JavaScript activé dans son navigateur, le malware s'exécute : il vole le cookie du lecteur et l'envoie au pirate (par e-mail par exemple), tout ceci à l'insu de la victime. Il pourra ensuite se connecter avec le compte de la victime pour changer son mot de passe, envoyer des messages sous son pseudonyme, etc.

Dans un Webmail (e-mail par navigateur) qui utilise une identification par cookie : les conditions et l'exécution du piratage sont les mêmes. Que le pseudonyme et le mot de passe soient cryptés n'empêche pas le piratage; les remplacer par un numéro identifiant non plus. Le pirate crée ces cookies dans son navigateur et se fait passer pour sa victime sur le site. Si ce dernier ne contrôle pas que deux adresses IP distinctes utilisent le même compte, le piratage est réussi [WEB05].

L'espionnage par cookie identifiant (tracking ou traçage)

Le but du tracking sur le Web est de cerner un profil-type de consommateur en fonction des sites visités ou des informations saisies dans des formulaires (centres d'intérêt) à partir duquel des sociétés vont pouvoir cibler de la publicité personnalisée dans les bandeaux ou des pop-ups. Pour cela, il leur faut associer ce profil à un individu. L'adresse IP est trop éphémère (le plus souvent elle sera différente à la prochaine connexion sur Internet).

Il est plus fréquent d'attribuer à un visiteur un numéro, qui identifiera son ordinateur de manière unique parmi toutes les machines du monde, enregistré sur son ordinateur dans un cookie pour une durée infinie (un cookie peut toujours être supprimé manuellement). Ainsi une société de tracking, qui affiche ses bandeaux, pop-up ou pop

[27] JavaScript est un langage de programmation utilisé principalement dans les navigateurs Web, il est directement inclus dans le code de la page HTML

under sur une quantité importante de sites, pourra constituer au fur et à mesure, une liste de sites, donc de thèmes de prédilection, donc un profil [WEB05].

Les web-bugs

Le terme anglais « web-bug » est un mouchard caché en micro-image invisible dans une page web ou un courrier électronique, servant à déclencher l'exécution d'un script depuis un site extérieur. Il est dissimulé derrière une image souvent invisible car la taille de celle-ci est typiquement réduite à 1 pixel. Le web-bug a été conçu pour tracer le lecteur d'une page web ou d'un courriel. Ils sont présents sous la forme d'un tag HTML.

Voici un exemple [28]:

```
<img src="http://ad.doubleclick.net/ad/pixel.quicken/NEW" width=1 height=1 border=0>

<IMG WIDTH=1 HEIGHT=1 border=0
SRC="http://media.preferences.com/ping?ML_SD=IntuitTE_Intuit_1x1_RunOfSite_Any
&db_afcr=4B31-C2FB-10E2C&event=reghome&group=register& time=1999.10.27.20.5 6.37">
```

Ces deux web-bugs ont été trouvés sur la page d'accueil du site de Quicken (http://www.quicken.com). Ceux-ci ont pour but de fournir à DoubleClick et MatchLogic (deux sociétés de publicité sur Internet) une information de consultation (en anglais « hit ») sur le visiteur.

Le web-bug est connu aussi sous le nom de « lien invisible » en français, et désigné par d'autres termes plus doux comme « clear GIF », « 1-by-1 GIF » ou encore « invisible GIF ».

Les web-bugs sont généralement invisibles mais ce n'est pas toujours le cas. Ils sont typiquement liés à un cookie afin de garantir une traçabilité. Le serveur qui héberge l'image « invisible » reçoit alors l'information suivante :

- l'adresse IP de l'ordinateur qui « visualise » l'image,
- l'URL de la page où se trouve le web-bug,
- l'URL du web-bug,
- le moment auquel le web-bug a été affiché,
- le type de navigateur utilisé,
- le contenu du cookie associé.

Le web-bug dans les courriels est utilisé de la même manière mais il permet de :

- déterminer si un message en particulier a été lu par quelqu'un, et quand dans l'affirmative,
- fournir l'adresse IP du destinataire si celui-ci tente de rester anonyme,
- donner, dans une organisation, une idée sur le nombre de fois que le message a été transmis et lu,
- mesurer combien de fois un message a été lu lors d'une campagne publicitaire,
- détecter si quelqu'un lit un message toutes boîtes. Un filtrage est alors possible en supprimant les destinataires qui n'ont pas lu le message de la prochaine liste de distribution,
- associer un cookie du navigateur Internet à une certaine adresse électronique.

Si quelqu'un utilise Outlook Express ou Netscape Messenger pour consulter les messages d'un groupe de nouvelles (« newsgroup »), les web-bugs fonctionnent également lorsque les messages sont au format HTML. Ils peuvent ainsi servir à tracer les utilisateurs qui consultent les messages d'un groupe particulier. Ces bugs peuvent être utilisés, par exemple, par des enquêteurs afin de tracer des activités illicites telles que la pornographie infantile, le commerce de fichiers musicaux protégés par droit d'auteur, ou pour surveiller les activités de personnes au sein de groupes politiques extrémistes.[SMI01]

[28] Cet exemple est traduit d'un article publié par Richard Smith sur le site de l'Electronic Frontier Foundation (http://www.eff.org) [SMI99]

1.6.3 Mots-clés de recherche

Un utilisateur qui cherche de l'information sur un thème précis va généralement effectuer sa recherche en entrant des mots-clés dans un moteur de recherche. Il en existe une multitude sur le marché fonctionnant quasiment tous sous la forme d'un service en ligne gratuit.

Les moteurs de recherche présentent différents modes de fonctionnement.

Annuaire de sites web

Il existe des annuaires (en anglais « Directory ») de sites qui sont constitués de catégories organisées "en arbre". Cette structure permet aux utilisateurs d'obtenir aisément une subdivision des sites par typologie, en isolant ainsi seulement ceux relatifs à l'argument recherché.[DIF01]

Ces annuaires sont également appelés « guide du Web ». On retrouve dans cette catégorie par exemple Yahoo![29], Linkcity[30] et Open Directory[31].

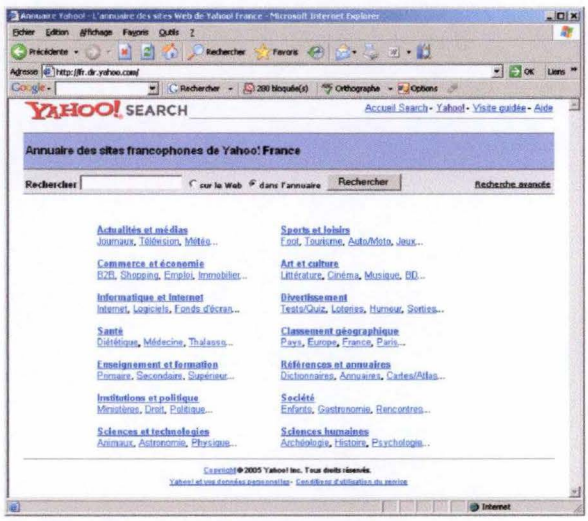


Figure 4 : Annuaire de recherche Yahoo!

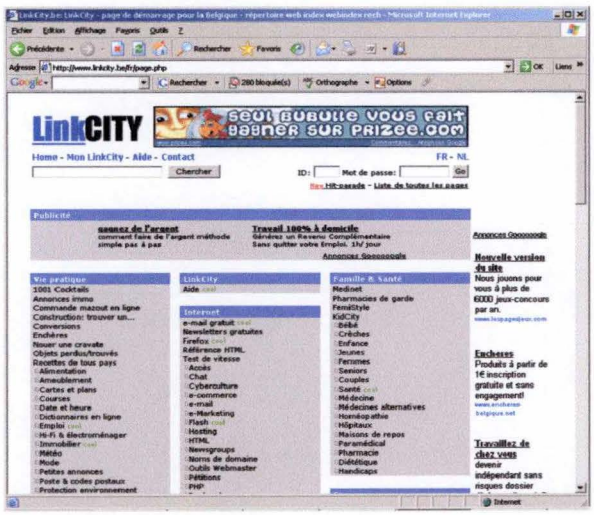


Figure 5 : Annuaire de recherche LinkCity

Moteurs de recherche

Cependant, la majorité des outils de recherche fonctionnent différemment. Il s'agit des outils appelés « Moteurs de recherche » (en anglais « Search Engines »). Ils recensent les sites Web sur la base de l'importance des mots contenus dans chaque page du site, mettant en évidence ceux qui apparaissent le plus souvent en supposant qu'ils représentent l'argument principal de la page même. Afin de faire ceci, ils classent non seulement les sites soumis par des utilisateurs mais sondent également et sans interruption tout le Web en utilisant des programmes spécifiques (appelés « spider » ou « crawler »), saisissant toutes les pages qui ne sont pas encore classées dans leurs archives. [DIF01]

---

29 Yahoo! Directory (http://fr.dir.yahoo.com)

30 Linkcity (http://www.linkcity.be)

31 Open Directory est une initiative "open source", il est développé par des éditeurs volontaires (http://www.dmoz.com). Le projet né avec le nom de NewHoo! en 1998, fut absorbé par Netscape en novembre 1998 et rebaptisé Open Directory Project; il fait maintenant partie de la famille AOL (America On Line) qui à son tour a acheté Netscape.[DIF01]

Parmi les plus utilisés, on retrouve Google[32], Lycos[33], Yahoo![34], Altavista[35], GoTo[36], Voila[37] et MSN[38]. Yahoo! permet une recherche dans les deux modes (moteur de recherche sur base de mots clés et de consultation d'annuaire). Google se classe actuellement parmi les moteurs ayant le plus d'avancée technologique en matière de moteurs de recherche. La multitude de moteurs de recherche se base généralement sur les mêmes « crawlers » qui sont en nombre réduit sur le marché. On peut citer par exemple : Google, Inktomi[39] et MSN.

En plus des moteurs de recherches précités, il existe également des sites qui exploitent plusieurs moteurs de recherche. Ceux-ci sont appelé « Méta moteur de recherche » (en anglais « Metasearch engine »). Dans cette catégorie on citera pour exemple Ariane[40], Answers[41], 123trouve[42], MetaSearch[43].

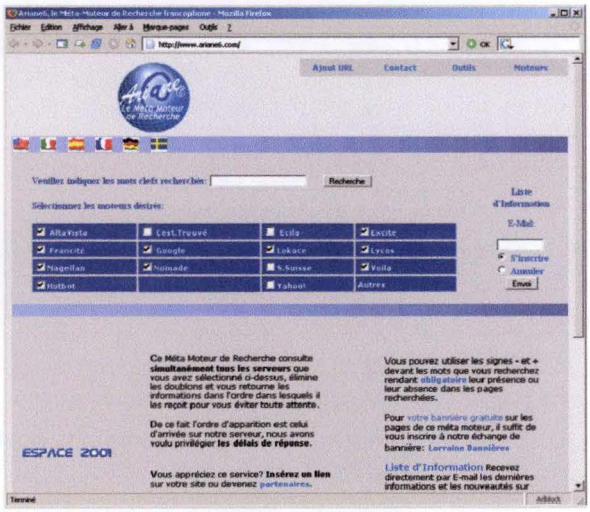


Figure 6 : méta moteur de recherche Ariane6

Portail

Les prestataires de service de recherche diversifient généralement leur offre, en proposant des espaces de discussion, un service de boîte aux lettres électronique, des jeux en ligne ainsi que des serveurs de « news ».

---

[32] Google (http://www.google.com, http://www.google.be)

[33] Lycos (http://www.lycos.fr)

[34] Yahoo! (http://www.yahoo.com, http://fr.yahoo.com)

[35] AltaVista (http://www.altavista.com, http://www.altavista.fr)

[36] GoTo (http://www.overture.com) a changé de nom en 2001 pour devenir Overture.

[37] Voila (http://www.voila.fr)

[38] MSN (http://www.msn.com, http://www.msn.fr)

[39] Inktomi (http://www.inktomi.com) est actuellement une filiale de Yahoo!.

[40] Ariane (http://www.ariane6.com)

[41] Answers (http://www.answers.com)

[42] 123trouve (http://www.123trouve.com)

[43] MetaSearch (http://www.metasearch.com)

Ces services sont souvent regroupés sur une page d'accueil appelé « portail » qui devient le point central d'accès vers la panoplie de services.

Figure 7 : portail Yahoo!

Figure 8 : portail MSN

Collecte de données

Les moteurs de recherche sont devenus des acteurs importants en termes de collecte de données comportementales sur les utilisateurs. En analysant les requêtes des utilisateurs, ainsi que le contenu des sites répertoriés dans leurs index, les moteurs de recherches sont capables de dresser un profil riche et précis de l'internaute. [LEO01]

De plus en plus souvent, en contrepartie de la gratuité du service, les fournisseurs demandent aux utilisateurs de leur fournir une série d'informations personnelles sous la forme d'un sondage ou proposent de s'inscrire afin d'accéder à un éventail plus étendu d'options ou de recevoir des offres publicitaires personnalisées.

Les sites de type « portail » ont ainsi tout le loisir de récolter et de mettre en corrélation les informations collectées sur un utilisateur. Ces informations sont non seulement celles fournies sciemment dans un formulaire d'inscription, mais également toutes celles déduites sur ses centres d'intérêts et ses habitudes d'internaute.

Mots-clés et référant

Dans un paragraphe précédent consacré au bavardage des navigateurs, on a vu qu'il était toujours possible de consulter le référant, comme il fait partie du protocole même de transfert des pages web. Les sites accédés par l'intermédiaire d'un moteur de recherche n'échappent pas à la règle.

Voici un petit exemple qui met en évidence comment un site peut lire tous les mots-clés entrés dans un moteur de recherche et qui ont conduit à la visite d'une page web.

Cherchons de la littérature sur les jeux d'échec. On tape donc « jeu d'échec livres » sur Google, un des moteurs de recherche des plus utilisés. Le premier résultat trouvé nous intéresse, on clique alors sur ce premier lien pour visiter la page proposée.

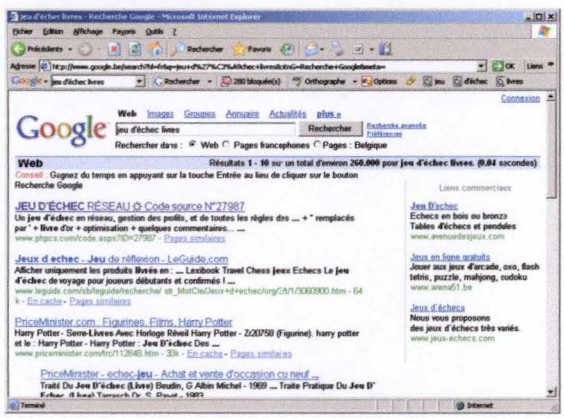


Figure 9 : recherche thématique sur Google

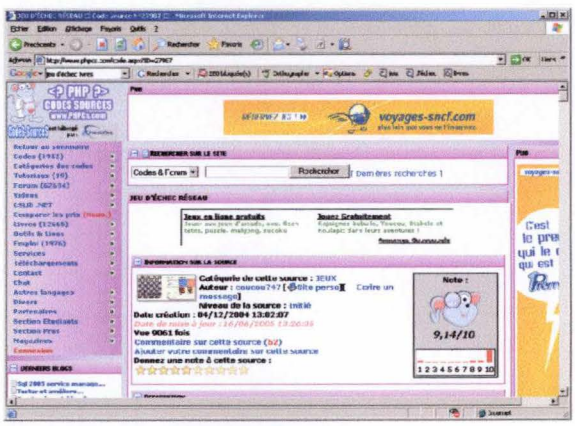


Figure 10 : page référée par Google

En analysant le flux HTTP[44], on peut constater que le site de jeu d'échec « phpcs.com » reçoit d'emblée les informations suivantes.

```
Accept-Language : fr-be
```

- l'internaute est un francophone de Belgique

```
User-Agent : Mozilla/5.0 (Windows; U; Windows NT 5.1; fr-FR; rv:1.7.12) Gecko/20050919
Firefox/1.0.7
```

- Le navigateur est Firefox version 1.0.7 pour Windows en français
- le système d'exploitation est Windows XP avec Service Pack 1

```
Referer:
http://www.google.be/search?hl=fr&q=jeu+d%27%C3%A9chec+livres&btnG=Recherche+Google&meta=
```

- avant d'aboutir sur ce site, l'internaute a effectué une recherché sur Google
- les mots-clés utilisés pour sa recherche sont « jeu d'échec livres »

En analysant un peu plus loin les paquets envoyés, on pourra constater que la page comporte des liens invisibles qui transmettent cette information à des tiers, « CS Ads » en l'occurrence (http://rp.devfr.net), vraisemblablement un fournisseur d'annonces publicitaires.

```
GET /adj.php?n=553311803
&what=zone:17
&target=_blank
&exclude=
&referer=http://www.google.be/search?hl=fr&q=jeu+d%27%C3%A9chec+livres&btnG=Recherche+Google
&meta=
Referer: http://www.phpcs.com/code.aspx?ID=27987
Host: rp.devfr.net
```

Non seulement CSAds connait les mots-clés de recherche mais il a également l'identifiant correspondant sur le site de PHPCS. En regardant du côté des cookies, on peut aussi constater la présence d'un cookie associé à rp.devfr.net.

Pour peu qu'il y ait des échanges d'informations entre PHPCS et CSAds, le lien entre l'internaute qui est tracé par rp.devfr.net est identifié sur PHPCS. A ce stade l'identification n'est pas encore nominative. Elle le devient dès que l'internaute s'enregistre sur le site pour devenir membre afin de bénéficier de certaines fonctionnalités ou services supplémentaires.

1.6.4 Historique de navigation

Les navigateurs offrent la facilité de conserver un historique des pages consultées afin de retrouver aisément une information qui a été vue sur un site visité précédemment. Cette fonctionnalité offre bien sûr une opportunité unique de collecter les informations nécessaires à la réalisation d'une étude des centres d'intérêts d'un internaute. La plupart des logiciels espions effectuent ce genre de pêche aux informations. Lorsque ceux-ci sont installés, ils ne se contentent pas de transmettre les données sur l'historique passé de l'internaute mais continuent à parasiter silencieusement le navigateur pour enregistrer et éventuellement transmettre simultanément les informations sur la navigation courante. Une fois greffé au navigateur, le spyware peut envoyer les adresses des sites visités, mais lorsque l'internaute accède à une page de type « formulaire », une copie de celui-ci avec les données entrées par l'utilisateur.

Le terme anglais « Browser junk » désigne toutes les informations qu'il est possible de trouver sur un utilisateur, ou plus précisément sur son comportement d'internaute via son outil de navigation. Dans ce cadre, l'historique de navigation n'est pas la seule source d'information. Quasi tous les navigateurs utilisent un système de mise en mémoire tampon, pour des raisons techniques de performance. Cette mémoire est appelée le « cache » du

[44] L'analyse du flux TCP/IP et HTTP a été réalisée à l'aide du logiciel libre « Ethereal – Network Protocol Analyzer » (http://www.ethereal.com)

navigateur. Elle renferme le contenu de toutes les dernières pages téléchargées avant d'être affichée à l'écran. L'historique de navigation ne contient que les adresses (« URL ») des pages visitées.

1.6.5 Le GUID

Il existe différents dispositifs qui ne sont pas directement des spywares mais qui les épaulent, le tout convergeant vers un ciblage nominatif et un traçage. C'est le cas des cookies ou des GUID dans les documents de toute nature créés par tous les logiciels des Pack Office de Microsoft et les GUID matériels relevés par les logiciels et insérés dans les logs, les transmissions etc.

GUID est un acronyme pour Globally Unique Identifier, un nombre unique qui est produit par Windows ou par toute autre application afin d'identifier un composant spécifique, une application, un fichier, un enregistrement de base de données et/ou un utilisateur.

GUID logiciel

Windows identifie des comptes par un nom d'utilisateur (ordinateur ou domaine et nom d'utilisateur) et lui assigne un GUID. Un GUID peut être créé de différentes manières, mais il y a généralement une combinaison de quelques paramètres uniques basés sur des points spécifiques dans le temps (par exemple une adresse IP, l'adresse MAC, la date et heure de l'horloge) [WWP01].

Un GUID est également utilisé dans la base de registre de Windows pour identifier les DLLs de type COM[45]. Microsoft, par exemple, utilise ce GUID pour identifier un utilisateur dans le lecteur multimédia livré en standard avec toutes les versions de Windows. Une option est accessible dans la configuration Internet du lecteur afin de désactiver ce paramètre.

GUID matériel

Outre le GUID de Windows et des applications, cette notion s'applique également sur le matériel tel que certains processeurs ainsi que des composants matériels comme les disques durs, des cartes mères ou les cartes réseaux.

MAC address

Les cartes réseaux ont depuis longtemps, pour des raisons techniques, un identifiant unique appelé « MAC address » (Media Access Control address).

Il est obligatoire qu'un utilisateur soit reconnu sur un réseau afin que les données arrivent à son attention. La seule solution pour connaître l'adresse unique et certaine d'un utilisateur sur ces réseaux a été officiellement codifiée dans la norme IEEE 802, qui date de 1970, et existe toujours. Cette adresse est liée à un code unique, écrit dans le microcode de la carte réseau de chaque ordinateur. Ce code y est écrit par le constructeur de la carte lui-même, à la fabrication de celle-ci et jamais deux cartes n'ont le même numéro. Les fabricants de carte réseau se voient attribuer des intervalles d'adresses et il n'y a aucune collision. Le revers de cette unicité absolue est que l'adresse MAC est un formidable GUID matériel, garantissant une très haute précision en espionnage des utilisateurs. Il y a un composant réseau dans chaque ordinateur, même si l'utilisateur n'en fait pas usage.

1.6.6 Cas particulier : les outils de rapport d'erreur

De nombreux programmes intègrent un outil de rapport d'erreur (en anglais « Error Reporting Tool »). Il a pour but d'intercepter les erreurs critiques d'un programme afin d'envoyer un rapport à une équipe de développement ou de maintenance qui est chargée d'en comprendre les raisons et d'y apporter un correctif. L'information envoyée est constituée d'un ensemble de données techniques propres au programme ainsi que des données relatives au contexte dans lequel l'erreur est survenue.

Ce type d'outil est conçu afin de permettre un débogage en cas d'erreur critique d'une application. Il ne constitue a priori pas un risque de type « spyware ». Cependant, de par son mode de fonctionnement et la nature des informations transmises, il mérite une attention particulière.

Ces procédures de gestion d'erreurs intégrées peuvent fournir à l'éditeur des informations à des fins de débogage. Par exemple, Internet Explorer 6 intercepte les erreurs non récupérables et prépare automatiquement un fichier de

[45] Component Object Model (COM) est le standard Microsoft pour les composants et objets répartis. Le DCOM (Distributed Component Object Model) est l'équivalant pour les systèmes distribués

données à envoyer aux services techniques de Microsoft. Ce fichier contient, entre autres, ce qui s'appelle un « dump mémoire » c'est-à-dire le vidage de la mémoire de l'ordinateur.

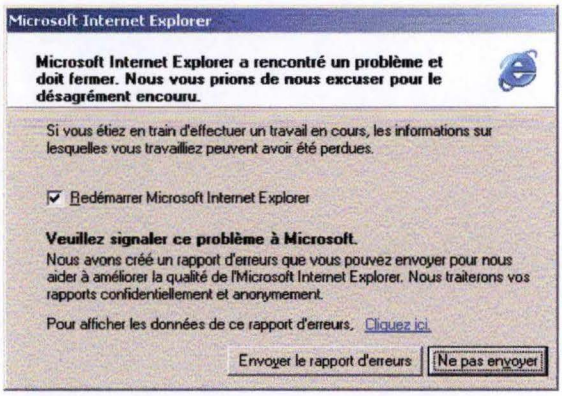


Figure 11 : Rapport d'erreur d'Internet Explorer

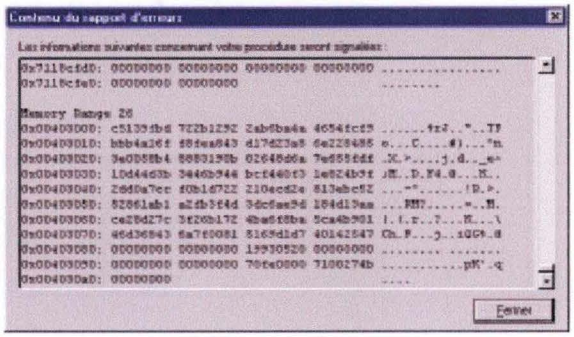


Figure 12 : exemple de dump mémoire

L'éditeur du logiciel est le mieux placé pour savoir quelles informations techniques il a besoin pour comprendre dans quelles circonstances l'un de ses programmes a pu avoir un problème critique. Ces informations se rapportent au matériel, aux autres programmes en mémoire, aux composants systèmes de l'ordinateur, au processeur, à la mémoire, etc. Ces outils de rapports sont à même de collecter des informations détaillées qu'aucun utilisateur quelque soit son niveau de connaissances techniques ne serait capable de fournir et encore moins de structurer d'une manière systématique et aisément exploitable par un service technique. [PIN05]

Il y a malheureusement des risques liés à l'envoi de ce type d'informations. Il s'agit ici d'un « dump mémoire », autrement dit, une copie intégrale de tout le contenu de la mémoire d'un ordinateur. Dans cette mémoire peuvent s'y trouver des informations confidentielles, il suffit par exemple d'utiliser un outil de gestion bancaire en ligne au moment de la constitution du dump mémoire et celui-ci contiendra peut-être les informations de compte en banque, voire les codes d'accès à la gestion du compte à distance. Il est donc recommandé de ne pas envoyer ces types de messages d'interception d'erreurs.[46]

1.6.7 Scripts

Les scripts sont des langages de haut niveau, ce qui signifie qu'ils se situent tout en haut des couches d'abstractions permettant d'accéder aux ressources des couches inférieures comme le système d'exploitation Windows et les ressources matérielles. L'assembleur par exemple est un langage de très bas niveau qui s'adresse directement au matériel. L'écriture de code dans un langage de haut niveau est relativement facile mais rencontre certaines limitations, à l'inverse des langages de bas niveau qui permettent de tout faire mais à un autre niveau de difficulté. Plus le niveau est élevé, plus il existe de couches d'abstraction entre le langage et le matériel. C'est ainsi qu'un script peut s'exécuter sur des systèmes d'exploitation différents.

Le but initial des scripts est notamment d'introduire une certaine interactivité entre un document et les applications de son environnement. Avant l'arrivée des scripts dans le contexte Web, les documents étaient statiques, ce qui est le cas pour les pages écrites purement en HTML. Les langages de scripts permettent de spécifier comment les documents vont prendre forme dynamiquement par rapport à l'environnement.

Les langages de script les plus répandus sont le JavaScript, le VBScript et les macros.

JavaScript

JavaScript a été créé en 1995 par Brendan Eich pour Netscape Communications Corporation. Il est apparu pour la première fois dans les versions bêta de Netscape Navigator 2.0. D'abord appelé LiveScript, il a été rebaptisé JavaScript et est décrit comme un complément à Java.

Le but de JavaScript est de manipuler de façon simple des objets logiques fournis par une application hôte. Du code JavaScript peut être intégré directement au sein des pages Web, pour y être exécuté sur le poste client. C'est alors le navigateur Web qui prend en charge l'exécution de ces petits bouts de programmes. Généralement,

[46] Le risque lié aux Rapports d'Erreurs de Microsoft fait l'objet d'un bulletin d'alerte au Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA), un organisme dépendant du ministère de la défense nationale française (http://certa.ssi.gouv.fr).[CER01]

JavaScript sert à contrôler les données saisies dans des formulaires HTML, ou à interagir avec le document HTML via l'interface du navigateur (on parle alors parfois d'HTML dynamique). C'est ainsi par exemple qu'un lien change d'aspect lorsque le pointeur de la souris passe dessus ou qu'une fenêtre s'ouvre automatiquement (dont les pop-ups).

JavaScript est aujourd'hui défini par la norme connue sous l'appellation ECMAScript. Son implémentation par Microsoft porte quant à elle le nom de JScript .

VBScript

Le VBScripts est une extension pour scripts du langage Visual Basic de Microsoft. VBScript est exploitable dans une page Web pour y intégrer les mêmes fonctionnalités que Javascript. Il est cependant utilisé dans un cadre plus large que le script web.

Les Macros

Nombreuses applications disposent d'un langage propre, au départ conçus dans le but d'automatiser des tâches répétitives, les macros se sont vues rapidement élargir leur champ d'action.

Les logiciels de la série Office de Microsoft, Word, PowerPoint et Excel par exemple peuvent être exploités de manière interactive dans des pages Web. Les tableaux écrits dans des pages Web sont généralement statiques mais il est possible d'y insérer l'interactivité Excel. Si les macros Word ou Excel sont insérées dans ce type de pages, elles seront chargées sur l'ordinateur en même temps que les pages visitées et seront en temps réel interprétées par le navigateur ou l'exécutif du logiciel d'origine présent sur l'ordinateur (le pack office de Microsoft en l'occurrence) ou ajoutées en tant qu'extension du navigateur.

Conséquences

Les langages de scripts et les scripts sont indispensables mais ils sont trop puissants ou trop permissifs. Ils permettent à quelques-uns, dont les pirates et les espions, toutes formes d'investigations ou de malveillances intrusives et / ou destructives.

1.6.8 ActiveX

Certains espions cherchent à s'installer automatiquement sur le poste de l'internaute au moyen de la technologie ActiveX. ActiveX est la troisième génération de la technologie OLE (Object Linking and Embedding). L'idée de départ de cette technologie étant de permettre à des programmes d'exécuter d'autres programmes à l'intérieur d'eux-mêmes. Ainsi, dans une page HTML, quand on rencontre un lien qui pointe sur un fichier PDF[47], ce fichier PDF va s'ouvrir directement dans le navigateur. ActiveX a été pensé pour permettre à différents logiciels écrits par des sociétés différentes de communiquer entre eux. [GRE03]

ActiveX n'est qu'une bibliothèque de commandes utilisables par les logiciels, on parle de contrôle ActiveX. Aujourd'hui un contrôle ActiveX sert essentiellement à insérer dans les pages Web des fichiers multimédias ou des documents réalisés avec des applications bureautiques comme Word ou Excel. On peut également faire afficher le disque dur ou voir une vidéo dans une page HTML.

Comme ActiveX se veut le concurrent de JavaScript (de Sun Microsystems), Microsoft n'a fixé aucune limite aux contrôles ActiveX, qui peuvent accéder à toutes les ressources matérielles et logicielles de l'ordinateur. Conscient du manque de sécurité introduit par cette technologie, Microsoft à mis en place un système de certification pour les contrôles ActiveX.

Certains sont soumis par leurs auteurs à des organismes certificateurs et ces certificats numériques sont vérifiés lorsque le contrôle est utilisé pour la première fois par une page du navigateur. Mais comme la conception de ces contrôles est libre, il existe donc 2 types de contrôles ActiveX, les « certifiés » et les « non certifiés » qui peuvent se révéler dangereux. Les contrôles non certifiés ne devraient jamais être acceptés d'autant plus qu'ils s'installent et s'exécutent, comme n'importe quel programme [GRE03].

Internet Explorer est configuré par défaut pour refuser les ActiveX non certifiés et demander à l'utilisateur l'installation d'un ActiveX certifié.

---

[47] Le format Adobe® PDF (Portable Document Format) est un standard ouvert utilisé par les organismes de normalisation du monde entier pour garantir la sécurité et la fiabilité de la diffusion et des échanges de documents électroniques.

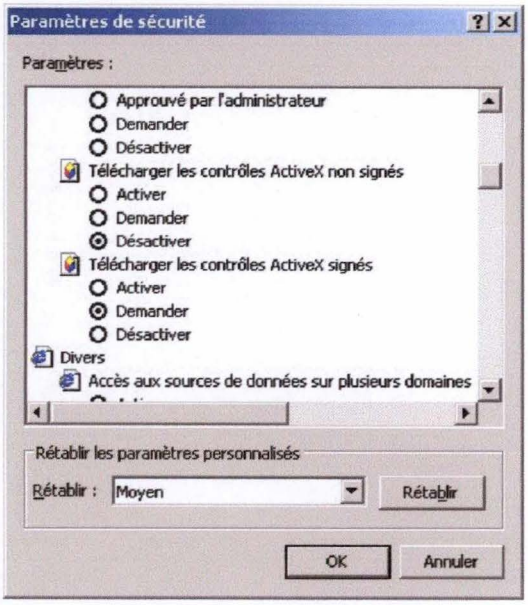


Figure 13 : Paramètres de sécurité IE ActiveX

Figure 14 : Installation d'un ActiveX signé

La signature numérique permet de vérifier l'auteur d'un fichier et que le fichier n'a pas changé depuis qu'il a été signé numériquement. Attention qu'une signature numérique valide ne vérifie pas que le contenu du fichier est inoffensif.

Dans ces différents produits indésirables utilisant les technologies ActiveX, on va en trouver de plusieurs types. Les plus courants sont les Browser Helper Objects, les hijackers et les dialers. Ceux-ci sont décrits ci-après.

Browser Helper Object (BHO)

Les Browser Helper Objects (BHO) sont conçus à l'origine pour être des petits programmes additionnels à Internet Explorer qui vont s'exécuter ensuite automatiquement chaque fois que l'on va utiliser le navigateur. Le BHO se présente généralement, lorsqu'il est visible, comme un ou plusieurs boutons ou une barre de boutons ajoutés au menu du navigateur. C'est cependant souvent une fonction cachée qui va être installée à l'insu de l'utilisateur. Beaucoup sont des espions servant à suivre les déplacements sur Internet ou des outils publicitaires servant à afficher des publicités [WAZ05].

Pirates de navigateurs (hijackers)

Les pirates de navigateurs (en anglais « hijackers ») sont des petits programmes ou des entrées dans la base de registre qui modifient le comportement du navigateur Internet Explorer.

Ils peuvent par exemple :

- changer la page de démarrage et/ou la page de recherche,
- forcer l'ouverture de la page en plein écran en masquant la quasi totalité des barres de boutons,
- modifier les paramètres d'acceptation des contrôles ActiveX,
- faire d'un site un site de confiance à l'insu de la personne, ce qui permettra de contourner les contrôles de sécurité.

Les pirates intelligents changent non seulement les pages de démarrage et de recherche, mais en plus ajoutent un petit fichier qui rétablira les réglages piratés à chaque démarrage du système[48].

[48] Aide en ligne de « Spybot Search & Destroy », http://www.safer-networking.org/fr/dictionary/hijacker.html (consulté le 20 juin 2005)

Composeurs téléphoniques (dialer)

Les composeurs téléphoniques (en anglais « dialers ») sont des programmes qui établissent une communication téléphonique depuis l'ordinateur vers un site extérieur, la communication, souvent surtaxée, étant à la charge de l'utilisateur. Ce type de programme est habituellement téléchargé automatiquement lors des visites de pages web douteuses, typiquement des sites pornographiques ou des sites offrant des téléchargements ou des logiciels illégaux, comme par exemple, des outils de craquage ou des numéros de série d'applications [IDN03].

Ce type d'ActiveX est généralement classé parmi les virus de la famille des chevaux de Troie ou des vers.

1.6.9 Les keyloggers

Les enregistreurs de frappe au clavier (en anglais « keyloggers »), qui peuvent être matériels ou logiciels, ont pour fonction d'enregistrer furtivement absolument tout ce qu'un utilisateur tape sur un clavier d'ordinateur. La plupart des keyloggers enregistrent également le nom de l'application en cours, la date et l'heure à laquelle elle a été exécutée ainsi que les frappes de touches associées à cette application. Leur capacité à enregistrer véritablement touche par touche tout ce qui est tapé sur un clavier -et ce avant qu'aucune opération de chiffrement n'ait eu lieu- donne accès aux phrases et mots de passe et autres données habituellement bien dissimulées.

Les keyloggers matériels[49] sont des dispositifs reliés à un clavier d'ordinateur qui enregistrent les données. Ces dispositifs ressemblent généralement à un adaptateur standard de clavier; ils peuvent de fait être difficiles à repérer si on ne les recherche pas spécifiquement. Afin de récupérer les informations enregistrées dans un keylogger matériel, l'instigateur de la surveillance doit y accéder physiquement. Les keyloggers matériels enregistrent les données localement et n'ont généralement pas la faculté de diffuser ou de faire transiter et sortir les données via un réseau.

Les keyloggers logiciels sont beaucoup plus répandus parce qu'ils peuvent être installés à distance (via un réseau, par le biais d'un troyen ou d'un virus), et ne nécessitent donc pas un accès physique à la machine pour la récupération des données collectées. Les keyloggers logiciels ont souvent la faculté d'obtenir bien plus de données que les keyloggers matériels parce qu'ils ne sont pas limités par la taille physique de leur mémoire [WBB05].

1.6.10 La capture d'écran

La capture d'écran (en anglais « snapshot ») des images de l'activité de l'utilisateur est en quelques sortes une photographie de l'écran de l'utilisateur à un moment donné. Pour que cette technique soit efficace, la photo est prise à intervalles réguliers. Cette méthode de capture d'information est généralement couplée à un keylogger afin de compléter l'information saisie par ce dernier.

1.6.11 Les messageries

Certains spywares sont capables de se greffer aux outils de messagerie instantanée les plus utilisés comme par exemple ICQ[50], AIM (AOL Instant Messenger)[51], MSN Messenger[52], Yahoo Messenger[53]. Ils fonctionnent non seulement avec ces produits mais également avec une grosse partie des programmes qui utilisent le même protocole de communication, par exemple, pour ICQ, il existe différentes variantes implémentant ce protocole de communication : Trillian[54], Miranda[55], SIM[56], IM2[57], etc. Une fois installés, ces spywares écrivent le contenu de tous les échanges dans des fichiers cachés quelque part sur le disque de l'utilisateur ou directement transmis à un serveur qui ne manquera pas de les réceptionner.

---

[49] Les produits KeyKatcher et Key Ghost qui sont les deux modèles les plus répandus sur le marché. KeyGhost fabrique aussi des claviers avec keylogger intégré, ce qui en rend la détection bien plus difficile. Comme ce sont des dispositifs de type matériel, KeyKatcher et KeyGhost ne peuvent être détectés par les logiciels anti-spyware, anti-viraux ou de sécurisation du poste de travail.

[50] ICQ de ICQ Inc. (http://www.icq.com)

[51] AIM de America On Line (http://aim.aol.fr)

[52] MSN Messenger de Microsoft (http://go.msn.fr/sas/messenger/msn.asp)

[53] Yahoo Messenger de Yahoo! Inc. (http://messenger.yahoo.com)

[54] Trillian de Cerulean Studios (http://www.ceruleanstudios.com)

[55] Miranda Instant Messenger de Miranda IM (http://www.miranda-im.org)

[56] SIM (Simple Instant Messenger) est un produit open source qui s'inscrit comme client ICQ (http://sim-icq.sourceforge.net)

[57] IM2, Instant Messenger 2 (http://www.im2.com)

Outre les outils de messagerie instantanée, il existe également des produits qui enregistrent toutes les conversations écrites sur les canaux de discussion de type IRC (« Internet Relay Chat »). A l'instar des outils de messagerie instantanée, il existe différents produits qui se basent sur ce même protocole de communication IRC comme par exemple mIRQ[58], ViRC (Visual IRC)[59], Bersirc[60], HydraIRC[61], Xchat, etc.

D'autres spywares peuvent lire tout ce qui passe par les protocoles de messagerie (POP3, IMAP ou SMTP).

Les spywares utilisant ces sources d'information enregistrent généralement tout ce qui circule sur le réseau tel les reniffleurs (en anglais « sniffer ») et filtrent le contenu afin de le structurer et le rendre plus lisible. Ce type d'information est plus difficilement exploitable de manière automatique. Ce genre de pratique est plus souvent associé à l'espionnage et la surveillance individuelle qu'au traitement de masse, bien que celui-ci soit toujours possible.

Pour avoir un aperçu des fonctionnalités offertes par de tels espions, un bon exemple est le produit WebMail Spy édité par ExploreAnywhere[62] :

- enregistrement des mails en POP3/SMTP,
- enregistrement des web mail tels que Hotmail, Yahoo!Mail, ICQ Mail, AOL Mail, Netscape Mail et bien d'autres,
- invisibles dans la liste des tâches,
- démarrage automatique,
- mise à jour automatique.

1.6.12 Backdoor

Un backdoor, en français "porte dérobée", exploite les vulnérabilités de logiciels installés afin d'obtenir un accès distant sur un ordinateur, en faisant fi des mécanismes de sécurité implémentés sur le système. Les spywares de type backdoor sont généralement secrètement installés par des virus, vers (en anglais « worms »), ou parfois des adwares malicieux.

Comme son nom le suggère, un backdoor agit sournoisement, se rendant très difficile à déceler et neutraliser sans utiliser de logiciels anti-spyware ou anti-virus.

[58] mIRC de mIRC Co. Ltd. (http://www.mirc.com)

[59] Visual IRC de MeGALiTH (http://www.visualirc.net)

[60] Bersirc est un produit open source (http://www.bersirc.com)

[61] HydraIRC (http://www.hydrairc.com)

[62] Exploreanywhere WebMail Spy (http://www.exploreanywhere.com/wms-features.php)

1.7 Modes de communication

Les spywares de par leurs natures et objectifs, doivent communiquer un moment où l'autre avec le serveur pour le compte duquel ils travaillent. Leur but, rappelons-le est généralement de collecter de l'information pour la délivrer à un tiers, tels qu'une agence de marketing, une régie publicitaire ou tout autre exploitant.

La communication peut s'établir de plusieurs manières différentes.

1.7.1 Transmission en temps réel

Les données peuvent être transmises en temps réel. Ce qui signifie que des lots d'informations sont transmis tant que la connexion est ouverte avec l'Internet. On constate que de plus en plus d'ordinateurs sont connectés sur l'Internet au moyen de lignes à haut débit (ADSL, câble de télédistribution, etc.). Or, l'utilisateur de ce type de connexion n'est pas regardant quant à la durée de connexion comme il le serait avec un modem analogique pour lequel il paie à la durée de communication avec son fournisseur d'accès.

La ligne à haut débit est propice au transfert d'informations en tâche de fond par un spyware car la perte de débit est souvent négligeable par rapport au taux de transfert supporté par une telle ligne. Les performances de la connexion peuvent cependant rapidement se dégrader par l'accumulation des différents agents espions qui transfèrent chacun leurs petits lots d'information à leur manière. Il peut également arriver que certains espions transmettent des flux de données de taille considérables, par exemple dans le cas d'envois d'impressions d'écrans ou d'enregistrements sonores. Dans ce cas, les éditeurs trouvent généralement un leurre qui tente de convaincre l'utilisateur crédule que les informations transmises sont légitimes.

Il existe un bon exemple d'espion qui camoufle son usage de bande passante, il s'agit du cas du couple de spywares « VX2 » et « Sputnik ». VX2 est un programme qui est livré par exemple avec un économiseur d'écran téléchargeable gratuitement sur Internet. Lorsque VX2 est installé sur un système, il installe son compagnon dénommé « Sputnik ». VX2 ouvre des pop-ups publicitaires et établi un profil d'utilisateur sur base des informations qu'il collecte sur son hôte. Sputnik quant à lui se charge de l'envoi des informations traitées par VX2. La subtilité de ce couple VX2 - Sputnik réside dans le fait que les pop-ups envoyés à l'utilisateur par VX2 ne proviennent pas d'un téléchargement sur un serveur de publicités, mais sont stockées localement. L'utilisateur suppose alors que la bande passante est consommée par le téléchargement des pop-ups publicitaires alors qu'en réalité celle-ci est complètement utilisée par Sputnik pour l'envoi des données collectées.

1.7.2 Transmission différée

Attente d'une connexion

Certains logiciels espions sont à l'affût d'une connexion à l'Internet pour démarrer leur transfert d'information vers les serveurs toujours prêts à la réception.

E-mail

Le logiciel espion peut transmettre les informations récoltées par courrier électronique, en utilisant la messagerie de l'utilisateur. Cette méthode de transmission de données se fait généralement par le biais du système de messagerie le plus répandu : Microsoft Outlook (ou Outlook Express), qui est installé par défaut avec Windows depuis ses premières versions.

Dialer

Le composeur téléphonique (en anglais « dialer ») est un programme qui se connecte seul à Internet en utilisant un modem branché sur une ligne téléphonique. La connexion se fait généralement sur des sites à taux de facturation élevés. Ces programmes changent les paramètres de connexion à l'Internet à l'insu de l'utilisateur et attend simplement que l'utilisateur établisse sa connexion, ou bien se connecte de lui-même. Le dialer est bien souvent mis en place par l'utilisateur de l'ordinateur lors d'une demande d'accès à un jeu soit disant gratuit ou à un site pornographique qui propose de charger un fichier et de se reconnecter.

1.7.3 Remarque sur le chiffrement

Les informations collectées par un processus d'espionnages logiciel sont souvent compactées et cryptées. Elles sont compactées afin d'optimiser le temps et l'usage de la bande passante lors de la transmission des données au destinataire. Elles sont chiffrées afin de dissimuler le type de contenu de ces informations, et ainsi rendre plus difficile leur détection.

1.8 Modes de propagation

1.8.1 Installation pseudo-consentie

La majorité des logiciels espions s'installent avec un accord des utilisateurs, généralement mal éclairés. La plupart installent des outils pseudo-gratuits sans se soucier que ceux-ci soient accompagnés d'espions.

La législation en matière de protection de la vie privée s'est endurcie ces dernières années. C'est pourquoi on a vu apparaître dans la plupart des conditions d'utilisation (« EULA : End User License Agreement ») des produits distribuant des logiciels espions, une clause sur la confidentialité des données et le respect de la vie privé (« Privacy statement »). Les utilisateurs ne prennent cependant pas la peine de consulter ces clauses, lorsqu'elles existent car ce n'est pas toujours le cas. On voit ainsi KaZaA afficher, outre un gros logo « NO SPYWARE », la liste des logiciels qui accompagnent le produit. Des logiciels espions figurent parmi ceux-ci mais KaZaA se décharge de toute responsabilité en affirmant qu'ils ne collectent, eux, aucune information personnelle et ne sont pas responsables du traitement des informations fait par Cydoor par exemple.

La majorité des produits intrusifs se retranchent derrière une subtilité du langage et une imprécision juridique. Ils déclarent tous ne collecter que des informations non personnelles sous forme agrégées à des fins statistiques ou démographiques.

C'est donc en profitant de l'ignorance ou de la négligence des utilisateurs que la majorité des logiciels s'installent sur les ordinateurs.

1.8.2 Zombie bots

Certains espions sont installés à l'insu des internautes à l'aide de failles de sécurité. 2004 et 2005 auront été des années témoins d'une nouvelle tendance, beaucoup plus rentable pour certains escrocs. Il s'agit du déploiement de client-robots (en anglais « bots ») sur des PC dont on a pris le contrôle à distance, ceux-ci constituent des réseaux de robots (en anglais « botnets ») installés sur des PC dits « zombies ». Le but de cette technique est de faire de l'argent, en louant des réseaux de bots pour relayer du spam par exemple. Les machines infectées contiennent aussi des données personnelles qui peuvent se vendre. Pour rentabiliser son programme, l'auteur limite donc au maximum la visibilité du bot. Une des techniques pour allonger artificiellement la fenêtre d'opportunité consiste pour les créateurs à tenter de ralentir l'analyse, par exemple en évitant d'envoyer des mails aux éditeurs d'antivirus. Ils jouent aussi sur la multiplication des variantes. Une technique commence d'ailleurs à revenir, celle du polymorphisme qui modifie le virus en se déployant, empêchant certains modes de détection.

Ainsi, selon le directeur de la sécurité de Microsoft France, Bernard Ourghanlian, la taille moyenne des réseaux de bots, en avril 2005, se situent entre 3 000 et 10 000 machines. Des chiffres confirmés par Symantec et une étude menée par Honeynets[63].

On peut lire dans un article publié en juillet 2005 dans The Register[LEY05] : « McAfee AVERT[64] rapporte que les bots propagateurs de spams, adwares et spywares ont été leur principale préoccupation en début 2005. Les zombies bots tels que Gaobot, MyTob et SDbot constituent un point central de distribution de logiciels espions. »

---

[63] The Honeynet Project & Research Alliance, Know your Enemy: Tracking Botnets, http://www.honeynet.org/papers/bots (mis à jour le 13 mars 2005)

[64] AVERT est un département de McAfee (Anti-virus and Vulnerability Emergency Response Team)

1.9 Les faux outils anti-spyware

Il existe une effarante quantité de faux utilitaires de sécurité agissant en véritables chevaux de Troie introduisant un ou plusieurs parasites, espionnant, installant des failles de sécurité tels que des portes dérobées et des composeurs téléphoniques.

La majorité des sites pornographiques proposent un anti-spyware, payant et généralement très cher, qui n'est souvent qu'un installateur de dialers. Cet outil tente de détruire les dialers de leurs concurrents pour installer le leur à la place.

Sans devoir aller sur les sites à caractère pornographique, une multitude de sites d'éditeurs de spyware fonctionnent de la même manière en proposant un outil anti-spyware payant. Dans ce cas, ce n'est pas l'installation de dialer mais l'installation de leur propre espion qui est visé.

Il faut également faire attention à certains faux sites qui exploitent des noms de domaines proches de ceux très visités ou jouant sur les fautes de frappe des internautes sur leurs claviers. Par exemple la recherche du site de l'éditeur du firewall ZoneAlarm, Zone Labs, conduit souvent à l'erreur de chercher, logiquement, le site http://www.zone-labs.com, hors ce site existe et n'est pas le site de ZoneAlarm. Il contient juste une redirection immédiate vers un site marchand américain (Netster) qui installe Gator.

1.10 Informations ciblées

Les informations volées sont difficiles à identifier car, si les sniffers détectent, dans les paquets transmis vers le Net, des données vers tel ou tel serveur que l'on sait appartenir à une société pratiquant ce genre de collecte, les données elles-mêmes sont souvent compactées et cryptées. On ne peut donc se fier qu'aux listes de données déclarées collectées par les sociétés gérant ces espions, dans leur « Déclaration de protection de la vie privée » (« privacy policy ») sur le site de l'éditeur du spyware ou de l'éditeur du logiciel embarquant un ou plusieurs spywares. Ces pages, lorsqu'elles existent, ont un contenu très variable qui peut être intéressant. Bien entendu, elles déclarent toutes en préambule que leurs sociétés sont très préoccupées par la vie privée des utilisateurs, attentives et vigilantes avec ces données, puis elles donnent, quelquefois, une petite liste des données rapatriées, liste surabondantes de « etc. », « entre autres », « non limitativement », « par exemple ». Quelquefois, un extrait de cette page est noyé dans les conditions générales de cession de droit d'usage du logiciel hôte que l'on installe, conditions générales que personne ne lit car :

- Il faut un temps fou pour les lire, sans rien y comprendre, même lorsqu'elles sont en français, alors que l'on a hâte d'installer le logiciel que l'on vient d'acheter ou de télécharger
- Si on n'est pas d'accord avec les conditions générales, le logiciel ne s'installe pas (mais, quelquefois, les spywares eux, s'installent quand même).

L'analyse de paquets sur le réseau permet de voir les adresses IP des serveurs par lesquels transitent les informations. Les Who'is[65] disponibles sur le Net permettent parfois de se faire une idée sur les intermédiaires. Cela permet quelquefois, de s'apercevoir que c'est totalement opaque ou qu'il s'agit d'une société dans un pays à la législation laxiste ou inexistante.

Les informations visées, qui peuvent être transmises en une fraction de seconde sont par exemple :

- les URL (adresses) des pages Web visitées avec quel navigateur : il suffit aux robots de lire ensuite ces pages pour en extraire les Mots-clés et connaître les centres d'intérêts, le profil personnel, social et psychologique,
- les informations sur la navigation actuelle et historique,
- les informations dans les formulaires en ligne remplis et envoyé par l'utilisateur,
- les mots utilisés dans les requêtes sur les moteurs de recherche,
- les sites sur lesquels un utilisateur accède par l'intermédiaire des annuaires de recherche,

[65] Whois est un service de recherche fourni par les Registres Internet régionaux ou bien les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine.

- l'adresse IP de l'ordinateur[66],
- un numéro identifiant unique, le GUID, contournant la volatilité des adresses IP et des surfs anonymes,
- le ou les cookies du site mais aussi les autres cookies (un spyware est un véritable programme à part entière contrairement à un site internet qui lui ne peut lire que le ou les cookies de son site),
- Le type de navigateur, sa version, sa licence, sa langue,
- le système d'exploitation, sa version, sa langue, sa licence,
- la résolution d'écran et le nombre de couleurs utilisées,
- la puissance processeur, sa marque, son modèle,
- les périphériques,
- les logiciels installés (bureautiques, jeux, utilitaires... tous - il semble que dans plusieurs cas de figure - dont les connexions sur les sites de Microsoft - ce soit la totalité de la base de registre qui soit envoyée c'est-à-dire tous les logiciels, toutes les clés, etc.).

De l'aveu même de Microsoft, à propos de XP Passport qu'on est habilement et obligatoirement amenés à utiliser (technologie Hailstorm, Hotmail, Msn, Kid's Passport, activations et enregistrements des composants logiciels et matériels de vos ordinateurs ...), la liste des informations échangeables par ce biais est incroyable tant l'outil est performant :

> Available information: person's home telephone number, office telephone number, fax number, home address, business address, and geographic locations; a person's actual name, nickname, birth date, anniversary, other special dates, and personal photograph; a complete list of all names of all contacts contained in an electronic date book, including names, addresses, contact dates, and personal details for all friends and associates; information concerning location and contact information; all forms of incoming mail, including voicemail, electronic mail, and fax mail; tracking information; personal and business documents; favorite websites and other identifiers; receipts, payment instruments, coupons and other transaction records, devices settings and capabilities across all platforms, including PC, PDA, and telephones; and detailed usage reports for each one of these services.

Figure 15 : Hailstorm, available information

Les informations récoltées peuvent varier à l'infini.

Les fichiers de renseignements ainsi constitués sont vendus à prix d'or à des sociétés commerciales ou de marketing. Les 3 Suisses ou La Redoute, les constructeurs automobiles, les compagnies d'assurances, la grande distribution, les voyagistes, les marchands de biens, les banques sont des acheteurs potentiels énormes des fichiers constitués par Radiate, XP Passport, Hailstorm et consorts.

---

[66] L'adresse IP n'est pas un identifiant car l'adresse IP change chaque fois qu'on se connecte au Net: elle est attribuée de manière dynamique et temporaire pour le temps d'un surf mais si la connexion est de type haute vitesse -ADSL ou câble par exemple- on a tendance à rester connecté en permanence et l'adresse IP change peu. D'un point de vue juridique, il n'a toujours pas été déterminé si cette adresse IP constituait une donnée à caractère personnel. Il est vrai également qu'une adresse IP est attribuée à un moment donné par un fournisseur d'accès qui possède les informations personnelles de l'utilisateur. C'est de cette façon que la police peut parfois retrouver un utilisateur à partir de l'adresse IP d'un ordinateur.

1.11 Aspect légal

La Belgique, comme les autres pays de l'Union européenne, dispose d'une législation sur la protection de la vie privée qui prévoit des conditions à la collecte de ces informations. Chaque pays a adopté une loi de ce type afin de transposer une directive européenne de 1995 relative à la protection des données à caractère personnel.[67].

La loi sur la protection des données à caractère personnel, est d'assurer un équilibre entre la libre circulation des données à caractère personnel, et les droits des personnes concernées par ces traitements à les contrôler, voire à s'opposer que des données nous concernant soient traitées.

S'il existe des actions conscientes d'enregistrement de données, notamment lorsqu'un utilisateur remplit un formulaire en ligne, ou lorsqu'il participe à un forum, on a vu qu'il existe toute une série de techniques qui permettent de collecter des données à l'insu de l'internaute.

Donnée à caractère personnel

Une donnée à caractère personnel est une information sur une personne physique.

Toute information a un caractère personnel, lorsqu'on peut faire un lien raisonnable entre cette donnée ou un ensemble de données et une personne physique. Par conséquent, une donnée est anonyme lorsqu'on ne peut établir ce lien de manière raisonnable. Cette recherche doit pouvoir être réalisée in abstracto, et donc quels que soient les moyens dont bénéficient l'internaute.

Ainsi, un numéro de sécurité sociale, une plaque de voiture, une photo, une adresse IP, tous les éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale (rajoute la loi), sont des données à caractère personnel.

Une des techniques qui est le plus souvent citée parmi les défenseurs du droit à la vie privée, est celle des cookies à des fins de profilage. Mais toutes ces données collectées par les cookies sont souvent techniques, et ne permettent pas automatiquement d'identifier l'internaute, mais plutôt tel internaute ayant tel numéro d'identification.

Selon une loi du 8 décembre 1991, il faut que les données permettent d'identifier une personne. Ainsi un visiteur d'une page Web peut être reconnu par le cookie comme étant le numéro x, ayant une adresse IP x.x.x.x. La jurisprudence a déclaré qu'une adresse IP était une donnée à caractère personnel, car elle permet d'identifier raisonnablement l'internaute.

Traitement

La loi précise qu'un traitement, est toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou tout autre forme de mise à dispositions, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel

Légitimité

Un traitement de données à caractère personnel requiert le consentement de la personne concernée.

Ce consentement doit être une manifestation d'une volonté libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

D'une part, la légitimité d'un traitement est conforme, lorsque les données collectées sont compatibles avec la finalité du traitement. C'est à dire que les données sont adéquates, pertinentes et non excessives, et tout cela en fonction de cette finalité. Pour cette raison, la finalité doit être déterminée et explicite. On ne peut collecter des informations qui n'ont rien à voir avec la finalité du traitement. Il faut donc toujours vérifier, lors d'un remplissage d'un formulaire, que les données demandées soient bien pertinentes avec la finalité du traitement.

D'autre part, les données doivent être exactes et de qualités. Il faut des données mises à jour. On ne peut pas garder des données d'anciens clients, qui n'ont plus rien à voir avec la gestion actuelle des dossiers en cours. Lorsqu'un dossier est terminé, les données relatives à un client doivent être retirées, sauf son accord. Ainsi, lorsque la finalité pour laquelle les données ont été collectées a été réalisée, toutes les données doivent être retirées, sauf s'il s'agit d'un traitement dont la finalité est du direct marketing.

---

[67] Commission de la vie privée (http://www.privacycommission.be)

Un traitement pour être légitime, doit être loyal et licite.

- Loyal, parce que la personne concernée doit être informée de la collecte des données la concernant, le destination de ces données doit être précisée.
- Licite, le respect de la loi sur la vie privée, ne se soustrait pas au respect de la législation en général. Elle n'entraîne pas l'autorisation du médecin à violer le secret médical, même avec l'accord de la personne concernée.

Principe de la transparence

Les personnes concernées par un traitement doivent pouvoir savoir ce que contiennent précisément toutes les données qui ont été collectées. C'est le principe du « qui sait quoi et sur quoi ». En fait, le principe de la transparence est lié au principe de ne pas tout interdire. C'est la libre circulation des données, mais en contre partie, on est tenus de laisser les personnes concernées le droit d'accéder, de rectifier et de s'opposer à la collecte de ces données.

Données sensibles

Les dispositions de l'article 6 interdisent le traitement des données à caractère personnel « qui révèlent l'origine raciale ou éthique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle ». Il s'agit manifestement de données trop personnelles pour constituer un traitement sans porter atteinte à la personne.

Le législateur a toutefois autorisé certaines exceptions à cette interdiction :

- lorsque la personne concernée a donné son consentement par écrit (ce consentement doit être libre, spécifique et informé)
- lorsque le traitement est nécessaire en raison d'obligations en matière de droit du travail ;
- lorsque le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ;
- lorsque le traitement est effectué par une fondation, une association ou tout autre organisme à but lucratif et à finalité politique, philosophique, religieuse ou syndicale (uniquement pour les données applicables)

Une violation de ces droits implique une infraction pénalement punissable. La législation en matière de protection de la vie privée est complexe et controversée. Une simple introduction à la législation en la matière est abordée, celle-ci étant du ressort de juristes.

Chapitre 2 Solutions anti-spyware

2.1 Détection

La première étape, la plus importante dans le processus de détection et d'éradication des logiciels espions est de prendre conscience qu'on est exposé à un tel risque et qu'il vaut la peine d'investiguer sur la présence éventuelle de spywares sur son ordinateur.

Typiquement, on soupçonne la présence d'un spyware lorsque la connexion Internet devient plus lente que d'habitude, même avec une connexion à haut débit. Il y a également d'autres symptômes qui pourraient laisser croire à la présence d'un logiciel espion sur un ordinateur, par exemple lorsque :

- la page de démarrage a changé,
- l'ordinateur semble consommer plus d'activité CPU et de plus nombreux accès disque de d'habitude,
- des bannières de publicité apparaissent plus fréquemment malgré l'utilisation d'outils de blocage,
- l'ouverture des pages Web semble arbitraire, le navigateur n'ouvre pas certaines pages demandées par l'utilisateur, systématiquement ou de manière aléatoire,
- une nouvelle barre d'outils de recherche[68] apparaît ou l'ancienne est remplacée,
- de nouvelles icônes apparaissent dans la barre de tâche,
- le logiciel anti-spyware ou anti-virus est coupé ou ne fonctionne pas correctement.

Ces indices devraient inciter un utilisateur conscient du risque des logiciels espions à soupçonner la présence d'un ou plusieurs de ceux-ci sur son système.

2.2 Les méthodes anti-spyware

2.2.1 Vigilance

Une solution qui vient à l'esprit de l'utilisateur moyen est d'éviter l'installation de spywares en étant vigilant sur ses habitudes d'utilisation. Cette solution simpliste est actuellement inefficace. Les logiciels espions sont tellement répandus que même les utilisateurs expérimentés disposant d'un système sain ne peuvent s'en tenir là pour éviter l'infection. De plus, cette approche est manifestement inappropriée pour les entreprises où les utilisateurs installent imprudemment de nouveaux programmes sur leurs systèmes sans disposer d'informations appropriées et sans penser à poser les questions nécessaires. La plupart du temps, les utilisateurs n'ont même pas conscience qu'un programme de spyware a été installé lors de leur navigation Web.[ALA04]

2.2.2 Eradication individuelle

On peut tenter d'éradiquer chaque spyware en utilisant les procédures spécifiques à chacun de ceux-ci. Chaque malveillance, même si son éditeur n'a jamais documenté une procédure d'éradication, peut être effacée d'une manière plus ou moins complexe. Ces procédures sont quelquefois données par les éditeurs des spywares eux-mêmes, sous la contrainte d'une décision de justice ou sous la levée de boucliers des utilisateurs. Elles sont alors volontairement très techniques et complexes à mettre en œuvre, voire dangereuses.

La méthode d'élimination d'un spyware est très variable. Certains fournissent des procédures de désinstallation, d'autres restent les plus discrets possibles tant durant leur exécution que sur la possibilité de s'en débarrasser.

Désinstallateur

Certains spywares prévoient un utilitaire de désinstallation appelé également désinstallateur (« uninstaller » en anglais). Celui-ci est généralement accessible par un raccourci créé dans le menu de démarrage des programmes. Attention que certains désinstallateurs laissent de nombreux fichiers sur le disque, parfois suffisamment que pour permettre de se réinstaller automatiquement plus tard.

[68] En anglais « Search Toolbar »

Ajout / suppression de Programmes de Windows

Certains logiciels espions utilisent la méthode d'installation et désinstallation commune à la plupart des applications Windows. Dans ce cas il est possible de le supprimer simplement en le sélectionnant dans la liste des programmes à supprimer via la commande **Ajout / Suppression de programmes** à partir du panneau de configuration de Windows.

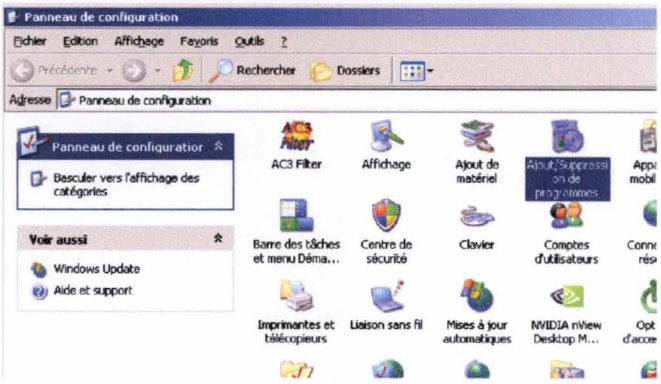


Figure 16 : Ajout/Suppression de programmes

Manipulations complexes

D'autres spywares nécessitent une manipulation complexe pour arriver à son élimination du système. Par exemple la suppression ou modification de clés dans la base de registre Windows, la suppression manuelle de fichiers (parfois cachés) sur disque dur. Ces procédures complexes d'élimination peuvent être décrites sur le site du fabricant ou dans un fichier accompagnant l'installation du programme. Ce n'est pas souvent le cas, la plupart du temps, ces procédures sont publiées par des organismes d'information et/ou de lutte contre ce type de programme.

Voici un exemple de manipulation, pour le Cydoor, qui est généralement installé avec des programmes de partage de fichiers comme Kazaa et LimeWire. Cydoor change certains paramètres du navigateur et télécharge des publicités à envoyer à l'écran.

Instructions de désinstallation de Cydoor [69]

Avant de pouvoir effacer les fichiers, il faut d'abord arrêter tous les processus de Cydoor qui tournent en mémoire. Cela peut se faire à partir du gestionnaire de tâches

Instruction d'effacement des valeurs dans la base de registre :
Ouvrez l'éditeur de la base de registre en cliquant sur le bouton "Démarrer", "Exécuter" et tapez "regedit" dans la boîte de dialogue qui apparaît, ensuite « OK ».
Une fois l'éditeur ouvert, voyagez dans l'arbre de la base de registres jusqu'à la localisation voulue.
Lorsque cette clé est localisée, pressez la touche « Effacer » afin de la supprimer.

Clés de la base de register à supprimer:
- *cydoor services*
- *Software\Microsoft\Windows\CurrentVersion\Run\Cydoor\CD_Load.exe*

Instructions de désenregistrement d'une DLL :
Pour désenregistrer un fichier de type DLL, localisez d'abord le fichier sur le disque dur.
Ouvrez une boîte de type ligne de commande en cliquant sur le bouton « Démarrer », « Exécuter » et tapez « cmd » dans la boîte de dialogue qui apparaît, ensuite « OK ».

Tapez ensuite « regsvr32 /u » suivi de la touche « ENTREE ».

Par exemple, pour désenregistrer un fichier nommé « maDll.dll » qui se trouve sur « C:\windows\system32 », vous devriez taper : « regsvr32 /u C:\windows\system32\myDll.dll » suivi de la touche « ENTREE »

Les fichiers à désenregistrer sont les suivants :
- cd_gif.dll
- cd_htm.dll
- cydoor
- Cydoor Services
- cydoor.com.csf

Figure 17 : Instructions de désinstallation de Cydoor

[69] Traduit du site d'Enigma Software Group : SpywareRemove, http://www.spywareremove.com/removeCydoor.html, (consulté le 12 décembre 2005)

La manipulation présentée dans cet exemple est relativement simple. Il en existe qui nécessitent la désactivation et la suppression d'une bonne centaine de libraires (DLL) ou de clés de registre.

Impossible sans outil spécifique

Certains spywares bloquent certaines manipulations qui pourraient arriver à leur suppression. Il est alors nécessaire d'installer des outils spécifiques anti-spyware, pour autant que l'installation de programme ne soit pas également bloquée, ce qui arrive pour certains spywares.

2.2.3 Blocage de la communication, filtre DNS

Un technique qui ne supprime pas le spyware mais l'empêche de fonctionner correctement consiste à bloquer la communication entre le spyware et le site à qui il rend compte et exploitant le fichier. Cette contre-mesure, la plus simple, et pourtant celle qui est mise en œuvre le moins souvent car elle donne l'apparence d'entrer dans les arcanes du système d'exploitation. Avec la liste hosts il n'y a plus de communication possible entre un ordinateur et les sites commanditaires identifiés donc même si les spywares survivent sur l'ordinateur ils ne pourront rien transmettre. [PIN05]

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Ceci est un exemple de fichier HOSTS utilisé par Microsoft TCP/IP
# pour Windows.
#
# Ce fichier contient les correspondances des adresses IP aux noms d'hôtes.
# Chaque entrée doit être sur une ligne propre. L'adresse IP doit être placée
# dans la première colonne, suivie par le nom d'hôte correspondant. L'adresse
# IP et le nom d'hôte doivent être séparés par au moins un espace.
#
# De plus, des commentaires (tels que celui-ci) peuvent être insérés sur des
# lignes propres ou après le nom d'ordinateur. Ils sont indiqué par le
# symbole '#'.
#
# Par exemple :
#
#      102.54.94.97     rhino.acme.com          # serveur source
#       38.25.63.10     x.acme.com              # hôte client x

127.0.0.1       localhost
10.0.0.10       lan.hades
10.0.0.14       lan.poseidon
10.0.0.15       lan.charon
10.0.0.138      lan.adsl

127.0.0.1       247media.com
127.0.0.1       ad.caramail.com
127.0.0.1       ad.dogpile.com
127.0.0.1       ad.infoseek.com
127.0.0.1       ad.linkexchange.com
```

Figure 18 : Exemple de fichier host

Dans cet exemple, pour les adresses mises en évidence, on redirige les adresses de serveurs connus pour leurs activités d'espionnage vers l'adresse locale. De cette façon, lorsque le spyware voudra contacter son serveur associé, il s'adressera à l'ordinateur sur lequel il est installé au lieu du serveur distant. L'information ne pourra pas être transmise.

Ce dispositif est présent dans tous les systèmes d'exploitation (Windows, Linux, Unix, MacOS, etc.) et toutes les versions de Windows.

On trouve ce fichier typiquement aux emplacements suivants :

- Windows 95/98/Me — C:\windows\hosts
- Windows NT/2000 — C:\winnt\system32\drivers\etc\hosts
- Windows XP (Home/Pro) — C:\windows\system32\drivers\etc\etc\hosts
- Linux / Unix — /etc/hosts

2.2.4 Blocage de l'entrée de certains spywares

Certains spywares sont "délivrés" par les pages Internet visitées. Il faut alors, en amont, analyser le flux entrant pour bloquer les mécanismes utilisés d'implantation des spywares, mécanismes qui s'appuient sur des scripts et / ou sur des contrôles ActiveX. [PIN05]

Les flux entrants de type HTTP

Le flux HTTP est celui qui est utilisé pour la consultation des pages Internet. Ces types de flux doivent être analysés en temps réel par des filtres agissant comme des proxy locaux capables de discriminer les scripts hostiles des scripts légitimes, réécrire à la volée le flux entrant et enfin le laisser atteindre votre navigateur. Des outils anti-scripts comme SpyBlocker[70] ou The Proxomitron[71] sont typique de ce genre d'analyse à la volée. [PIN05]

Les flux entrants de type POP/SMTP

Les flux entrants de type POP/SMTP correspondent au courrier entrant. Ils doivent être analysés également en temps réel. Les bons antivirus génériques ou certains, spécifiques au protocole de transmission du courrier, SMTP, le font. D'autre part, les scripts ne doivent pas être autorisés dans les courriers et les newsgroups.

Les flux entrants de type FTP

Les flux de type FTP sont ceux utilisés lors des téléchargements, ainsi que les copies de fichiers depuis un support (cd, disquette, etc.). Ils doivent être analysés avec un antivirus et un anti-spywares avant d'être ouverts.

2.2.5 Détecter et empêcher les activations de malveillances en temps réel.

La détection et la fermeture des malveillances se fait par analyse en temps réel des programmes résidant en mémoire. Ces utilitaires sont actifs en permanence et agissent comme des chiens de garde (en anglais « watch dog »). Ils interceptent un spyware qui serait passé au travers des autres mailles du filet grâce à diverses formes de camouflages. Un spyware a beau se camoufler, il faut bien, à un moment ou à un autre, qu'il s'exécute, en tant que programme, et que, pour cela, il "monte" en mémoire. Cette méthode est celle utilisée généralement par la plupart des logiciels anti-virus qui scannent les fichiers à la volée.

2.2.6 Empêcher l'installation des Spywares

Une approche très particulière est celle adoptée par un outil gratuit appelé SpywareBlaster qui installe, dans la base de registre, les clés de toutes les malveillances connues et les verrouille. Si jamais une malveillance tente de s'installer elle est stoppée dans son processus d'installation.

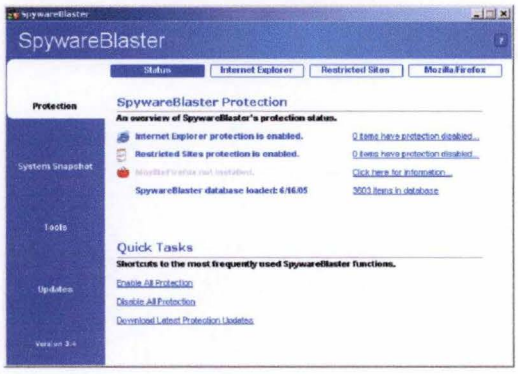


Figure 19 : SpywareBlaster

[70] SpyBlocker Software (http://spyblocker-software.com/spyblocker)

[71] The Proxomitron, de lipsheim.org (http://www.lipsheim.org/foret/proxomitron.htm)

2.2.7 Détection différée des malveillances stockées en fichier

Une méthode différée consiste à détecter les malveillances stockées sous forme de fichiers. Il s'agit d'utiliser un scanner anti-spyware. C'est la méthode la plus simple mais elle intervient trop tard par rapport aux utilitaires en temps réel. Même si on scanne sa machine tous les jours, le spyware a déjà provoqué ses dégâts. Toutefois on trouve d'innombrables scanners temps différé dont certains sont gratuits et très bons - en particulier à SpyBot Search and Destroy. Le spyware peut continuer à fonctionner même hors connexion à l'Internet et préparer la prochaine transmission. Les anti-spywares sont tous multifonctions et s'occupent d'une collection de spywares en même temps que d'autres implants malveillants comme les dialers, les adwares, les keyloggers, les chevaux de Troie etc. [PIN05]

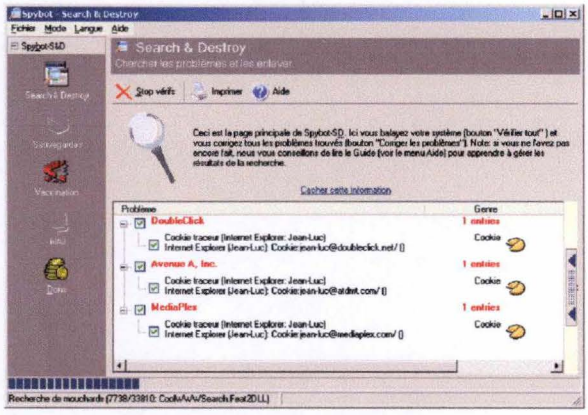


Figure 20 : Recherche différée Search & Destroy

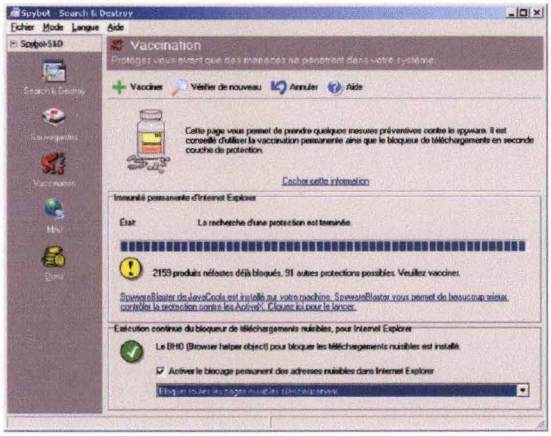


Figure 21 : Vaccination Search & Destroy

2.3 Les outils

2.3.1 Le contrôle des ActiveX

Ce problème ne concerne qu'Internet Explorer de Microsoft et les navigateurs s'appuyant sur la couche physique de celui-ci comme les navigateurs qui n'en sont que des habillages. Les navigateurs comme Opéra, Netscape ou Mozilla ne sont pas affectés par cette technologie non standard et propriétaire de Microsoft.

Paramètres de sécurité

Autoriser votre navigateur à exécuter un contrôle ActiveX est exactement la même chose qu'exécuter un programme. Un contrôle ActiveX diffère des autres programmes par la manière de le lancer. Au lieu d'être recherché et exécuté depuis le disque dur, il est recherché sur le Net, téléchargé depuis une page Internet, installé et exécuté.

Un simple réglage de paramètres de sécurité de Windows permet de garder le contrôle sur l'installation des ActiveX.

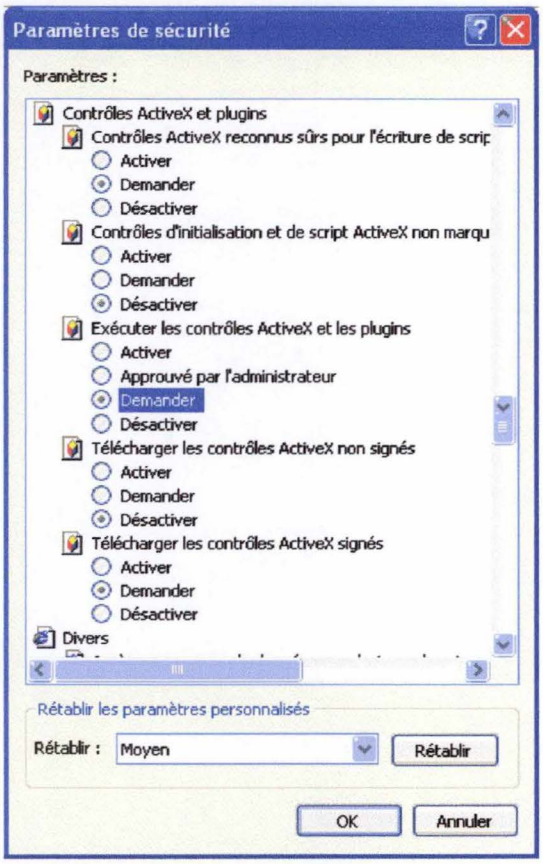


Figure 22 : Paramètres de sécurité de Windows

Kill bit

Une technique appelée « kill bit »[72] permet d'empêcher automatiquement l'installation des ActiveX réputés hostiles. Les contrôles ActiveX sont identifiés au moyen d'un identificateur unique, de type GUID, appelé Class identifier - CLSID. Internet Explorer utilise une liste d'exclusion[73] de CLSID qui est stockée dans la base de registre. Lorsqu'une page piégée essaiera d'installer un composant présent dans cette liste, elle échouera. Lorsqu'une page essaiera d'exploiter un composant présent dans cette liste, même si celui-ci était préalablement

[72] Microsoft Knowledge Base KB240797 : "How to stop an ActiveX control from running in Internet Explorer" [MKB05]

[73] Clé de la base de registre : « HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility »

réellement installé dans une machine, elle échouera également. Il existe donc des utilitaires fondés sur cette technique de blocage pour installer dans la base de registre de Windows tous les CLSID hostiles répertoriés. Internet Explorer peut ainsi être lancé en confiance avec la technologie ActiveX activée. Celui-ci ne chargera jamais, n'exécutera jamais et ne demandera même jamais l'autorisation d'installer un contrôle ActiveX hostile, dans la limite de ceux connus par l'utilitaire bien sûr. Les ActiveX inconnus réagiront selon les paramétrages du navigateur. Le kill bit une technique exploitée par Spybot Search and Destroy dans son processus de vaccination.

2.3.2 Les anti-adservers, les listes Hosts

Les anti-adservers sont tous les utilitaires qui touchent aux listes hosts qui sont utilisées comme filtre DNS, sur base d'une liste d'adresses de serveurs de publicités connues.

Cette solution présente l'avantage de fonctionner sous n'importe quel navigateur (InternetExplorer, Netscape, Opera, etc.) et n'importe quel système d'exploitation (Windows, Linux, Unix, MacOS, etc.). Les outils sont généralement livrés sous forme de scripts ayant pour but de générer des listes d'exclusion ou d'outils qui se basent sur des listes pour effectuer une réécriture des URLS avant de le passer au navigateur afin de procéder à une redirection. [SQU05]

Ces listes sont disponibles selon des catégories (appelées également « classe de redirection »), par exemple :

- serveurs de publicités,
- sites pornographiques,
- forums et mail gratuits (hotmail, caramail, etc.),
- sites de piratage (warez).

```
247media.com
ad.caramail.com
ad.dogpile.com
ad.infoseek.com
ad.linkexchange.com
ad.vol.at
ad1.pamedia.com.au
ad2.jwtt3.com
adbot.com
adbot.theonion.com
adbureau.net
adclub.net
adcount.hollywood.com
adfinity.*media.com
adforce.adtech.de
adforce.imgis.com
adfu.blockstackers.com
adimage.blm.net
adimages.criticalmass.com
adimages.sanomawsoy.fi
adisnet.com
adlink.de
adlink.deh.de
admanager.beweb.com
adone.com
adpower.de
ads-fr.spray.net
ads.activeagent.at
ads.bfast.com
ads.bluemongoose.com
ads.bomis.com
ads.cashsurfers.com
ads.csi.emcweb.com
ads.eu.msn.com
ads.fairfax.com.au
ads.filez.com
ads.focalink.com
ads.fp.sandpiper.net
ads.freshmeat.net
```

Figure 23 : Extrait d'une liste de redirection de type "publicité"

Toutes ces adresses seront alors redirigées vers le 127.0.0.1, l'adresse locale d'une machine. Ainsi, les requêtes sur ces serveurs ne sortiront jamais de l'ordinateur.

2.3.3 Les anti-Adwares

Les spywares de type adware agissent sur deux plans : une partie visible (publicité intrusive) et une partie cachée (scripts et programmation).

La partie visible : les publicités

Les techniques d'affichage sont variées (pop-up, bannières, interstitiels et autres méthode présentées précédemment) et de plus en plus intrusives. Il existe différents outils empêchant les publicités de s'afficher. Les outils anti-adware visent à supprimer toutes les formes de publicité intrusive de manière générique. Certains outils bloquent directement le comportement suspect (pop-up, bannières, animations) des objets manipulés par le navigateur ou les substituent par des objets fictifs.

La partie cachée : le code

Cette partie concerne « l'intelligence » du spyware, il est constitué d'un code de programmation ou d'un script. Elle véhicule la publicité de manière intelligente. C'est cette partie qui exploite les différentes techniques d'intrusion. Il convient de mettre en place les différentes techniques de parade disponibles à tout utilisateur :

- usage d'outils d'éradication anti-adwares pour les adwares déjà installés,

- réglage des paramètres de sécurité afin d'éviter des installations furtives d'ActiveX hostiles,
- application des mises à jour des correctifs de failles de sécurité du système d'exploitation et des outils de navigation,
- usage d'outils préventifs contre l'installation de code malveillant (pare-feu, listes de sites hostiles et éventuellement anti-virus).

2.3.4 Les Barres d'outils

Les barres d'outils (en anglais « toolbar ») ont deux buts : espionner et bombarder de publicité. Pour se faire, ils utilisent généralement la technologie ActiveX pour installer des composants de type hi-jacker (sous Microsoft InternetExplorer uniquement). Les outils d'éradication génériques font généralement office d'anti-barre d'outils, anti-adwares, anti-spywares et anti-hijacker.

2.3.5 Les BHOs

Les BHOs ne sont pas tous hostiles, mais la plupart servent à l'installation de spywares (de type adware ou barre d'outils) en utilisant la technologie ActiveX. Il existe assez peu d'outils spécifiques aux BHOs. Il en est cependant qui affichent la liste des BHOs installés ainsi que leur notoriété (connus et légitimes, connus et hostiles ou inconnus). Les BHOs peuvent se désinstaller manuellement sans trop de difficultés.

2.3.6 Les méthodes anti-cookies

Les cookies sont utilisés à des fins de traçage mais tous les cookies ne sont pas néfastes. Toute la difficulté réside dans la distinction à faire entre les cookies utiles et les néfastes. La plupart des navigateurs permettent de consulter les cookies stockés sur un ordinateur et de les supprimer de manière sélective. Cette sélection est très difficile, tant pour un connaisseur que pour un néophyte.

Il existe des outils anti-cookies qui permettent de désigner les cookies autorisés, ainsi que d'autres permettant de bloquer les cookies à la demande. On trouve malheureusement beaucoup d'outils qui fonctionnent à l'inverse de cette première catégorie : ils demandent de désigner les cookies à détruire et ils laissent passer les autres. On tombe dans le même travers que les anti-popup qui demandent de désigner ceux à fermer et qui laissent passer les autres. Ce qui a pour conséquence, une sollicitation très fréquente, à chaque nouveau site visité.

Une astuce utilisable avec Internet Explorer consiste à vider les cookies indésirables de leur contenu et de la marquer « en lecture seule » au niveau du système de fichier de Windows. Les sites exploitant ces cookies trouvent les fichiers cherchés mais ne peuvent les exploiter.

Les navigateurs permettent également de définir les types de cookies autorisés, par exemple en n'acceptant que les cookies provenant du site visité et pas ceux provenant d'autres sites référencés par des web-bugs (images visibles ou invisibles incrustés dans la page visité).

2.3.7 Anti-GUID

GUID matériel des microprocesseurs

Pour les Pentium III d'Intel, il existe un GUID matériel, marqué au sein même du microprocesseur qui identifie chaque CPU de manière unique. Il existe la possibilité d'inhiber ce GUID via le BIOS. Si ce n'est le cas, il est toujours possible d'installer une nouvelle version du BIOS (flash) afin d'activer cette possibilité.

GUID de Windows

Windows dispose d'un générateur de GUID qui est utilisé lors de son installation. Face à un mécontentement général, Microsoft a été contraint de fournir un outil permettant d'effacer le GUID généré. Celui-ci est disponible sur le site de mise à jour automatique (« Windows Update ») de Microsoft sous l'appellation de « Mise à jour de l'Assistant Inscription ». La désactivation du générateur de GUID (appelé « regwiz ») peut se faire par une manipulation simple documentée sur Internet et différente selon les versions de Windows.

2.3.8 Gestionnaire de liste de démarrage

Au démarrage d'un ordinateur, un ensemble de tâches sont lancées automatiquement. Toutes ces tâches sont consignées dans une liste appelée « liste de démarrage ».

Lorsqu'un logiciel malveillant parvient à s'installer sur un système, il fera en sorte de se trouver dans cette liste afin d'être démarré au même titre que les autres tâches automatiques du système.

La « Liste de démarrage » n'est pas une liste unique au sens propre mais un ensemble dispersé d'objets qui coopèrent et concourent au démarrage d'un PC d'abord, et de Windows ensuite.

Il existe des utilitaires qui collectent les différentes informations relatives aux tâches lancées depuis le démarrage de l'ordinateur. Ces utilitaires affichent ces informations sous la forme d'une liste virtuelle unique pour en simplifier la lisibilité.

Les objets dispersés peuvent être regroupés en catégories d'emplacement qui sont les suivants :

- Master Boot Record,
- fichiers de démarrage de MS-DOS (config.sys et autoexec.bat),
- fichiers de démarrage de Windows (system.ini et win.ini),
- répertoire de Démarrage,
- la Base de registre,
- ...

Master Boot Record (MBR)

Au démarrage de l'ordinateur, le premier programme à s'exécuter est le BIOS[74]. Celui-ci est contenu dans un composant matériel de la carte mère, une mémoire de type ROM, qui n'est modifiable que par « flashage ». Lorsque le système a été testé par le BIOS, il lance le tout premier programme qui se situe en début du premier lecteur de démarrage. Ce premier programme est appelé « bootStrap » et la zone dans laquelle il se trouve est le « Master Boot record ». Le BootStrap va alors à son tour charger le système d'exploitation installé sur la machine.

Le MBR est connu pour avoir eu, pendant des années, la capacité d'être modifié librement et c'est là que se chargeaient les tous premiers virus qui infestaient les secteurs de boot, dont ceux de toutes les disquettes qui circulaient. Aujourd'hui le MBR peut facilement être protégé par le BIOS.

Fichiers de démarrage MS-DOS

Héritage du monde MS-DOS, les fichiers de démarrage config.sys et autoexec.bat sont des fichiers textes éditables qui sont exécutés au chargement du système, depuis les premières versions de MS-DOS jusqu'aux versions 98 et Me de Windows. Les versions de Windows basées sur le noyau Windows NT, tels que Windows 2000 et Windows XP, démarrent réellement en mode Windows et émulent le DOS dans l'Invite de commande.

Fichiers de démarrage Windows

Au démarrage de Windows, deux fichiers (en texte clair) de configuration sont lus automatiquement, il s'agit du system.ini et win.ini. Le premier comporte une liste de paramètres tels que l'emplacement du shell, le pilote du clavier et de la souris, de l'interface graphique, des modules économiseurs d'écran, des gestionnaire de la carte son, etc. Le second fichier sert à l'initialisation de l'environnement de Windows. Il contient divers paramètres, dont une liste de services à charger et à exécuter. Ces listes sont généralement vides de nos jours car les versions plus récentes de Windows exploitent de préférence la base de registre de Windows.

Répertoire de Démarrage

Il existe la possibilité à tout utilisateur de créer un raccourci vers un programme dans un endroit spécifique appelé « Répertoire de Démarrage ». La particularité de cet emplacement est que tout programme référencé dans ce répertoire est automatiquement exécuté à l'ouverture de session de Windows pour cet utilisateur.

[74] Basic Input Output System

La base de registre

Microsoft a centralisé toute la configuration de Windows dans une base de données propre au système Windows, appelé « la base de registres ». La structure de cette base est complexe et la lecture des informations s'y trouvant n'est pas à la portée de tous. Cette base comporte près d'une cinquantaine d'emplacements provoquant le chargement et l'exécution de programmes.

Scheduler de Windows

Le scheduler est un gestionnaire de planification de tâches. Une tâche dans le planificateur correspond généralement à l'exécution d'un script ou d'un programme.

Les utilitaires

Il existe un certain nombre d'utilitaires qui permettent de regrouper virtuellement l'ensemble des tâches exécutées automatiquement et de les manipuler comme si elles faisaient partie d'une liste unique[75].

La difficulté de la gestion de la « startup list » ne réside pas dans la manipulation elle-même mais plutôt dans la discrimination des tâches. La plupart portent des noms de tâches (programmes ou clés dans la base de registre par exemple) ne fournissant aucune information sur le contenu ou la légitimité de la tâche.

Parmi les programmes de gestion de listes on trouve des utilitaires gratuits tels qu'Autoruns de Systernals[76] ainsi que l'outil standard livré avec Windows 95 et 98 « msconfig ».

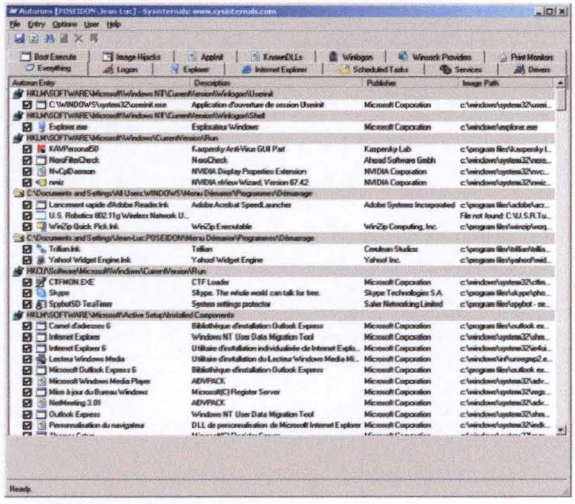


Figure 24 : SysInternals Autoruns

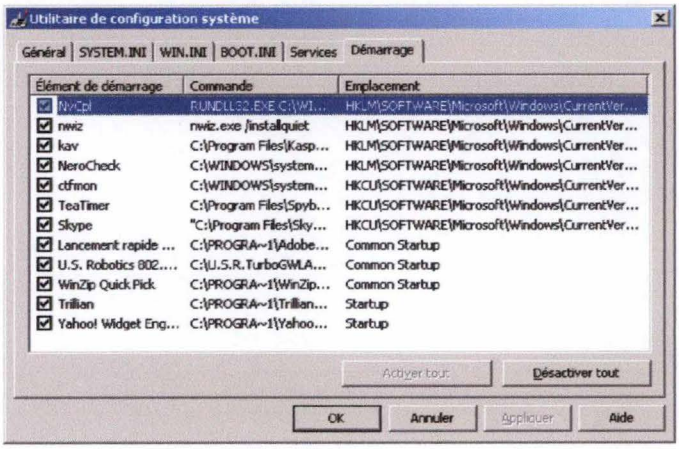


Figure 25 : Microsoft msconfig

[75] Toutes ces applications permettent de modifier directement les fichiers de démarrage suivants : Config.sys, Autoexec.bat, Win.ini, System.ini, menu démarrer et les sections « Run », « RunOnce », « RunOneEx », « RunServices », « RunServicesOnce » liées au démarrage de Windows dans la base de registre.

[76] Autoruns de SysInternals.com (http://www.sysinternals.com/Utilities/Autoruns.html)

Il existe également des outils donnant une information sur chaque élément connu pouvant se trouver dans une liste de démarrage. Une référence dans le domaine est celle dite « liste PacMan »[77] maintenue par son auteur Paul Collins. L'outil anti-spyware bien connu « Spybot Search & Destroy » intègre cette liste dans son module de gestion des listes de démarrage.

2.3.9 Désactivation des modules « auto-update »

Les programmes dits « auto-update » permettent une mise à jour automatique pour une application donnée. Le plus connu est bien-sûr celui de Microsoft qui se connecte régulièrement sur son site afin de déterminer les mises à jour à effectuer. Il n'est pas le seul à utiliser cette méthode, de plus en plus d'applications pratiquent cette technique de mise à jour.

Certains trouvent une justification bien légitime, tels que les bases de données de signatures d'anti-virus ou d'autres logiciels de protection du système nécessitant la dernière version pour être efficace. C'est également le cas de Microsoft et des mises à jour de sécurité. Cependant, il faut se méfier de la manière dont cette technique est exploitée.

Correctifs Windows

Le module auto-update de Windows propose d'installer automatiquement les correctifs de failles de sécurité, ce qui, en soi, est une bonne chose. L'auto-update n'est pas le seul moyen permettant de tenir à jour son système, il est toujours possible de se connecter directement sur le site de mise à jour en ligne de Microsoft afin de procéder au téléchargement des correctifs et des Service Packs. Il faut cependant prendre conscience que lorsque qu'on fait la mise à jour en ligne, via auto-update ou à partir du site de Microsoft, il y a un échange d'informations sur les logiciels installés. Celles-ci sont transmises à Microsoft, lui laissant la possibilité d'invalider certains produits dont le numéro de licence ne serait pas valable[78]. Windows Update se permet également de changer des paramètres qui auraient été modifiés par l'utilisateur tels que le lancement automatique de MSN Messenger.

Les correctifs sont disponibles en ligne afin de pouvoir les télécharger une seule fois et de les installer sur un parc de machines. Dans ce cas, on n'est pas obligé de passer par l'auto-update ou la mise à jour en ligne. Cette alternative est un bon compromis pour tenir son système à jour, éviter le risque d'espionnage et les mises à jour non sollicitées.

Sous Windows XP, plusieurs composants sont responsables du téléchargement et de la mise à jour du système[79] :

- Windows Update,
- Windows Media-Player,
- MSN Explorer,
- Windows Messenger,
- Help & Support Center,
- Root Certificates,
- Certificate Revocation,
- Dynamic Update,
- ActiveX controls,
- Internet Time Service,
- Digital Rights Management.

---

[77] PacMan Startup List (http://www.pacs-portal.co.uk/startup_index.htm)

[78] Windows Update Privacy Statement (http://v4.windowsupdate.microsoft.com/en/about.asp)

[79] Windows XP and the Internet Managed Environment (www.microsoft.com/technet/prodtechnol/winxppro/maintain/intmgmt/03_xpcer.mspx)

Internet Explorer

Depuis la version 5 d'Internet Explorer, il vérifie à chaque démarrage s'il existe une mise à jour disponible sur le site de Microsoft. Ce paramètre de mise à jour automatique peut être désactivé aisément dans les « options Internet » (voir figures ci-après).

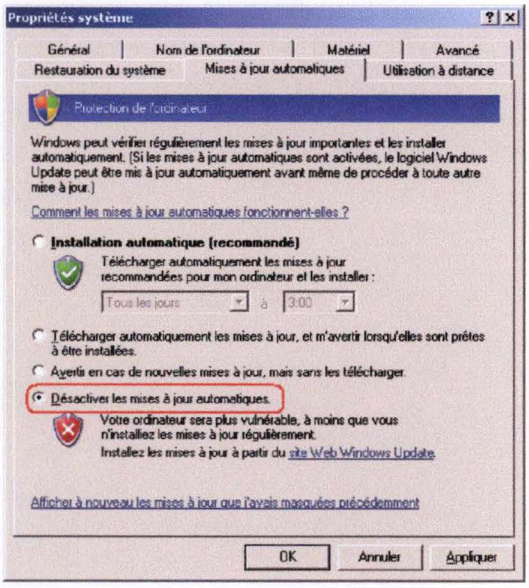


Figure 26 : Mise à jour automatique de Windows

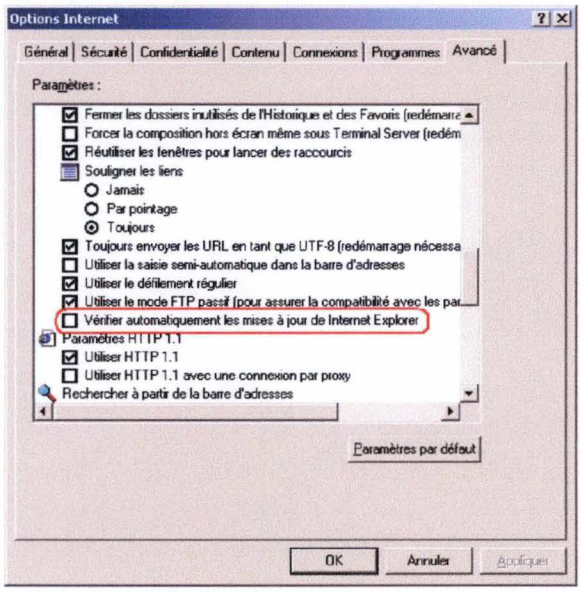


Figure 27 : Mise à jour d'Internet Explorer

Autres programmes de mise à jour automatique

Microsoft n'est bien sûr pas le seul à fournir des composants de mise à jour automatique. Parmi les plus répandus, il est intéressant de mentionner deux produits : « BigFix »[80] et « BackWeb »[81]. Ces éditeurs ont passé des contrats avec certains constructeurs d'ordinateurs. Par exemple, le service auto-update de BackWeb est utilisé par Cisco, Hewlett-Packard / Compaq, Ericsson, Siemens et Logitech.

Leur but est de permettre à un constructeur d'accéder à tous les ordinateurs qu'il a vendu et de forcer un téléchargement de composants logiciels et de mises à jour de manière automatique. Il va sans dire que cette procédure nécessite un examen complet du système afin de déterminer quels sont les logiciels installés, quelles versions et quelle langue sont utilisées.

2.3.10 Mesures anti-scripts

Les scripts étant du code à l'intérieur des pages Web reçues, il y a deux approches qui doivent s'exécuter en temps réel.

Blocage

L'une des approches est le blocage systématique de scripts en temps réel au niveau de l'interpréteur. Le risque est bien sûr de tout bloquer, même les scripts qui ne sont pas hostiles. Il est possible d'effectuer certains réglages au niveau du navigateur en ce qui concerne les différents langages de scripts. Tout bloquer n'est pas une solution car les sites qui utilisent des scripts à des fins esthétiques ou fonctionnelles sont nombreux. Les ActiveX par contre sont dangereux et plus rarement utilisés.

Les navigateurs proposent généralement un réglage à trois options : accepter, refuser ou demander à être alerté. Les figures ci-dessous montrent les paramètres d'Internet Explorer relatifs aux scripts.

---

[80] BigFix (http://www.bigfix.com)

[81] BackWeb (http://www.backweb.com)

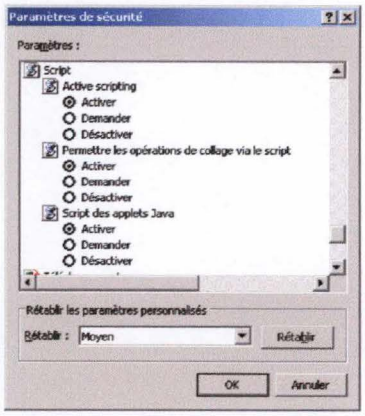


Figure 28 : Paramètres de sécurité, les scripts

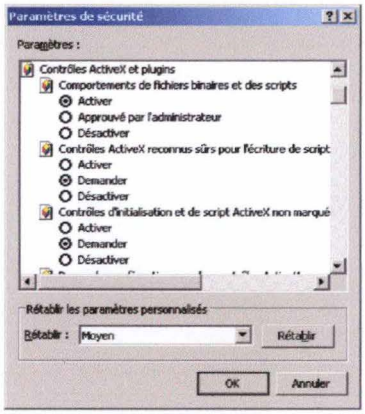


Figure 29 : Paramètres de sécurité, les ActiveX

Filtrage

La deuxième méthode consiste à analyser et filtrer le flux entrant en temps réel. Des filtres plus ou moins intelligents lisent le code des pages Web lorsqu'elles arrivent, avant qu'elles ne soient prises en charge par le navigateur. Ils qualifient les scripts selon les instructions qu'ils contiennent et ce, conformément aux paramétrages de l'outil. Le code des pages Web est alors réécrit à la volée, et est enfin passé au navigateur Internet. Ainsi les scripts créant, lisant, écrivant, réécrivant des cookies peuvent être gérés. Ceux modifiant l'affichage peuvent être interdits. Les scripts faisant référence à des serveurs autres que le serveur du site visité peuvent être bloqués. Ceux permettant le défilement des affichages publicitaires peuvent être inhibés et les scripts considérés hostiles sont purement et simplement effacés.

Compte tenu de la puissance de calcul des ordinateurs, le temps additionnel pris par ces filtres temps réel est insignifiant, et d'autre part, du temps est gagné grâce à des fonctions qui ne s'exécuteront pas, des pubs qui ne seront ni chargées ni affichées, etc.

Chapitre 3 Etude de cas et démonstrations

3.1 Objectifs de l'étude

De par sa nature, le logiciel espion a pour objectif, entre autres, de rester le plus discret possible à l'inverse des virus. Pour cette raison, l'utilisateur moyen a bien plus de difficultés à percevoir le danger d'un logiciel espion. La notion de risque prend une toute autre dimension lorsque celui-ci est invisible. Un dégât causé par un virus informatique a un caractère apparent et marquant pour celui qui subit le dommage, plus qu'une violation de la vie privée dont la majorité des utilisateurs ne se soucient guère. Le risque lié à un spyware est beaucoup plus sournois et plus mal aisé à mettre en évidence.

Les objectifs de l'étude sont donc la conscientisation de l'utilisateur aux risques liés aux spywares et la complexité de faire face à ce phénomène pour un néophyte. Cette complexité est en partie due à la confusion et à l'ambigüité amenée volontairement par les principaux acteurs du secteur.

Dans le cadre de cette expérience, plusieurs logiciels anti-spyware seront pris en considération. Parmi ceux-ci, il y en a malheureusement peu de vraiment fiables. L'expérience prendra compte de cet état de fait en mettant en jeu un anti-spyware fiable et d'autres, faux ou douteux.

3.2 Méthode

Afin pour mettre en évidence le risque encouru par l'internaute, démontrons qu'un surf anodin, sans protection anti-spyware spécifique, peut entraîner très rapidement une contamination conséquente en terme de logiciels espions.

La démonstration nous place dans la peau d'un utilisateur lambda ayant entendu parler des logiciels espions et qui, naïvement, va installer des logiciels anti-spyware trouvés au hasard de sa navigation sur Internet. Celui-ci sachant qu'il existe de vrais et de faux anti-spyware, en installe donc plusieurs en espérant que les meilleurs feront leur travail et la part des choses en mettant en évidence le bon grain de l'ivraie.

La première partie de l'expérience consiste à démontrer l'existence et la prolifération de logiciels espions. Afin de procéder à cette démonstration, différents scenarios seront présentés :

1. l'installation du logiciel d'échange de fichiers : Kazaa[82],
2. l'installation d'un économiseur d'écran de la famille « SceenScenes » de Gator[83].

Ensuite, testons la réaction de deux outils anti-spyware différents face à l'installation d'un logiciel suspect : un décodeur vidéo d'eMedia[84].

1. eMedia Codec face à SpywareQuake,
2. eMedia Codec face à Spybot Search and Destroy.

Examinons enfin les différents scenarios possibles en imposant comme base de travail trois logiciels prétendument anti-spyware. Ceux-ci seront mis en concurrence afin d'observer les interactions, entre eux et vis-à-vis des espions éventuellement installés sur le système :

1. Spybot Search and Destroy,
2. SpywareStrike,
3. AdwareSpy.

[82] Kazaa (http://www.kazaa.com)

[83] GAIN ScreenScenes (http://www.screenscenes.com)

[84] eMedia Codec (http://www.emcodec.com)

3.3 Mise en place du laboratoire

Pour débuter la démonstration, une phase préparatoire est indispensable afin d'assurer la fiabilité et la reproductibilité de l'expérimentation.

3.3.1 Installation matérielle

L'expérience a été réalisée sur un ordinateur de type portable IBM Thinkpad dont les caractéristiques sont les suivantes :

- 64 MB de mémoire vive,
- processeur Pentium II 300 MHz,
- un disque dur de 6,4 Go,
- carte réseau PCMCIA : Xircom CreditCard Ethernet 10/100 + Modem 56,
- écran de portable sur une carte vidéo NeoMagic MagicGraph256AV, résolution de 1024x768 pixels.

L'ordinateur est connecté à l'Internet via un routeur ADSL sur la connexion réseau Ethernet à 100 Mbps.

3.3.2 Installation logicielle

Installation initiale

Afin de se prémunir d'une éventuelle infection de parasites résiduels quelconques, le premier démarrage du système se fait à partir d'un CD-Rom d'installation de Linux (Mandriva 2005). La totalité du disque dur est alors formatée en mode « extended3 », en choisissant l'option d'effacement complet du contenu du disque. Une fois la partition créée et formatée, le système est redémarré en utilisant le CD-Rom d'installation de Windows 2000 (Service Pack 2). Celle-ci est de type standard sans aucune modification par rapport aux options présentées par défaut par Windows durant le processus d'installation[85].

Afin de faciliter la remise à zéro du système à chaque initialisation d'un nouveau scénario, une image du système est créée par « TrueImage » de la société Acronis. Cet outil a la possibilité de démarrer à partir du CD-Rom sur son propre système d'exploitation afin de ne pas interférer avec le système d'exploitation installé. La procédure de sauvetage de l'image du système est la suivante :

- démarrage à partir du CD-Rom TrueImage,
- gravure de l'image de la partition complète sur CD.

Les logiciels système

Sont repris sous la catégorie « logiciels système » le système d'exploitation ainsi que les outils ayant servi à l'installation de base du système.

Microsoft Windows 2000 Professional
Version : Windows 2000 Professional 5.0 Service Pack 2 Build 2195
Site web : http://wwww.microsoft.com

Microsoft InternetExplorer
Version : InternetExplorer 5.0 Build 3315.1000

Acronis TrueImage
Version : 6.0 build 311
Editeur : Acronis Inc., 395 Oyster Point Boulevard, Suite 213, South San Francisco, CA 94080 USA
Site web : http://www.acronis.com
Remarques : TrueImage est distribué en version française par Micro Application sous le nom de « PC Cloneur Expert »

[85] Les écrans successifs de la totalité de l'installation est consultable dans les annexes.

Mandriva Linux 2005

Version : Mandriva Linux Limited Edition 2005 for i586 and x86-64
Editeur : Mandriva (anciennement Mandrakesoft)

Les produits anti-spyware

Les produits sélectionnés sont tous disponibles gratuitement sur Internet.

Spybot Search & Destroy

Version	Spybot Search and Destroy 1.4, detection update 2006-03-17
Editeur	Safer Networking Limited P.O. Box 16 Greystones, Co. Wicklow, Irlande
Site web	http://www.safer-networking.org
Whois[86]	safer-networking.org est un nom de domaine enregistré par Safer Networking Limited Patrick Michael Kolla Rampenstrasse 16 Bochum Germany
Détails	Spybot S&D est un outil anti-spyware écrit par un ingénieur en informatique allemand, Patrick Michael Kolla, distribué par la société de l'auteur Safer Networking Limited. Spybot S&D est un véritable anti-spyware de renom. Il est difficile de vérifier si l'outil fait exactement ce qu'il prétend, néanmoins il fait partie des produits recommandés par la presse spécialisée, par les sites Web spécialisés en sécurité et protection de données, ainsi que par de nombreux forums.

SpywareStrike

Version	SpywareStrike 2.5
Editeur	SpywareStrike, Chypre, pas d'adresse publiée
Site web	http://www.spywarestrike.com
Whois	SpywareStrike.com est un nom de domaine enregistré par Keramitsu LLC David Alan Taylor 321 th Melburn Street Seatle, Washington, 98107 USA
Détails	SpywareStrike est reconnu comme faux outil anti-spyware. Une fois installé, il ouvre des pop-ups de fausses alertes aux spywares. Il propose alors de se débarrasser de ce problème moyennant l'achat du produit pour 49,50 US$. SpywareStrike est également distribué sous les noms de SpyAxe, AdwareDelete, AntiVirus Gold et SpyFalcon. [SPW06] Le moteur de SpywareStrike est complètement inadéquat à la détection de mouchards, il ne trouve généralement rien, si ce n'est les fausses alertes qu'il génère.

AdwareSpy

Version	AdwareSpy 4.0
Editeur	Elite Concept Inc., 825 Phillips Hill Road, Coventry, Rhode Island 02816, USA

[86] Chaque nom de domaine est enregistré par une personne physique ou morale, qui a dû préalablement fournir des informations légales relatives à la propriété et la responsabilité d'une personne vis-à-vis dudit domaine. Ces informations sont enregistrées dans une base de donnée appelée WHOIS, celle-ci étant consultable librement sur Internet. La rubrique « Whois » de la description de chaque produit représente donc l'information disponible dans la base de donnée WHOIS pour le nom de domaine mentionné.

Site web : http://www.adwarespy.com

Whois adwarespy.com est un nom de domaine enregistré par
Elite Concepts, Inc
David Taylor
623 Post Road
Warwick, Rhode Island 02888
USA

Détails AdwareSpy est référencé sur la liste des outils anti-spyware/adware non fiables. Il incite à la vente par des fausses alertes. Il détecte effectivement certains spywares mais génère également des fausses détections pour effrayer l'utilisateur et le convaincre de la nécessité de son produit.
Il est également distribué sous les noms suivants : AdDriller, 2004 Adware/Spyware Remover & Blocker, ADS Adware Remover, AdWare SpyWare Blocker & Removal, AdwareX Eliminator, Ad-Where 2005, ETD Security Scanner, Privacy Tools 2004, SpyBeware, Spy-Kill et The Web Shield. [SPW06]

Les applications

Les logiciels présentés dans cette rubrique ne sont pas nécessairement des logiciels espions mais sont réputés pour être des vecteurs de distribution de logiciels espions liés à Gator, l'un des éditeurs de spywares des plus réputés sur le marché.

Claria ScreenScenes

Version Claria ScreenScenes – MagicWaterfalls for Windows

Editeur GAIN Publishing
555 Broadway St
Redwood City, CA 94063
USA

Site web : http://www.screenscenes.com

Détails : L'économiseur d'écran comprend des animations, des sons ainsi que quelques paramètres configurables. Tout comme les autres produits de GAIN Network, il affiche des publicités sous la forme de pop-ups et pop-unders, d'autres pop-up sliders peuvent également apparaître dans le navigateur lorsqu'il est sur Internet. La clause relative à la vie privée stipule qu'aucune information qui rende l'utilisateur personnellement identifiable n'est collectée ou transmise. Des informations non personnelles sont cependant collectées et utilisées afin de créer le profil de l'utilisateur pour déterminer ses préférences de consommation.

Kazaa

Version KaZaA 3.0

Editeur Sharman Networks
aucune adresse disponible

Site web : http://www.kazaa.com

Whois kazaa.com est un nom de domaine enregistré par
Sharman License Holdings Ltd
C/- BDO House
Father WH Lini Hwy, PO Box 240
Port Vila, Efate

(Pour le détail, Efate est un paradis fiscal, une île située près de la Nouvelle-Calédonie)

Détails Kazaa est une application de partage de fichier point à point (P2P) qui utilise le protocole FastTrack. Le client officiel est téléchargeable gratuitement et est financé par des programmes malicieux en dépit du logo « No-Spyware » affiché sur le site Web.
Kazaa a été longtemps accusé d'installer du code malicieux. Sharman Network, éditeur du logiciel, affirme que ces produits ne sont pas des publiciels et ne collectent aucune information personnelle. La partie adware de Kazaa est présentée comme module optionnel du produit, bien qu'il soit techniquement difficile de l'éviter durant l'installation. Les modules

incriminés sont livrés automatiquement avec le produit et il est impossible de les désinstaller. Les outils de détection et d'éradication de logiciels espions éprouvent généralement des difficultés à supprimer ces modules sans une intervention manuelle spécifique de l'utilisateur. Les modules incriminés sont les suivants :

- Cydoor, il se charge de collecter des informations sur les habitudes de navigation et les transmet à la société qui édite Cydoor,
- B3D, une extension qui affiche des pop-ups publicitaires lorsque l'utilisateur visite un site Web réceptif à ce module,
- Altnet propose des liens de téléchargement sur des sites Web rétribués par la publicité en substitution aux liens de téléchargement de fichiers chez des utilisateurs particuliers,
- GAIN, module de Gator qui identifie et profile l'utilisateur sur base de ses habitudes de navigation. La version de Kazaa distribuée après le 16 août 2005 ne contient plus ce module,
- InstaFinder redirige les pages d'erreurs sur le site InstaFinder en lieu et place de la page standard de recherche MSN de Microsoft,
- RX Toolbar est une barre d'outils qui enregistre les adresses de tous les sites visités sous Internet Explorer et fournit les liens vers les sites Web concurrents,
- New.net est une extension du navigateur qui propose la vente de noms de domaines.

3.4 Démonstration 1 : Gator

3.4.1 Introduction

Nous allons jouer le rôle de l'utilisateur naïf qui ne s'y connait pas en matière de logiciels espions mais qui néanmoins s'y intéresse car il en a entendu parler. Il cherche donc à se prémunir de ces désagréments et choisit d'installer un logiciel anti-spyware et de soumettre les logiciels qu'il désire installer à l'analyse avant de les utiliser.

Pour cette démonstration, le choix des produits se porte sur des programmes répertoriés comme étant liés à Gator : Kazaa, un programme de partage de fichier, et ScreenScenes, un produit édité par Claria.

3.4.2 Présentation

La société Gator, qui a changé de nom pour devenir Claria[87] est le nom d'un des plus importants éditeurs de spywares. Leurs spywares sont intégrés dans de nombreux utilitaires, souvent limités, mais gratuits. Le plus connu de ceux-ci est OfferCompanion, un module permettant à Gator - Claria de gérer les bannières publicitaires des sites visités et de les remplacer suivant ce que l'utilisateur est susceptible d'acheter. Gator est l'un des plus grands propriétaires, et opérateur de serveurs de publicités basés sur l'analyse comportementale des internautes. Selon cette même société, en février 2004, plus de 27 Millions de PC auraient été « contaminés » par OfferCompanion. [SAL04]

GAIN est l'acronyme de Gator Advertising and Information Network, le réseau de Gator, partie de Claria Corporation, le plus grand réseau mondial comportemental et contextuel. A travers leurs bases de données, construites à l'aide des statistiques réunies par leurs spywares, GAIN établit donc le profil des utilisateurs et les inonde de publicités intrusives.[SAL04]

3.4.3 Gamme de produits Gator

Les outils proposés par Gator embarquent le spyware OfferCompanion ainsi qu'un autre outil au nom de « Enhancement Technologies ».

Le spyware OfferCompanion traque les sites et pages visitées par un internaute et renvoie ces informations, avec d'autres données privées, aux serveurs de Gator. Gator vend le droit d'usage de ces informations, agrégées ou nominatives, à des régies publicitaires qui peuvent également lui acheter une possibilité d'incruster des pop-ups grâce à la partie adware de OfferCompanion. Ces publicités apparaissent sur les sites visités, à des moments choisis par eux, ou lors de l'occurrence de certains mots. Ils incrustent de la publicité en temps réel sur les sites concurrents de leurs clients.

Outre le fait d'être un spyware, OfferCompanion télécharge des bannières ou des pop-ups qui viennent, eux-mêmes, avec d'autres spywares qui s'implantent silencieusement.

OfferCompanion est installé avec de nombreux logiciels, dont les plus répandus comme KaZaA ou le codec DivX, ainsi que les utilitaires proposés par la gamme Gator :

GotSmiley	GotSmiley permet d'insérer des émoticônes dans le courrier électronique, parmi un choix dans une librairie de plus de 1000 images. GotSmiley fonctionne avec Outlook, Yahoo!, Hotmail et d'autres messageries.
ScreenScenes	ScreenScenes offre un grand choix d'économiseurs d'écrans représentant des décors naturels animés et sonorisés.
WebSecureAlert	WebSecureAlert se pretend être un outil de sécurisation de vie privée et permettant d'épurer régulièrement l'historique de navigation d'Internet Explorer.
DashBar	DashBar est une barre de recherche qui vient se greffer au navigateur.
Precision Time	Gator Precision Time est un outil permettant de synchroniser l'horloge d'un ordinateur avec une horloge atomique américaine.

[87] Gator Corporation est devenue Claria Corporation le 2 octobre 2003. L'adresse du site internet est http://www.claria.com.

Date Manager Gator Date Manager est un outil qui permet de prendre des notes dans un calendrier (rendez-vous, anniversaires, évènements, etc.).

Weatherscope Weatherscope est un outil qui permet d'afficher un mini bulletin météorologique du jour et des jours prochains.

Gator eWallet Gator eWallet est un outil d'aide au remplissage des champs d'un formulaire. C'est-à-dire qu'il se souvient, entre autres, de l'identification ainsi que du login et mots de passe des utilisateurs[88].
Gator eWallet est le seul produit de la gamme qui a conservé son ancienne appellation « Gator ». Selon la présentation du site[89], Gator eWallet est prétendument parfaitement sécurisé car il encrypte les informations saisies dans les formulaires et les sauve localement.

3.4.4 Méthode

La démarche suivie par la démonstration est la suivante. A partir d'un système sain (libre de tout spyware, virus et autres malveillances), on procède à l'installation d'un programme déterminé. On analyse alors le système avant et après ce processus d'installation afin de constater ce qui a été réellement installé sur cet ordinateur muni d'une connexion haut débit.

Remarques

Les outils de détection et d'éradication de logiciels espions sont désactivés durant l'installation. Ils sont ensuite réactivés durant la phase d'analyse du système une fois l'installation terminée.

Les paramétrages de sécurité de Windows et du navigateur sont laissés tels qu'ils sont par défaut après l'installation du système. Aucune précaution particulière n'est prise concernant l'utilisation des ActiveX, du fichier hosts ainsi que toute forme de scripts.

Les outils anti-spywares une fois installés sont configurés pour une détection approfondie. Par défaut, il est courant que, dans un souci de performances, ces outils soient configurés pour une détection rapide et non pas une détection approfondie.

---

[88] Microsoft Internet Explorer intègre cette fonctionnalité de remplissage automatique de formulaire (en anglais « Auto-complete ») et de mémorisation automatique des mots de passe depuis sa version 5, il en est de même pour Mozilla.

[89] Présentation des produits de la gamme Claria (http://www.claria.com/products/software)

3.4.5 Diagramme de séquence

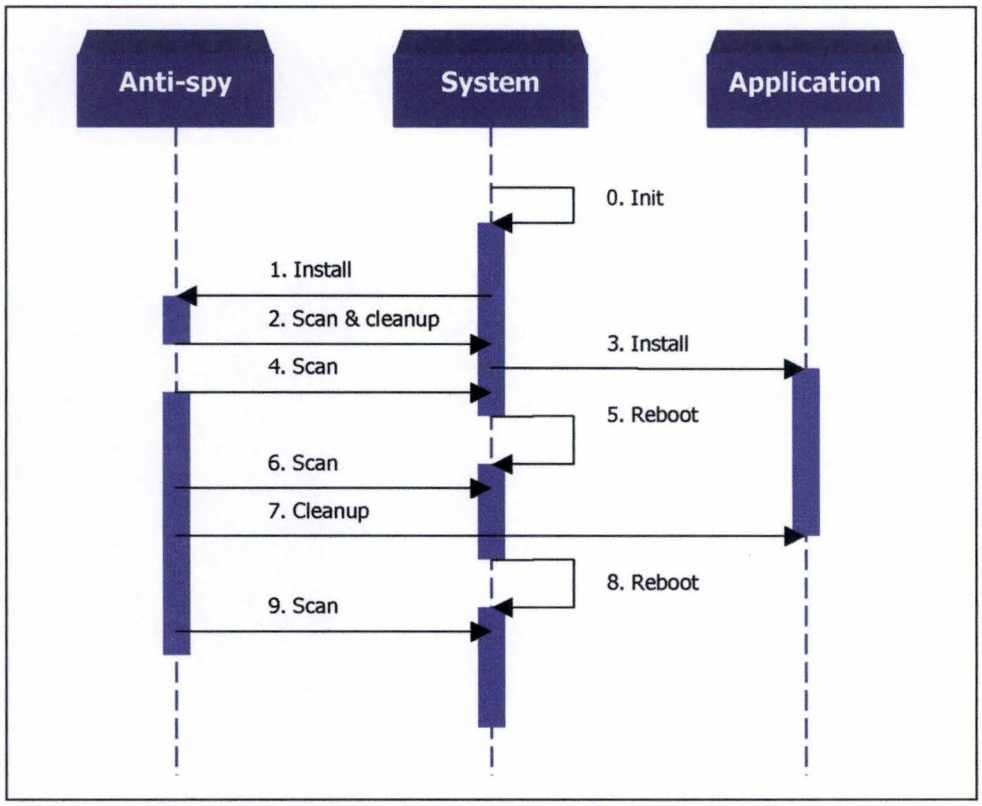


Figure 30 : Diagramme de séquence, test d'applications

0. Init

L'étape d'initialisation comprend les tâches suivantes :

- Démarrage du système à partir d'un CD d'installation Linux (Mandriva 2005), le disque dur est complètement reformaté (une seule partition « ext3 ») en utilisant l'option « Erase entire disk » du logiciel d'installation,
- démarrage du système à partir d'un CD de démarrage de TrueImage. L'image de la partition sauvée sur CD est alors installée sur le système,
- redémarrage avec le système nouvellement restauré.

Cette phase correspond à l'étape marquée « 0. Init » dans le diagramme de séquence ci-dessous.

3.4.6 Scenario 1 : KaZaA

1. Install Anti-Spy

Description Téléchargement et installation de Spybot Search & Destroy

Tâches - Démarrage du navigateur Internet Explorer,
- navigation sur la page de téléchargement de l'anti-spyware (http://www.safer-networking.org),
- lancement de l'installation du produit.

Les étapes de téléchargement et d'installation de Spybot S&D sont illustrées en annexe sous la rubrique « Installation de Spybot S&D ».

2. Scan Anti-Spy

Description Analyse du système par Spybot Search & Destroy

Tâches

- Démarrage de Spybot S&D,
- configuration de l'outil pour une analyse approfondie[90],
- vaccination du système[91],
- analyse du système,
- résolution de tous les problèmes détectés.

Résultats et observations

Résultat de l'analyse du sytème :

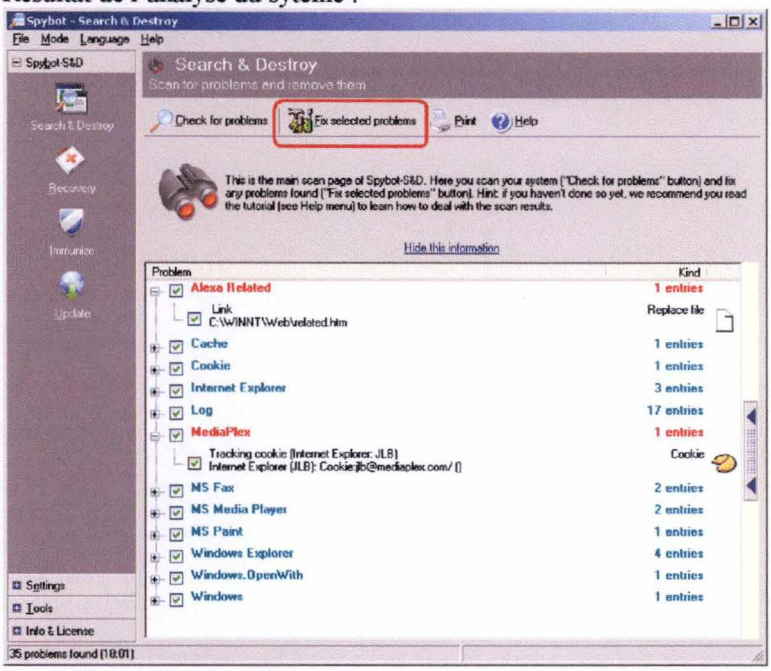


Figure 31 : Analyse du système initial

L'analyse du système met en évidence la présence du lien Alexa ainsi qu'un cookie de MediaPlex. Tous les objets sont sélectionnés pour effectuer le nettoyage.

Différentes boîtes de dialogue de confirmation ou d'information apparaissent. On les accepte.

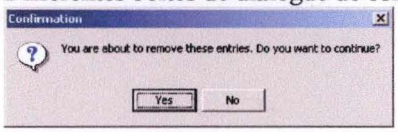


Figure 32 : Spybot, confirmation de nettoyage

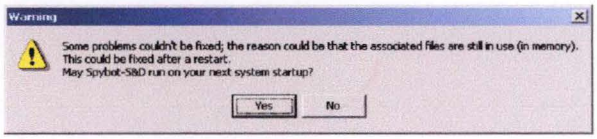


Figure 33 : Spybot, avertissement de redémarrage nécessaire

Figure 34 : Spybot, résultat et redémarrage

[90] Les impressions d'écran de la configuration de Spybot S&D sont disponibles en annexe.

[91] La vaccination correspond à l'inscription d'une liste clés de blocage dans la base de registre (sites Internet et CLSID).

Le nettoyage est terminé et Spybot affiche le résultat suivant :

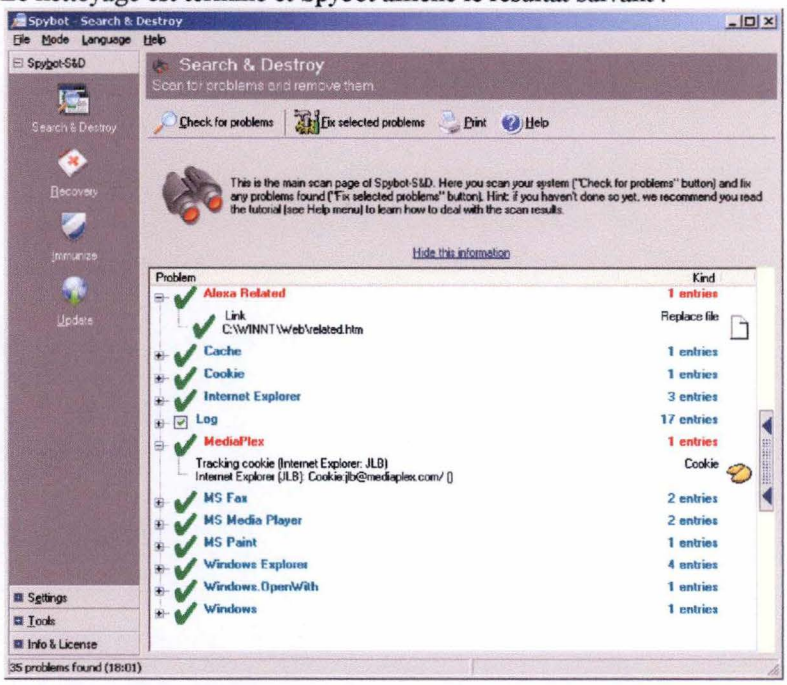


Figure 35 : Spybot, résultat après nettoyage

Spybot exige un redémarrage pour finir son nettoyage, le système est donc redémarré.
Lors du démarrage, Spybot démarre et effectue une vérification du système (recherche sur une base de près de 40000 éléments) avant même que l'utilisateur ne puisse prendre la main sur Windows.

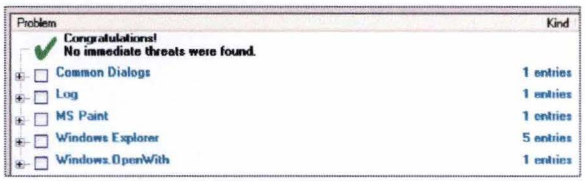


Figure 36 : Spybot, résultat après redémarrage

A chaque redémarrage, les éléments en vert dans la liste reviennent mais ce sont des éléments marqués comme éléments non gênants inoffensifs. Ils ne contiennent que des éléments résultant d'un usage normal de Windows tels que la liste des fichiers ouverts, l'historique des pages web visitées et le journal de démarrage de Windows.
Afin d'éviter de voir apparaître ces éléments dans les prochaines analyses, un paramètre de Spybot permet de désactiver la recherche de ces traces appelées « Usage Tracking » :

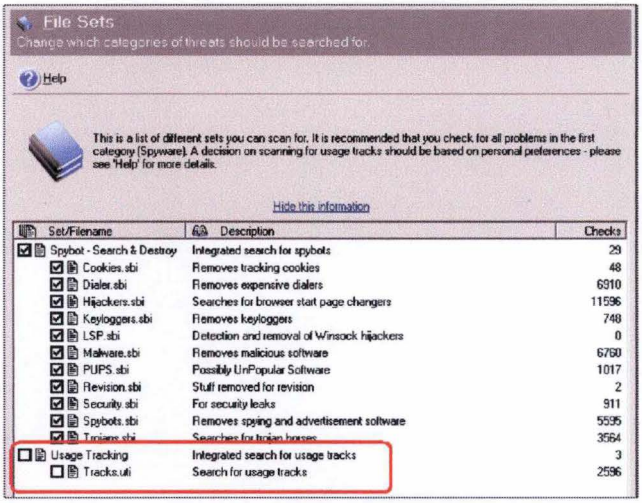


Figure 37 : Spybot, désactivation des détections de traçage

Au premier scan, sans avoir installé quoi que ce soit sous Windows, l'analyse du disque révèle un élément qualifié de spyware. Il s'agit du lien d'Alexa[92].
Les autres éléments sont les traces d'activités laissées par l'utilisateur sur le système, ainsi que des identificateurs de produits installés sur le système tels que Windows Media Player, la liste des derniers fichiers ouverts par MS Paint, les journaux d'activité de différentes applications, etc. (Le rapport complet de l'analyse se trouve en annexe)
Le cookie marqué de rouge « MediaPlex » est un cookie qui a été mis par la navigation sur la page du site miroir qui propose le téléchargement de Spybot S&D.

Alexa related le fichier related.htm est en réalité juste un script qui ouvre le panneau de recherche d'Internet Explorer sur l'adresse http://related.msn.com/related.asp avec comme paramètre les critères de recherche. Cette adresse est en réalité une redirection vers l'adresse http://xslt.alexa.com/data, le serveur de la société Alexa, éditeur du logiciel espion du même nom.

3. Install Kazaa

Description Installation de KaZaA

Tâches
- Démarrage de Internet Explorer et connexion à l'adresse http://www.kazaa.com,
- téléchargement du produit,
- lancement de l'installation,
- démarrage du produit.

[92] Le lien Alexa est présenté de manière plus détaillée dans la partie théorique comme illustration de la notion de spyware intégré dans la constitution logicielle.

- Démarrage de Internet Explorer et connexion à l'adresse http://www.kazaa.com

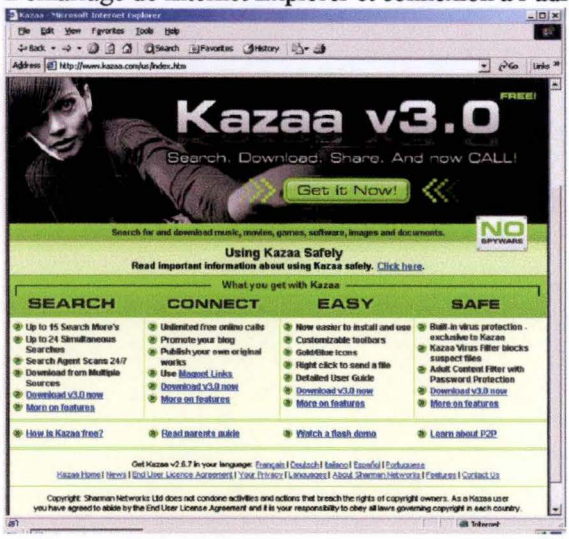


Figure 38 : Page d'accueil de Kazaa

Le site nous met en confiance, il affiche un logo « No Spyware », l'installation peut démarrer dès la fin du téléchargement.

- Téléchargement du produit et installation

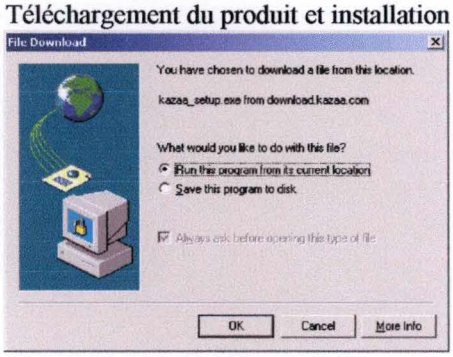


Figure 39 : Téléchargement et installation de Kazaa

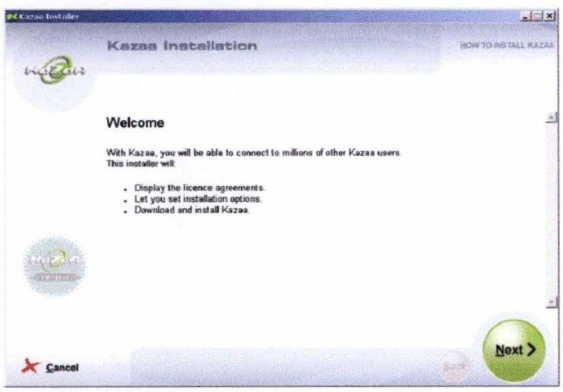


Figure 40 : Démarrage de l'installation de Kazaa

Un des écrans d'installation[93] nous prévient que l'installation comporte une protection anti-virus Bullguard et probablement un outil de recherche dénommé « Altnet Topsearch ».
La gratuité du produit découle de l'usage d'annonces publicitaires de Cydoor, The Best Offers, InstaFinder et RXToolbar.

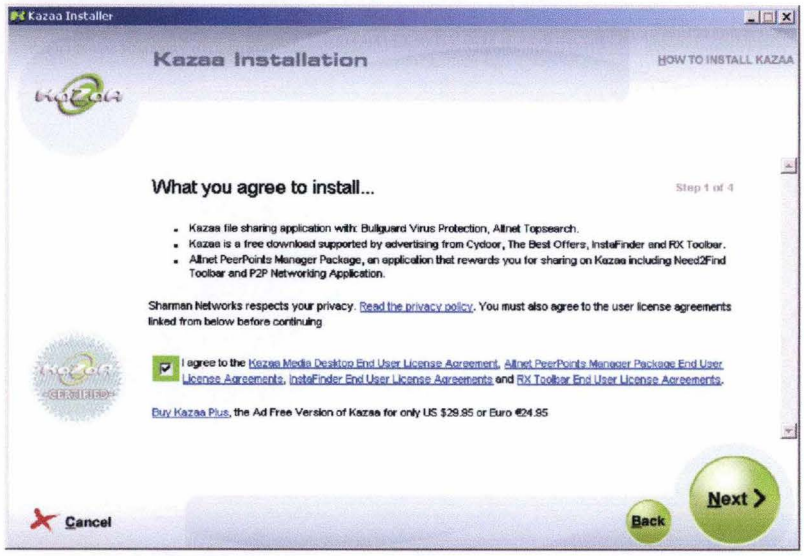


Figure 41 : Installation Kazaa, accord d'installation

Un simple « Next » valide notre accord. Quelques écrans se succèdent pour arriver finalement au premier écran de démarrage de Kazaa.

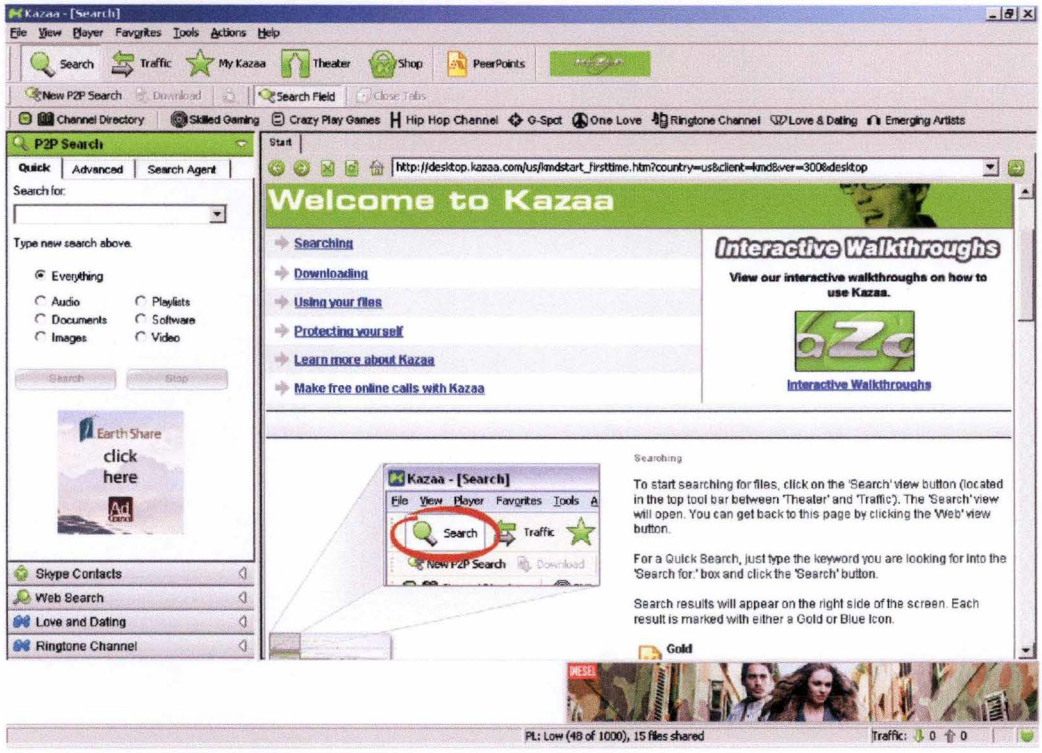


Figure 42 : Kazaa, premier démarrage

Après l'installation, on démarre une nouvelle session Internet Explorer et on peut faire le constat suivant :
- de nouvelles icônes sont apparues sur le bureau (« Free Casino » et « Play Poker »),

[93] Tous les écrans de l'installation de sont en annexe dans la rubrique intitulée « Installation KaZaA »

- deux nouvelles barres de recherche sont greffées à Internet Explorer

Figure 43 : Kazaa, premier démarrage d'Internet Explorer

Notons que dès le premier démarrage de Kazaa, on voit apparaître des fenêtres publicitaires en série, qui s'ouvrent au fur et à mesure qu'on en ferme. Ces annonces proviennent apparemment toutes du site http://ad.yieldmanager.com, voici par exemple :

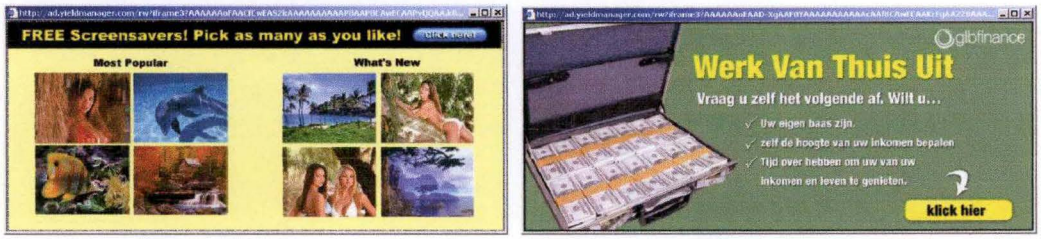


Figure 44 : pop-ups de Yieldmanager

Après investigations prises sur Kazaa, notons que la version précédente installait les logiciels espions de la famille Gator (GAIN Network et GAIN Office Compagnon). Ce n'est visiblement plus le cas dans cette version.

4. Scan Anti-Spy

Description Analyse du système par Spybot Search & Destroy

Tâches
- Démarrage de Spybot S&D
- Analyse du système

Résultats et observations

Résultat de l'analyse du sytème :

Figure 45 : Kazaa, résultat d'analyse de Spybot S&D

Spybot trouve donc 51 objets suspects installés sur le système, ces objets étant liés à : AltNet, CommonName, Cydoor, InstaFind, MyWay.MyBar, SpyShield et Sumom.A.

AltNet

AltNet (ALTernate NETwork) est une technologie de réseau développée par The Brilliant Digital. Elle s'appuie sur la même technologie P2P de FastTrack permettant de transformer chacun de nos ordinateurs en un nœud d'un réseau captif totalement privé. The Brillant Digital s'approprie ainsi la puissance de calcul inutilisée (en moyenne 80% de la puissance des ordinateurs), de la bande passante Internet, des surfaces disques (pour faire du stockage réparti) et de la mémoire Ram (pour en faire de la mémoire cache de son réseau) des utilisateur repris dans ce réseau, pour des travaux commerciaux d'informatique distribuée qui lui sont strictement personnels et qu'il revend à ses clients (dont DoubleClik)

CommonName[94]

CommonName Toolbar est un spyware de la société CommonName Ltd.
CommonName crée des raccourcis vers des pages Internet.
La page relative à la vie privée est claire :
« Nous pouvons vendre ou passer l'information qui vous est personnellement identifiable à des organisations précautionneusement sélectionnées en lesquelles vous pourriez être intéressé »
« Si vous installez ce logiciel et utilisez le service CommonName pour localiser un site web, CommonName collecte des informations personnellement identifiables tels que votre nom, le nom de votre société, votre numéro de téléphone, votre adresse, votre email, votre pays de résidence et votre code postal afin de fournir un service plus approprié.[…] ».
Notons que même si une entrée CommonName est décelée, ce spyware semble ne pas être réellement installé. Peut-être s'agit-il d'une trace d'installation oubliée car Kazaa installait cet espion dans les précédentes versions.

---

[94] CommonName Ltd (http://www.commonname.com), la fiche produit est consultable à l'adresse http://www.commonname.com/english/ug/toolbar/default.asp, et les informations relatives à la vie privée sur http://ww.commonname.com/English/Master.asp?asp=/English/LegalDocs/PrivacyPolicy.html.

Cydoor[95] Cydoor est un produit de Cydoor Desktop Media qui a longtemps utilisé un identifiant unique (GUID) pour tracer chaque utilisateur mais il a affirmé avoir arrêté cette pratique depuis la dernière version.
Parmi les fonctionnalités de Cydoor, notons les éléments suspects suivants :
- il télécharge du code exécutable,
- il transmet les informations fournies par l'utilisateur à des fins « d'études démographiques » et les communique à des tiers sous forme agrégée,
- il utilise les cookies et profile l'utilisateur à des fins publicitaires.

InstaFink InstaFink correspond au produit InstaFinder de la société InstaFinder.com.
InstaFinder est un pirate de navigateur qui redirige vers le portail d'InstaFinder.com toutes les requêtes sur base de mots clés.

SpyShield SpyShield est le module adware livré avec Best Offers qui provoque l'ouverture de fenêtres publicitaires contextuelles.[96]

Sumum.A Sumum.A est un vers qui se répand via MSN et les logiciels de partage de fichiers. Il se copie dans les répertoires systèmes et modifie les entrées dans le fichier hosts pour bloquer l'accès aux sites de la plupart des éditeurs d'anti-virus. Il tue également toute une série de processus pouvant le mettre en péril.[97]

5. Reboot

Description Redémarrage du système

Tâche
- Redémarrage,
- lancement du produit.

Résultats et observations

Au démarrage, les performances du système s'écroulent complètement, il prend plusieurs minutes à terminer l'ouverture de session.
Une invite à l'installation de Bullguard s'affiche, on ferme la fenêtre (bouton « Cancel ») pour ne pas surcharger, c'est déjà bien assez pour l'instant.

Figure 46 : Kazaa, installation de Bullguard

[95] Cydoor (http://www.cydoor.com), la page relative à la protection de la vie privée est disponible sur http://www.cydoor.com/Cydoor/Company/CompanyPrivacy.html.

[96] McAfee, Adware-SpyShield, http://vil.nai.com/vil/content/v_138885.htm, (mise à jour le 3 mars 2006)

[97] Viruslist.com, IM-Worm.Win32.Sumom.A, http://www.viruslist.com, (mise à jour le 10 mars 2005)

Des fenêtres de téléchargement de fichiers en provenance de ad.yieldmanager.com s'ouvrent successivement et les offres publicitaires de tardent pas à s'afficher en avant plan.

Figure 47 : Téléchargement d'annonce de Yieldmanager

L'utilisation de la mémoire a triplé, des alertes de saturation mémoire surviennent.

Lors du démarrage de l'outil Spybot S&D, probablement dû à une saturation mémoire, certaines fenêtres se figent, il devient difficile de travailler. L'ordinateur est alors redémarré.

Au redémarrage suivant, on reçoit une alerte de Spybot qui a avorté des processus qu'il considère malicieux, relatifs à AltNet

Figure 48 : Spybot, interruption de processus Altnet

Pour l'expérience, on permet l'exécution de ces processus en désactivant la protection active de Spybot. Le module résident est donc désactivé et le système est redémarré à nouveau.
Pour constater éventuellement quelque chose de nouveau, on procède à un démarrage du produit et une session Internet Explorer sur sa page de démarrage.
Les annonces publicitaires ne tardent pas à affluer et un panneau d'avertissement nous signale des erreurs dans la base de registre (le but étant bien sur de forcer le téléchargement d'un autre produit)

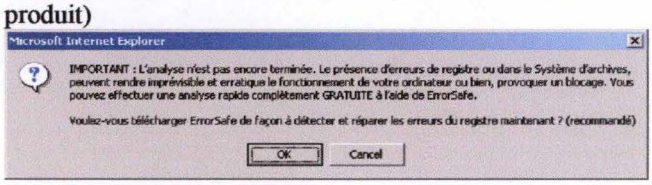


Figure 49 : Fausse alerte d'inconsistance de la base de registres

Par curiosité, on effectue une recherche d'inconsistance dans la base de registre par Spybot S&D qui n'en trouve évidemment aucune.

6. Scan Anti-Spy

Description Analyse du système par Spybot Search & Destroy

Tâches - Démarrage de Spybot S&D,
- analyse du système.

Résultats et observations

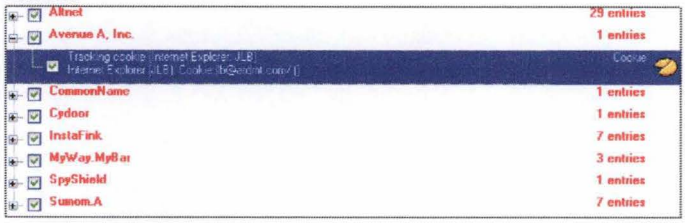


Figure 50 : Kazaa, résultat d'analyse Spybot après redémarrage

L'analyse ne décèle aucun nouvel élément si ce n'est un cookie de traçage vers Avenue A, agence de marketing (voir ci-dessous)

Avenue A tel qu'expliqué par le directeur général de Avenue A en France « Avenue A se positionne comme une réponse au développement exponentiel de la publicité et du marketing sur Internet. Grâce au système des cookies, la société est à même de connaître les habitudes d'utilisation d'Internet par une grande partie des utilisateurs américains. La société profite du fait que seulement 1,5 % des personnes prennent le temps de supprimer régulièrement les cookies de leur ordinateur. Grâce à une technologie propriétaire, Avenue A a développé tout un système d'enregistrement de données et d'analyse en temps réel des campagnes publicitaires. » [SAN01]

7. Cleanup

Description Nettoyage du système par Spybot Search & Destroy

Tâches - Fermeture des modules applicatifs liés à Kazaa
- Correction des problèmes détectés par l'outil anti-spyware

Résultats et observations

Les programmes résidents sont fermés à l'aide des icônes figurant sur la barre de démarrage.

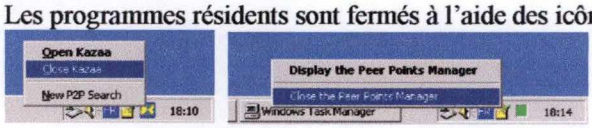


Figure 51 : Kazaa, fermeture du Peer Point Manager

Le nettoyage ne peut se faire directement, un redémarrage est nécessaire pour terminer le travail.

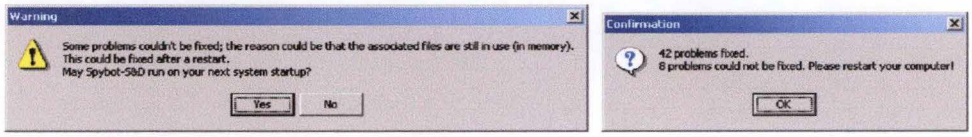


Figure 52 : Kazaa, résultat après nettoyage de Spybot

Les éléments restants correspondent à des fichiers exécutables ou des libraires en cours d'utilisation relatifs à AltNet.

8. Reboot

Description Redémarrage du système

Tâches
- Redémarrage du système
- Lancement de l'application Kazaa

Résultats et observations

Au démarrage, le nettoyage par Spybot se poursuit, les éléments qui étaient verrouillés avant le redémarrage sont corrigés.

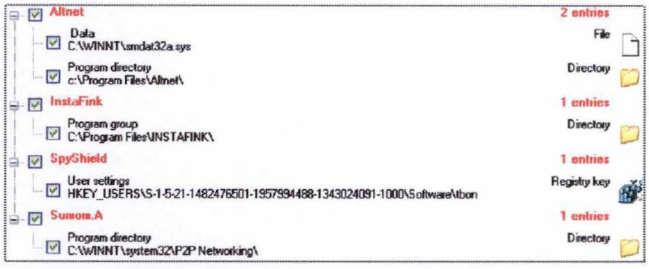


Figure 53 : Kazaa, nettoyage Spybot après redémarrage

9. Scan Anti-Spy

Description Analyse du système par Spybot Search & Destroy

Tâches
- Démarrage de Spybot S&D
- Analyse du système

Résultats et observations

Le dernier scan, malgré le nettoyage, fait apparaître à nouveau AltNet, Cydoor et SpyShield.

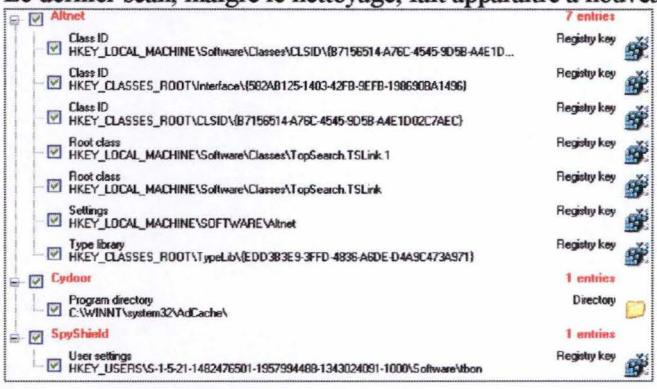


Figure 54 : Kazaa, analyse Spybot après nettoyage

Vu que les éléments persistent, on décide alors de procéder à la désinstallation complète du produit. Dans le panneau d'ajout/suppression de programme de Windows on peut voir les différents éléments installés avec Kazaa :
- Need2Find Bar
- P2P Networking
- Peer Point Manager
- RX Bar
- The Best Offer

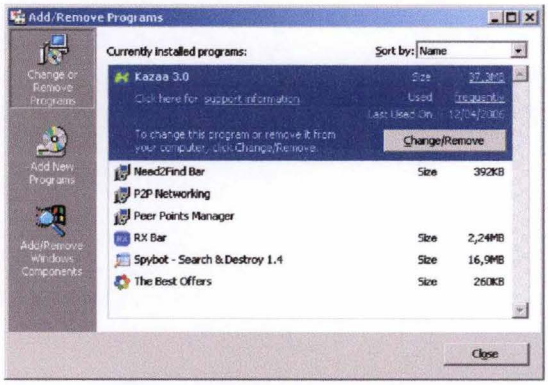


Figure 55 : Kazaa, Ajout/Suppression de programme de Windows

Figure 56 : Kazaa et RXToolbar, confirmation de la désinstallation

Le désinstallateur démarre alors une session Internet Explorer sur son site pour s'informer des raisons qui nous ont poussés à désinstaller le produit.

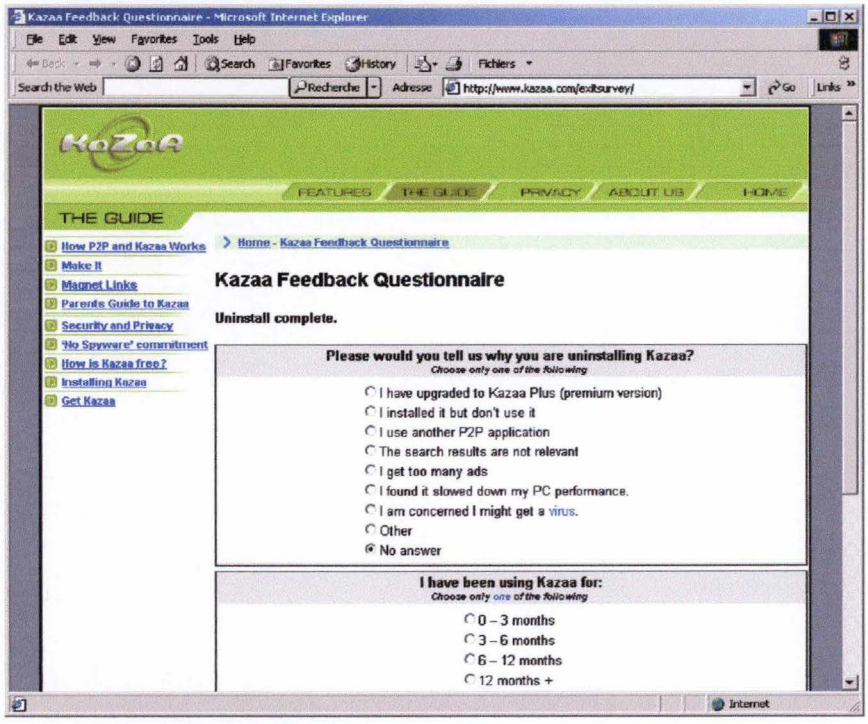


Figure 57 : Kazaa Feedback Questionnaire

Après avoir supprimé Kazaa et toutes ses dépendances, on relance le module d'ajout/suppression de programmes pour vérifier que c'est effectivement désinstallé.

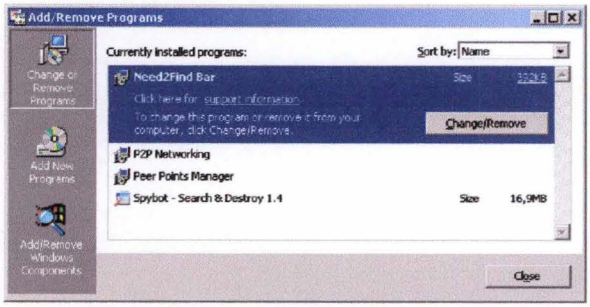


Figure 58 : Modules Kazaa, Ajout/Suppression de programmes de Windows

On remarque que les modules Need2Find Bar, P2PNetworking et Peer Point Manager. Comme le panneau d'avertissement de désinstallation demande un redémarrage de la machine, redémarrons et revenons à ce point pour voir si quelque chose a changé.
Après redémarrage, ces modules sont toujours installés, la suppression se fait alors un par un. :
- Need2Find Bar :

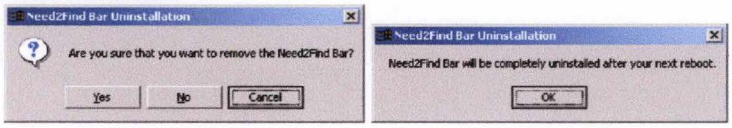


Figure 59 : Need2Find Bar, confirmation de désinstallation

- P2PNetworking :

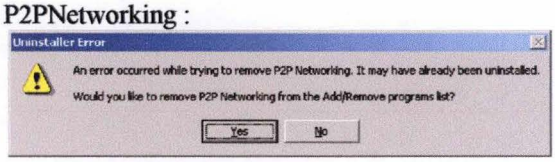


Figure 60 : P2P Networking, désinstallation

- Peer PointManager :

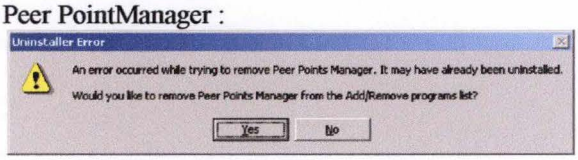


Figure 61 : Peer Point Manager, désinstallation

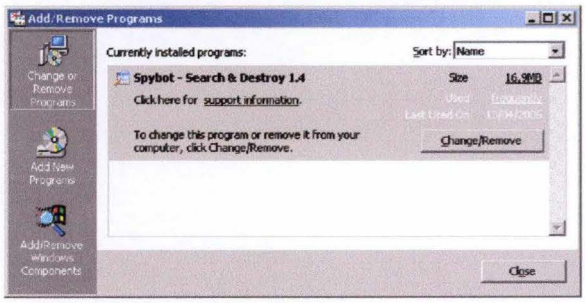


Figure 62 : Ajout/Suppression de Programmes de Windows après désinstallation

Il semble que les éléments soient effectivement supprimés mais la désinstallation nécessite un redémarrage, qui est fait immédiatement.
Un dernier scan Spybot S&D est alors lancé pour s'assurer que le système est maintenant sain.

Le résultat du scan nous révèle la présence persistante des éléments AltNet.

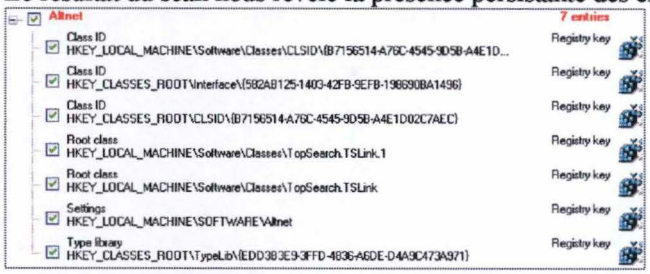


Figure 63 : Altnet, analyse après désinstallation

Tentons le nettoyage par Spybot S&D encore une fois, tous les problèmes semblent être résolus.

Figure 64 : Altnet, nettoyage après désinstallation

Pour en être certain, redémarrons encore une fois la machine avant de ré-exécuter une nouvelle analyse par Spybot S&D. Le nouveau scan ne décèle plus aucun élément suspect.

3.4.7 Scenario 2 : Claria ScreenScenes

0. Init

Le système est réinitialisé à partir du CD-Rom d'installation.

1. Install Anti-Spy

Description Installation de Spybot S&D

Tâches
- Démarrage du navigateur Internet Explorer,
- navigation sur la page de téléchargement de l'anti-spyware (http://www.safer-networking.org),
- lancement de l'installation du produit.

Les étapes de téléchargement et d'installation de Spybot S&D sont illustrées en annexe sous la rubrique « Installation de Spybot S&D ».

2. Scan & cleanup

Description Analyse du système par Spybot Search & Destroy

Tâches
- Démarrage de Spybot S&D
- Vaccination du système
- Analyse du système
- Résolution de tous les problèmes détectés

Résultats et observations

Cette étape est identique à celle exécutée pour l'expérience avec Kazaa à la différence qu'on n'a pas activé l'option de détection de traçage.

Tout comme dans le premier cas de figure, l'analyse détecte et corrige l'élément lié à Alexa.

3. Install ScreenScenes

Description Installation de ScreenScenes

Tâches
- Démarrage d'Internet Explorer et connexion à l'adresse http://www.claria.com pour trouver l'économiseur d'écran qui nous intéresse
- Lancement de l'installation du produit

Résultats et observations

La navigation sur le site de Claria nous conduit sur la page de téléchargement des économiseurs d'écran, choisissons par exemple la cascade animée intitulée « Magic Waterfall » (http://www.screenscenes.com/product.html?screensaver=MagicWaterfall).

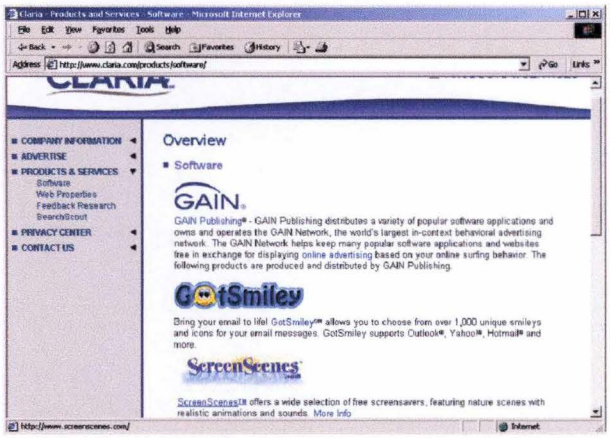


Figure 65 : Page de téléchargement des produits Claria

Notons que cette page a été sélectionnée volontairement pour les besoins du laboratoire. On n'arrive cependant que très rarement par ce biais à l'installation du produit. En général, c'est en naviguant sur des sites autres que Claria qu'on peut se voir proposer l'installation d'un économiseur d'écran en un simple click sur l'image proposée (ou imposée) sous la forme d'une bannière publicitaire sur des sites de sociétés partenaires ou de pop-up tel que celui présenté ci-dessous.

Figure 66 : Pop-up ScreenScenes

Figure 67 : Page de téléchargement des ScreenScenes

Par la page de téléchargement de Claria, notons que l'explication de la gratuité du produit se trouve en bas de page dans un encart explicite :

Why are ScreenScenes screensavers free?
ScreenScenes screensavers are provided free, because they are supported by advertising from the GAIN Network, which helps keep many popular software applications free in exchange for delivering advertising. As you surf the Web, you will occasionally see GAIN branded ads (pop-ups and others) selected based on your online activities. These ads are displayed by GAIN AdServer Software - not by any Web site. Click here to get ScreenScenes screensavers with no GAIN advertising for $30 each.

Figure 68 : Justification de gratuité des produits Claria

Désireux et pressé d'installer ce merveilleux décors animé, on clique sur "Download Now", Windows demande confirmation pour l'installation du produit signé par GAIN Publishing, qui assure que le contenu est sécurisé, donc rien à craindre en théorie.

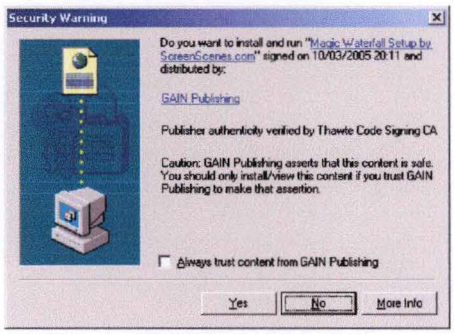


Figure 69 : Téléchargement certifié GAIN Publishing

L'installation démarre automatiquement mais Spybot réagit en interceptant un changement relatif aux ActiveX dans la base de registres.

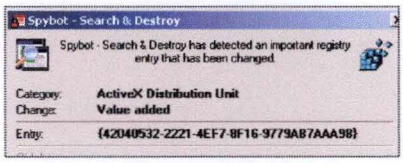


Figure 70 : Alerte Spybot sur la base de registre (ActiveX)

Pour éviter ces interférences, désactivons d'abord le programme résident de Spybot S&D avant de poursuivre.

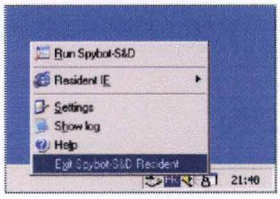


Figure 71 : Désactivation du résident Spybot

L'installation peut donc se poursuivre et se terminer[98]
Afin de voir si l'économiseur d'écran est correctement installé, on lance son activation par l'intermédiaire du panneau de réglage de l'affichage Windows.

[98] Les écrans d'installation de Magic Waterfall ScreenScenes sont disponibles en annexe sous la rubrique « Installation de GAIN Magic Waterfall ScreenScnenes »

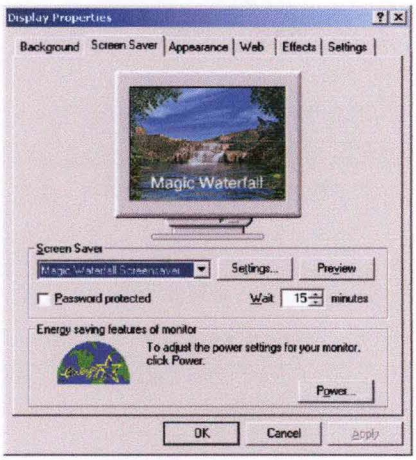


Figure 72 : Activation de l'économiseur d'écran ScreeScenes

Le bouton « preview » lance bien l'économiseur d'écran « Magic Waterfall ».

4. Scan Anti-Spy

Description Analyse du système par Spybot S&D

Tâches
- Démarrage de Spybot S&D
- Scan Spybot S&D

Résultats et observations

L'analyse détecte deux catégories d'éléments : GAIN DashBar et GAIN Gator

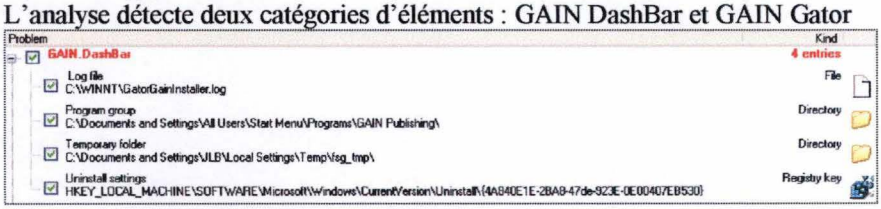


Figure 73 : Résultat d'analyse Spybot (GAIN DashBar)

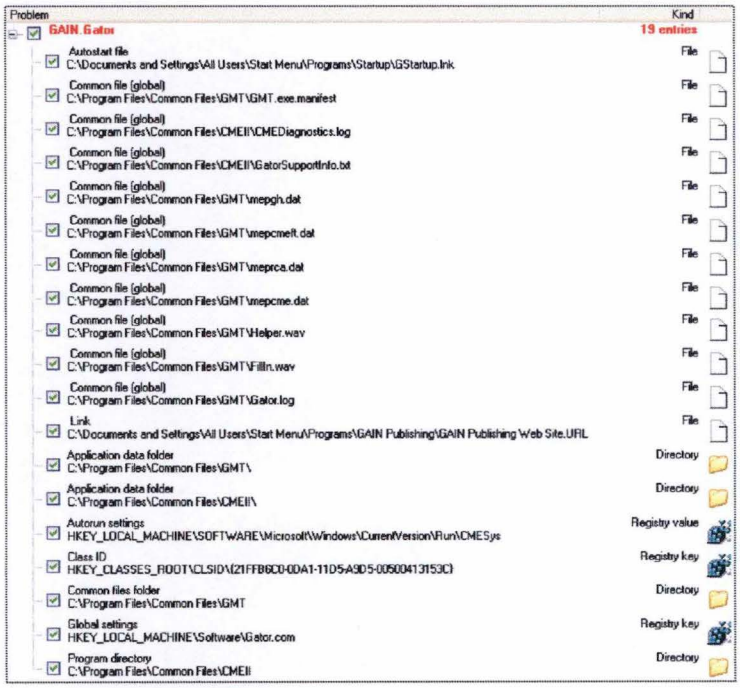


Figure 74 : Résultat d'analyse Spybot (GAIN.Gator)

GAIN.DashBar DashBar est une extension du navigateur Internet Explorer sous la forme d'une barre d'outils de recherche. DashBar permet d'entrer les critères de recherche directement dans un champ de recherche dans la barre d'outils. Par défaut, ce champ est automatiquement mis à jour en fonction des habitudes de navigations. Lorsqu'on laisse le pointeur de souris sur ce champ de recherche, il ouvre automatiquement une nouvelle fenêtre avec le résultat.

En cliquant sur la page de résultat de la recherche, le navigateur se connecte chez un intermédiaire fournisseur du service de recherche pour arriver finalement sur la page de destination. En plus de la page de destination, des données cryptées sont transmises au fournisseur. Dans les versions précédentes de DashBar, les données étaient en clair sous forme de texte, et contenait les informations suivantes : les critères de recherche, la langue de l'utilisateur, la date et l'heure, un identifiant et la localisation de la page de résultat. Le fait d'amener le client par la page d'accueil du fournisseur permet également de collecter l'adresse IP du visiteur.[99]

GAIN.Gator Gator est le module adware, qui se charge de rapatrier et d'afficher les annonces publicitaires.

3.4.8 Conclusion

L'idée de départ de cette démonstration était centrée sur Gator. Lors de la rédaction de l'étude théorique, celui-ci figurait clairement sur la page de présentation de Kazaa (« Advertising - delivered by Cydoor and the GAIN Network »). Il a été constaté au cours de l'expérience que Gator n'était pas installé avec Kazaa. Partant de ce constat, des renseignements sont pris sur Kazaa : Gator a été supprimé du paquetage depuis la version distribuée après le 16 août 2005. Le contenu de ce paquetage est affiché clairement durant le processus d'installation et les conditions générales de licence y sont accessibles, de même que les conditions de licence de chaque module annexe.

Il n'y a pas vraiment de surprise du coté du ScreenScene, Claria annonce clairement le mode de fonctionnement de la version gratuite : elle est supportée par l'affichage de publicités provenant d'Internet, dont la sélection et l'affichage sont gérés par Gator. Notons que l'économiseur d'écran est téléchargé sur le site de l'éditeur mais ce n'est pas toujours le cas, Claria ayant des contrats de distribution avec d'autres sociétés présentes sur la toile.

[99] Nye Dan, F-Secure Spyware Information Page: DashBar, http://www.f-secure.com/sw-desc/dashbar.shtml (mis à jour le 17 novembre 2005)

3.5 Démonstration 2 : eMedia Codec

3.5.1 Hypothèse

Notre utilisateur a reçu dans sa boite aux lettres une séquence vidéo humoristique envoyée par un ami. Il ouvre donc le fichier pour en visionner le contenu mais il reçoit un message lui indiquant que son ordinateur ne dispose pas du décodeur vidéo approprié et suggère de le télécharger. Il s'agit du décodeur d'eMedia téléchargeable gratuitement. Procédons donc à cette installation, d'autant que c'est visiblement un codec plus performant au niveau audio et une meilleure compression vidéo.

3.5.2 Méthode

Le but de l'expérience n'est pas de montrer de quelle manière on peut se défaire d'un logiciel tel qu'eMedia Codec, mais de démontrer les hypothèses suivantes :

- n'importe quel logiciel aux allures innocentes peut contenir du code malicieux ;
- un spyware peut engendrer l'installation d'un autre spyware ou autre code malicieux, et générer une réaction en chaîne de type pyramidal ;
- le logiciel espion vient rarement seul, il n'est souvent qu'une composante d'un lot de code malicieux. Il est vecteur de distribution d'adware (ou l'est lui-même) ou virus (généralement de type cheval de Troie) et constitue de ce fait un réel problème de sécurité pour un système informatique.

Pour ce laboratoire, deux logiciels anti-spywares sont mis en concurrence afin de vérifier la réaction de chacun face à l'installation d'un logiciel tel que celui-ci : Spyware Quake et Spybot Search & Destroy

3.5.3 Diagramme de séquence

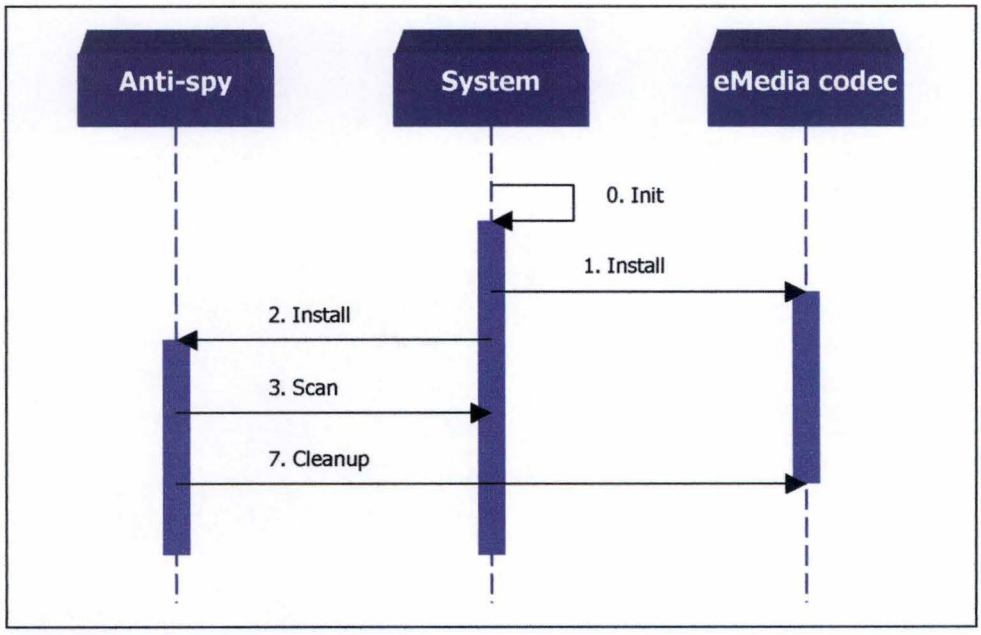


Figure 75 : test eMedia codec, diagramme de séquence

3.5.4 Scenario 1 : SpywareQuake

1. Installation

Description Installation du codec vidéo d'eMedia

Tâches - Démarrage de Internet Explorer et connexion à l'adresse http://www.emcodec.com ,
- téléchargement et installation du pilote.

Résultats et observations

Démarrage de Internet Explorer et connexion à l'adresse http://www.emcodec.com

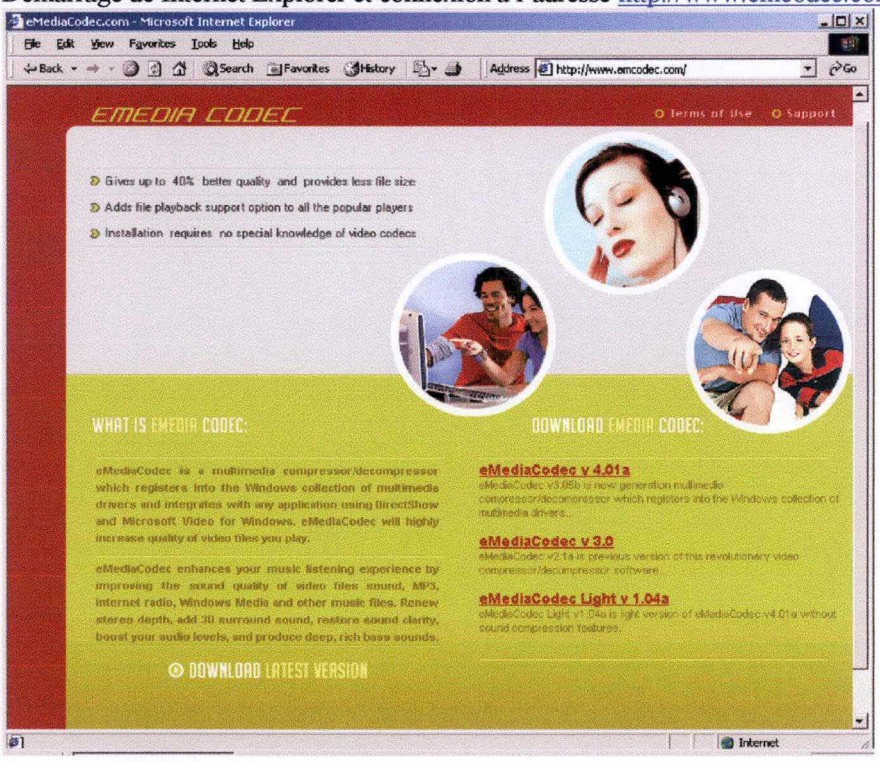


Figure 76 : EMedia Codec, page d'accueil

On lance alors l'installation en cliquant sur le lien « download ».

Rappelons que la protection active de Spybot a été volontairement désactivée afin d'autoriser le téléchargement et l'installation du produit. Une fois installé, l'ordinateur est resté quelques heures sans activité, durant ce temps une quinzaine de fenêtres publicitaires, principalement relatives à des logiciels anti-spyware, ainsi que des sites de rencontres « pour adulte » et de casinos en ligne ont fait leur apparition.

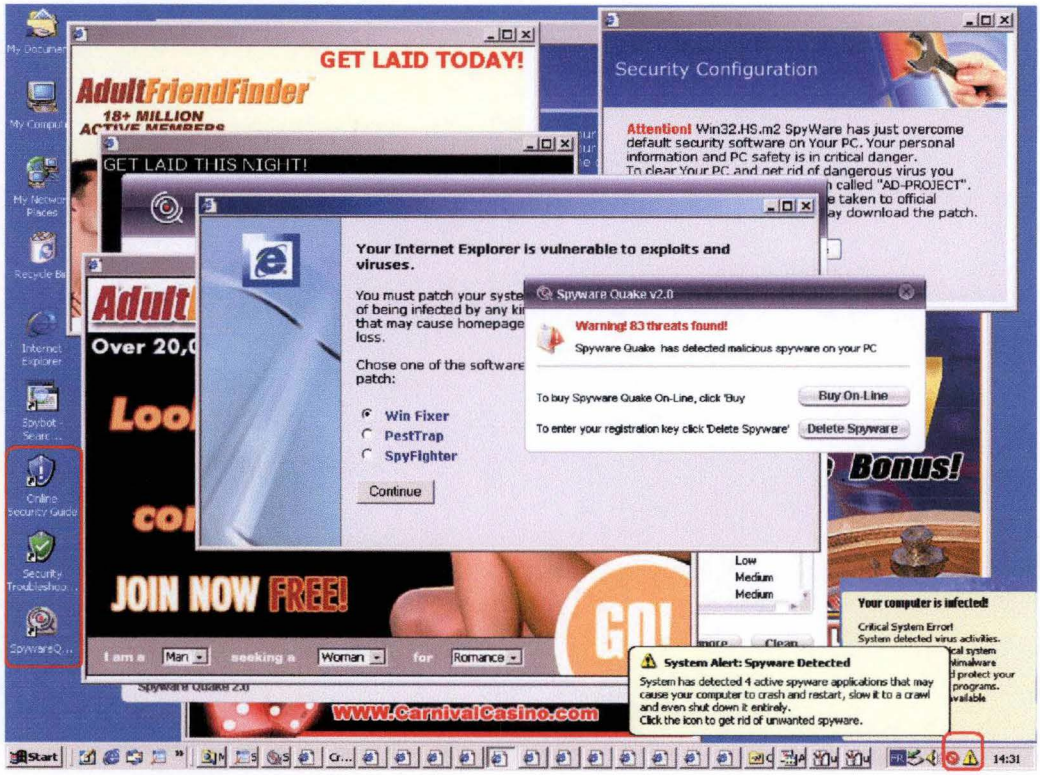


Figure 77 : eMedia Codec bureau pollué de pop-ups

Des nouvelles icônes ont fait apparition également sur le bureau, qui est bombardé de messages d'alerte virus et spyware. Au vu du contenu de la barre de démarrage, il semble que de nouvelles applications soient installées, vérifions-le dans le panneau d'ajout et suppression de programmes.

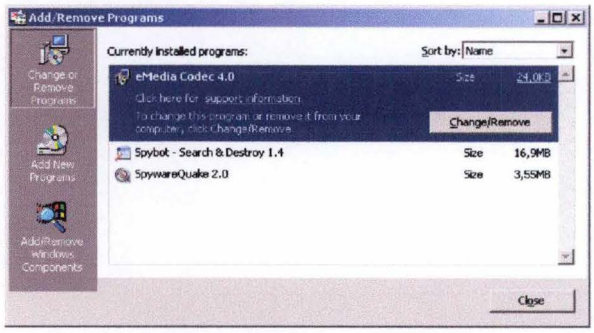


Figure 78 : eMediaCodec et SpywareQuake, Ajout/Suppression de Programmes

On constate effectivement qu'un logiciel nommé « SpywareQuake » a été également installé.
En basculant sur la fenêtre de cet outil anti-spyware, on constate qu'il a détecté 83 éléments malicieux ou suspects.
Examinons alors ce nouvel outil anti-spyware. Il détecte une série d'éléments liés à l'installation de Kazaa, que Spybot n'aurait pas détecté.

Kazaa a installé une série d'éléments qui restent sur le système malgré une désinstallation complète du produit.
Lorsque eMedia codec est installé, on voit apparaître conjointement l'installation d'un outil anti-spyware : « SpywareQuake ». Ce dernier trouve beaucoup d'éléments non détectés par Spybot.
La question se pose donc, quel est l'anti-spyware le plus fiable ? Les espions installés proviennent-ils du codec nouvellement installé ou d'un résidu de l'installation de Kazaa ?
Le seul moyen de faire la part des choses est de repartir sur une base propre en remettant le système dans son état de base.
Ce qui nous conduit à recommencer l'analyse en isolant eMedia Codec et en faisant alors une comparaison de logiciels anti-spyware vis-à-vis de ce produit.

Notons que cette étape est le résultat d'un test hasardeux, le codec a été installé sur le système tel qu'il a été laissé par l'expérience précédente pour voir d'éventuelles interractions entre un résidu spyware et une nouvelle installation. La constatation de l'installation de SpywareQuake a été le facteur qui a déterminé le but de l'expérience. Ayant découvert ainsi un nouveau anti-spyware, il a été décidé de comparer les résultats de cet outil avec l'anti spyware de référence (Spybot S&D).

0. Réinitialisation

Le système est réinstallé complètement à partir de l'image de Windows sur CD-Rom, l'expérience peut recommencer à sa première étape.

1. Installation du logiciel eMedia Codec

Description Installation du codec vidéo d'eMedia

Tâches - Démarrage d'une session Internet Explorer sur http://www.emcodec.com,
- téléchargement et installation du produit.

Résultats et observations

Les étapes de l'installation sont identiques à celles décrites lors de la première installation. Remarquons cependant que seul le codec est installé, aucun logiciel parasite annexe ne semble être installé.

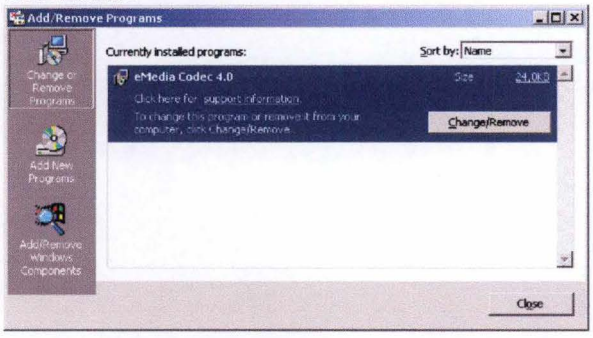


Figure 79 : eMedia Codec, Ajout/Suppression de Programmes

2. Installation du logiciel anti-spyware : SpywareQuake

Tâches - Démarrage d'une session Internet Explorer sur la page http://www.spywarequake.com
- Téléchargement et installation du produit

Résultats et observations

La page d'accueil propose d'emblée un scan gratuit sans engagement.

Figure 80 : Page d'accueil de SpywareQuake

Le bouton intitulé « free scan » lance le téléchargement du produit.

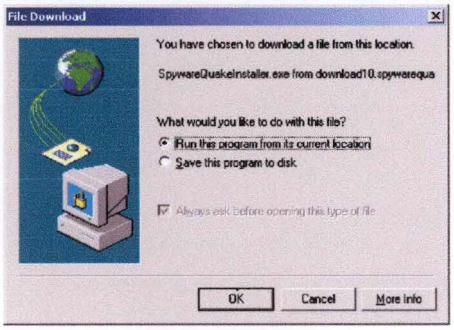


Figure 81 : SpywareQuake, téléchargement

Les illustrations des étapes d'installation sont en annexe sous la rubrique « Installation de SpywareQuake »
A la fin de l'installation, l'analyse du système est effectuée par SpywareQuake qui détecte 7 éléments malveillants liés au Codec

3. Scan SpywareQuake

Tâches - Redémarrage du système
- Lancement de SpywareQuake

Résultats et observations

Afin de finaliser l'installation, l'ordinateur est redémarré, l'analyse du système est effectué automatiquement par SpywareQuake qui ne détecte rien de plus qu'à son analyse précédente.

Après un jour et une nuit complète d'inactivité, des pop-up commencent à apparaître sur l'écran,

similaires à ceux décrits dans la première étape : alertes spyware, alerte aux virus, publicités pour casinos en ligne, publicité pour des sites de rencontre « pour adulte », des icônes supplémentaires apparaissent également sur la barre d'outil de Windows ainsi que sur le bureau (raccourcis vers des URL de site de concepteurs de produits de sécurité).

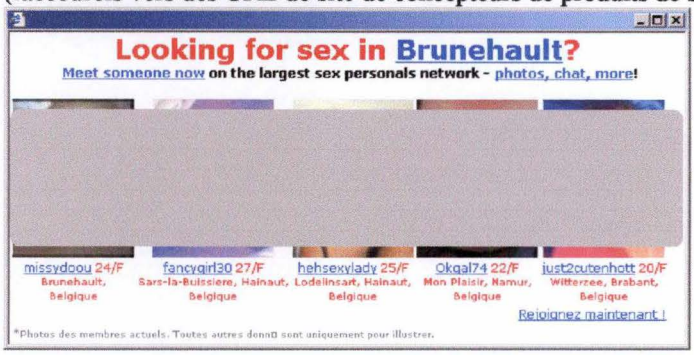


Figure 82 : Pop-up "adulte"

Remarquons que les annonces sont personnalisées dans le sens où, malgré une installation de Windows totalement en anglais, les annonces paraissent (partiellement) en français pour des annonces de filles en Belgique. Le navigateur est effectivement configuré pour recevoir les pages en français (de Belgique).

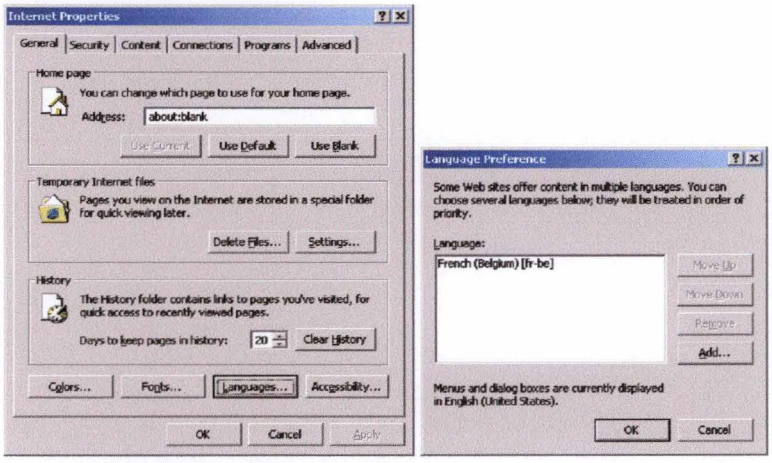


Figure 83 : Paramètres de langue dans Internet Explorer

Des fausses annonces d'alertes surgissent en utilisant des informations de l'entête HTTP et en les présentant de manière à effrayer un néophyte en affirmant que l'ordinateur est sous contrôle et qu'il faut absolument acheter les produits de sécurité présentés.

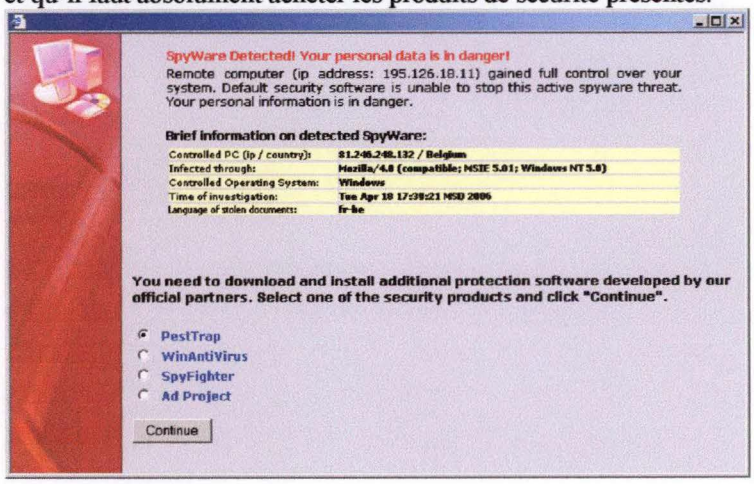


Figure 84 : Fausse alerte de sécurité (1)

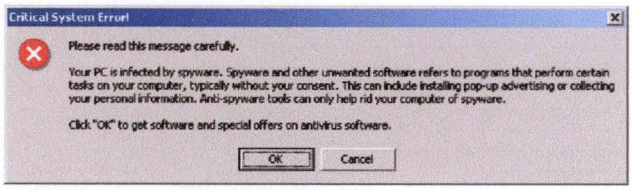


Figure 85 : Fausse alerte de sécurité (2)

Même les virus sont de la partie, les popups invitent à mettre à jour le système immédiatement.

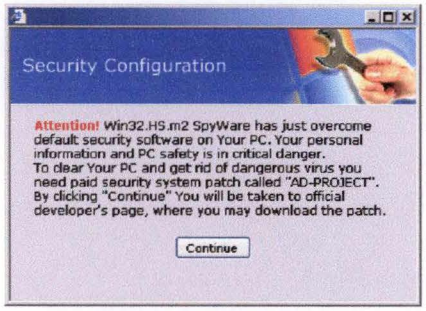


Figure 86 : Fausse alerte de sécurité (3)

Les exemples d'annonces du genre sont innombrables.

Le démarrage d'Internet Explorer est également pollué dans le même sens. Bien que la page de démarrage n'ait pas changé[100], l'ouverture d'Internet Explorer se fait sur une page d'alerte qui informe que le PC est contrôlé à distance et qu'une série de répertoires sur le disque dur sont accessibles. On est bien sûr invité à acheter une solution anti-spyware le plus vite possible.

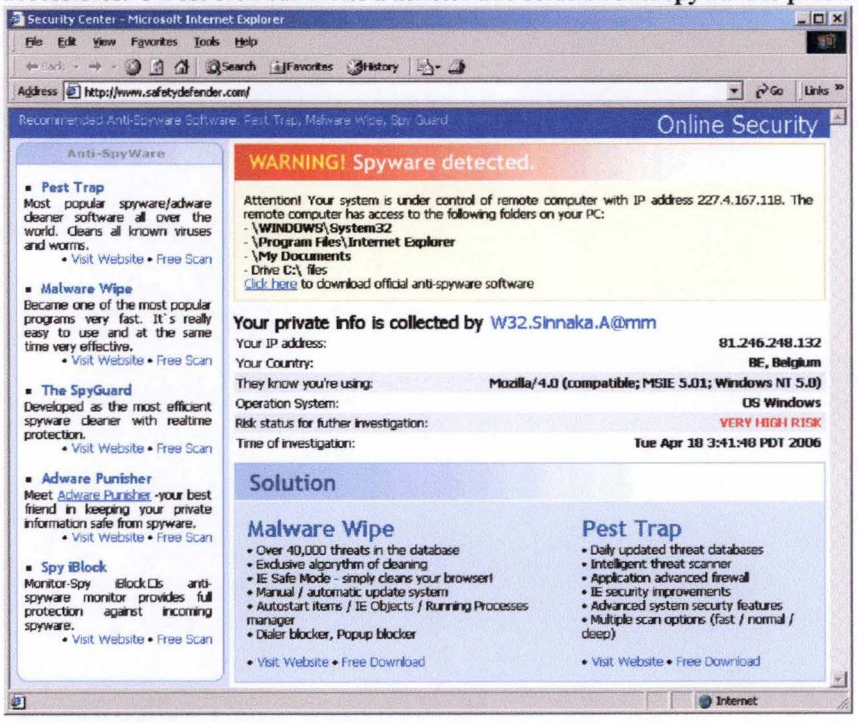


Figure 87 : Fausse alerte de sécurité dans Internet Explorer

[100] Il s'agit de l'action typique d'un Browser Hijack.

Nous démarrons finalement l'analyse du système avec le produit SpywareQuake

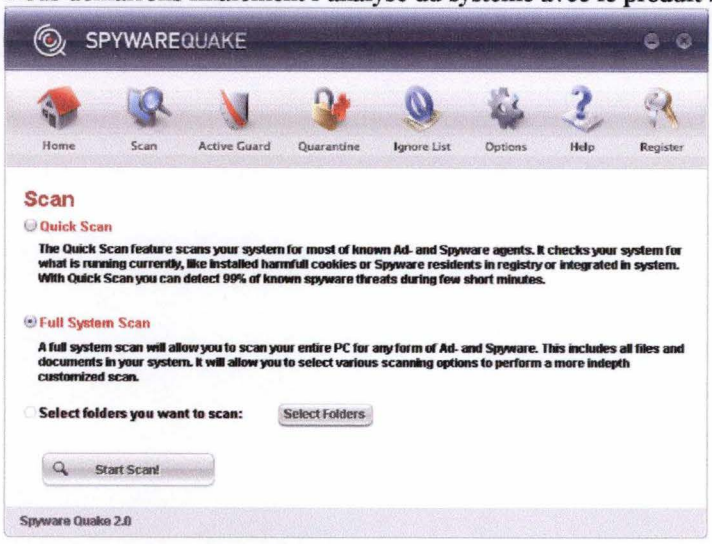


Figure 88 : SpywareQuake, démarrage

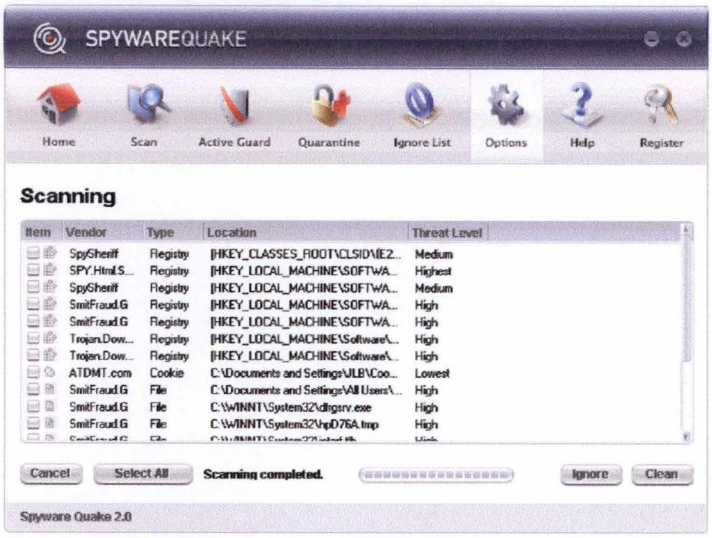


Figure 89 : SpywareQuake, analyse du système

Le scan de l'outil met cette fois en évidence 17 éléments répartis sous différentes formes (entrées dans la base de registres, fichiers ou libraires, cookie). Ceux-ci peuvent être regroupés par produit malicieux ou suspect :
- SpySheriff (registre et fichier),
- SmitFraud.G (registre),
- Trojan.Downloader.Slvr (registre et fichiers),
- ATDMT.com (cookie).

SpySheriff

SpySheriff est une application anti-spyware qui prétend enlever les logiciels espions malicieux mais nécessite le paiement d'un enregistrement avant que tout problème détecté puisse être résolu. Afin de forcer la main à l'achat d'une version complète du produit, il provoque l'ouverture de fenêtres d'alertes invitant l'utilisateur à acheter le produit complet le plus rapidement possible. Il se configure également pour un lancement automatique à chaque démarrage de Windows.[101]
La personne qui est détenteur du nom de domaine a une adresse de type « .RU », une adresse en Grèce, et un numéro de téléphone incorrect.

[101] McAfee, Adware-SpySheriff, http://vil.nai.com/vil/content/v_135033.htm (mis à jour le 27 décembre 2005) (consulté le 16 avril 2006)

Domain Name: SPYSHERIFF.COM

Registrant:
Popandopulos Ltd
Alison Popandopulos (crystaljones@list.ru)
2 Pyramid, Room 34
Chalkidiki
Chalkidiki,126322
GR
Tel. +001.4151**2345678**

Creation Date: 28-May-2005
Expiration Date: 28-May-2007

Notons que SpywareQuake est le successeur de SpyAxe qui est lui-même un produit dérivé de SpySheriff.

SmitFraud.G SmitFraud.G est une version récente du SmitFraud. Actuellement, seules les versions A et C semblent être répertoriées dans les bases publiques des éditeurs des logiciels anti-spyware et anti-virus (McAfee, PandaSoftware, PCTools, Kaspersky).

Trojan.Downloader.Slvr

Trojan.Downloader.Slrv est aussi répertorié sous le nom de « DesktopScam ».
Ce cheval de Troie est classé dans la catégorie des produits à risque élevé pour la sécurité.
Il est téléchargé conjointement à certaines applications de sécurité frauduleuses ayant pour seul but d'effrayer l'utilisateur et le pousser à l'achat d'autres programmes tout aussi frauduleux.
DesktopScam affiche des faux messages d'infection de l'ordinateur, ainsi que des fenêtres qui ont l'aspect du module de mise à jour automatique de Windows afin de donner l'impression que le rapport d'infection provient directement de Windows. Un clic sur une de ces notifications conduit sur une page de commande de logiciel de désinfection.[102]

4. Nettoyage SpywareQuake

Tâches Lancement de l'action de nettoyage du système.

Résultats et observations

On sélectionne tous les éléments incriminés et on clique sur le bouton intitulé « Clean » pour lancer le nettoyage. On tombe alors sur la page d'enregistrement du produit.

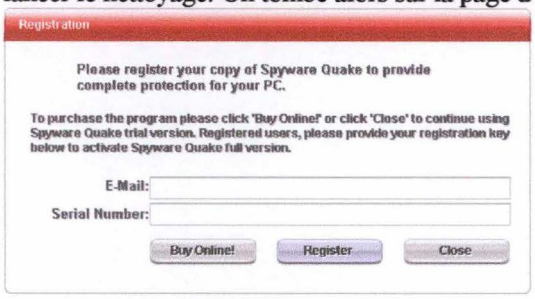


Figure 90 : SpywareQuake, enregistrement

[102] SunBelt SpyCounter, DesktopScam, http://research.sunbelt-software.com/threat_display.cfm?name=DesktopScam&threatid=43465 (consulté le 17 avril 2006)

Le nettoyage est impossible par SpywareQuake car il faut entrer une clé d'enregistrement que l'on peut commander en ligne moyennant environs $50. Le bouton « Buy Online » nous redirige vers le site marchand.

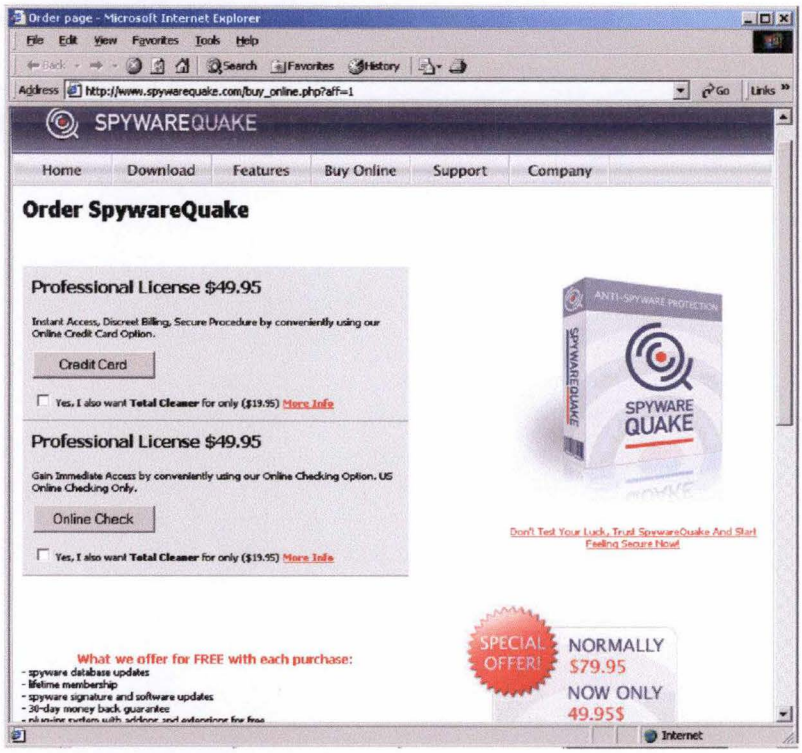


Figure 91 : SpywareQuake, commande en ligne

3.5.5 Scenario 2 : Spybot Search & Destroy

0. Réinitialisation

Le nettoyage est donc impossible avec SpywareQuake, et le scan donne un certain résultat. Afin de comparer ce résultat avec un autre outil anti-spyware, exécutons la même opération à l'aide cette fois de Spybot S&D. Le système est réinstallé complètement à partir de l'image de Windows sur CD-Rom.

1. Installation du logiciel eMedia Codec

Tâches - Démarrage d'une session Internet Explorer sur http://www.emcodec.com,
- téléchargement et installation du produit.

Résultats et observations

Le résultat est identique à la précédente réinitialisation.

2. Installation de Spybot S&D

Description Téléchargement et installation de Spybot Search & Destroy

Tâches - Démarrage du navigateur InternetExplorer,
- navigation sur la page de téléchargement de l'anti-spyware (http://www.safer-networking.org),
- lancement de l'installation du produit

Résultats et observations

Les étapes de téléchargement et d'installation de Spybot S&D sont illustrées en annexe sous la rubrique « Installation de Spybot S&D ».

Figure 92 : eMedia Codec et Spybot S&D

On peut voir qu'il n'y a que Spybot et eMedia codec installés sur l'ordinateur.
Cependant, on remarque également que les publicités et alertes aux spywares commencent à se manifester avant même que Spybot ne soit démarré pour la première fois.

3. Scan Spybot Search & Destroy

Description Analyse du système par Spybot Search & Destroy

Tâches
- Démarrage de Spybot S&D,
- configuration de l'outil pour une analyse approfondie,
- analyse du système.

Résultats et observations

Le tout premier rapport d'analyse est éloquent.

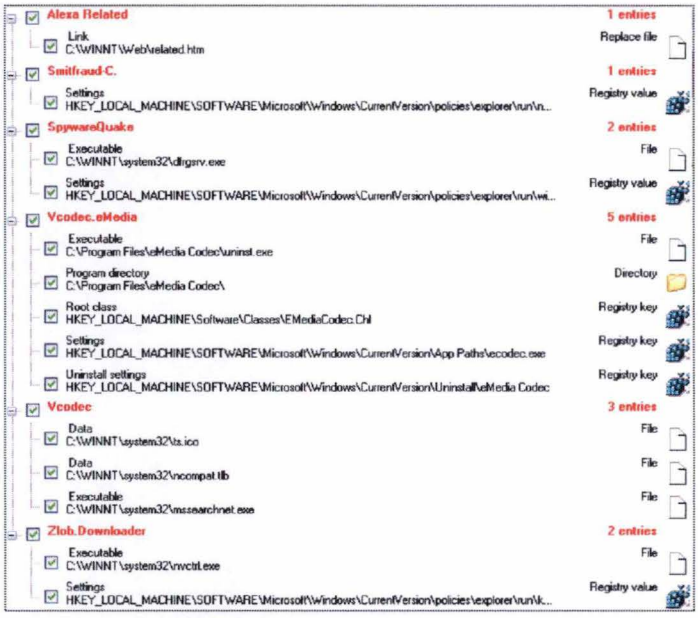


Figure 93 : eMedia Codec, résultat d'analyse Spybot

Etrangement, on se retrouve avec un élément relatif à SpywareQuake, bien que ce produit ne soit pas installé.
Examinons les éléments trouvés :

Alexa Cet élément a déjà fait l'objet d'une description et existe dès l'installation de base de Windows

SmitFraud.C SmitFraud existait dans la démonstration précédente, mais Spybot fournit une explication plus complète relative à cet élément [103] :
« Ce programme s'installe de lui-même au travers d'Internet et crée un fond d'écran. Celui-ci ressemble à l'écran bleu de crash système de Windows 98 et contient un message d'avertissement informant que l'ordinateur a contracté un virus pour lequel il faudrait lancer un scanner antiviral, et qu'il est incapable de fonctionner en mode normal.
En plus de cela, une icône apparaît sur le bureau qui conduit à une application soi-disant anti-virus appelée PSGuard. Ce programme rapportera la découverte d'un virus (que le logiciel a lui-même installé). Afin de pouvoir enlever ce virus, il faut télécharger une version complète qui coûte environs 20 €.
Un autre effet indésirable de SmitFraud-C est que des options de paramètres sont rendus indisponibles sur le panneau de configuration. De cette manière, il empêche l'utilisateur de changer son fond d'écran, l'obligeant ainsi à garder l'écran bleu.
Avant tout, SmitFraud-C est un logiciel furtif qui tente de vendre PSGuard en effrayant les utilisateurs inexpérimentés ».

SpywareQuake SpywareQuake a refait une apparition, Spybot en fournit la description suivante :
« La version de démonstration officielle semble s'installer correctement mais affiche énormément de fausses détections, la plupart intentionnelles dans le but de forcer l'utilisateur à acheter une version complète.
La version furtive est installée conjointement à Vcodec ou Zlob et est également capable de se réinstaller en piratant la séquence de démarrage et par le biais de pop-up d'alertes virales ».

Vcodec.eMedia

Fonctionnalité
"eMedia Codec", connu également sous le nom de "Stream Video Codec" est un compresseur/décompresseur multimédia.

[103] Traduit de l'aide du programme anti-spyware Spybot Search & Destroy.

Description
Installateur de malveillances. Il installe des logiciels malicieux tels que SpyGuard, WinFixer, WinAntiVirus Pro,...

Vie privée
« Installation logicielle : les composants paquetés avec le logiciel peut rapporter, à son éditeur ou à ses affiliés, le statut d'installation de certaines offres marketing, tels que des barres d'outils, ainsi que des informations générales telles que la préférence linguistique et la version du système d'exploitation, afin d'assister l'éditeur dans le développement de son produit. Aucune information personnelle ne sera communiquée à eMedia Codec Software ou à ses affiliés durant ce processus. L'éditeur peut offrir des composants supplémentaires par l'intermédiaire du système de mise à jour. Ces composants incluent : barre d'outils, publicités sous forme de pop-ups, gestionnaire de page de démarrage (Commercial homepage manager), Commercial messenger. »

Vcodec

Voici l'information fournie par Spybot :
« **Fonctionnalité**
VCodec est un compresseur/décompresseur multimédia de nouvelle génération, qui s'inscrit dans la collection de pilotes multimédia de Windows »

Description
Gestionnaire de téléchargement de code malicieux. Il change les ZoneMaps (ndla : Les ZoneMaps de Windows sont des entrées dans la base de registres qui servent à autoriser ou interdire l'accès à certains domaines Internet), il installe des malveillances telles que SpyAxe, PSGuard, AV-Gold et SmitFraud-C»
SpyAxe est le prédécesseur de SpywareQuake. PSGuard[104] et AV-Gold sont des faux outils anti-virus/spyware générateurs de fausses alertes de sécurité de Windows.

La rubrique "privacy statement" est identique à celle qui est sous l'élément Vcodec.eMedia.

Zlob.Downloader

« **Fonctionnalité**
Gestionnaire de téléchargement de programmes malicieux.

Description
Cheval de Troie qui télécharge et installe différents spywares et malveillances sur les ordinateurs infectés : SpyAxe, SpywareStrike, SpyTrooper, Vcodec, ... »

SpyTrooper est un logiciel espion et adware émetteur de fausses alertes spyware. Il exploite des vulnérabilités pour forcer son installation ou peut être également librement installé à partir d'un site web.

4. Nettoyage Spybot Search & Destroy

Description Analyse du système par Spybot Search & Destroy

Tâches
- Redémarrage de l'ordinateur,
- démarrage de Spybot S&D,
- analyse du système,
- nettoyage des problèmes détectés.

L'expérience précédente a montré qu'il pouvait y avoir des installations ou des effets qui ont lieu seulement après un redémarrage et un certain temps d'activité. Effectuons donc un redémarrage préalable. Le système est alors laissé allumé une nuit entière. Le second scan est donc effectué après ces étapes préalables.

Résultats et observations

Après le redémarrage, l'ouverture de l'explorateur Internet Explorer a été piratée pour amener l'utilisateur sur une page l'informant que son système est piraté et qu'il doit télécharger les produits proposés pour supprimer les spywares et virus installés. De manière aléatoire, des messages d'erreur de type « erreur système » de Windows surgissent pour signaler une contamination spyware.

---

[104] PSGuard utilise une faille de programmation (rootkit) basée sur une différence d'API entre Win32 et le code natif pour se créer une entrée invisible dans la base de registre de Windows.

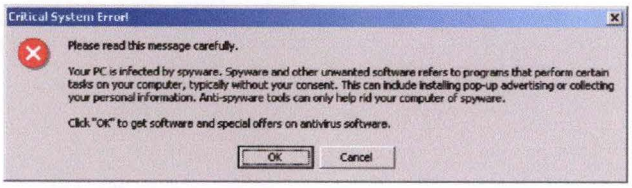


Figure 94 : Fausse erreur sytème

Lorsque l'on veut consulter les programmes installés par le panneau de configuration (« Ajout/suppression de programmes »), l'accès est rendu impossible sur la majorité des objets du panneau de configuration Windows.

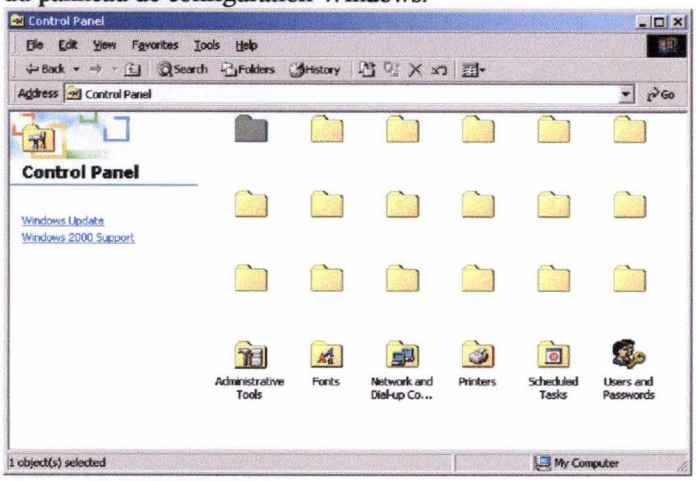


Figure 95 : Panneau de configuration inaccessible

Le résultat de l'analyse est identique à celui d'avant le redémarrage.

Le nettoyage s'effectue sur la totalité des problèmes détectés. Ceux-ci ne peuvent cependant pas être éliminés sans un redémarrage de la machine et une exécution de Spybot. Ce qui est fait immédiatement.

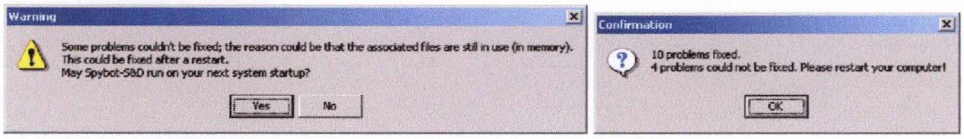


Figure 96 : Spybot, nettoyage avant redémarrage

Spybot démarre donc bel et bien au lancement de Windows et effectue une recherche. Il propose l'élimination des éléments perturbateurs. Le nettoyage se déroule correctement à première vue, du moins s'il faut en croire le résultat de Spybot.

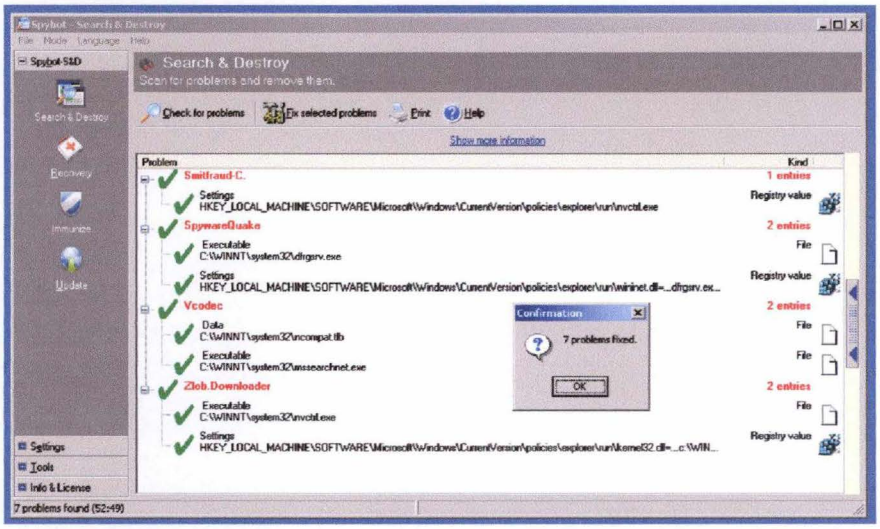


Figure 97 : Spybot, nettoyage après redémarrage

A la fin de la phase de démarrage, afin de s'assurer que le système est nettoyé, on va voir si le panneau de configuration est redevenu accessible et si le codec a été supprimé. C'est effectivement le cas, cependant on peut voir immédiatement que tout n'a pas disparu.

Internet explorer est démarré afin de vérifier qu'il est débarrassé du pirate de navigateur. Celui-ci est toujours là. Les bannières publicitaires et messages d'alertes ne tardent pas à arriver.

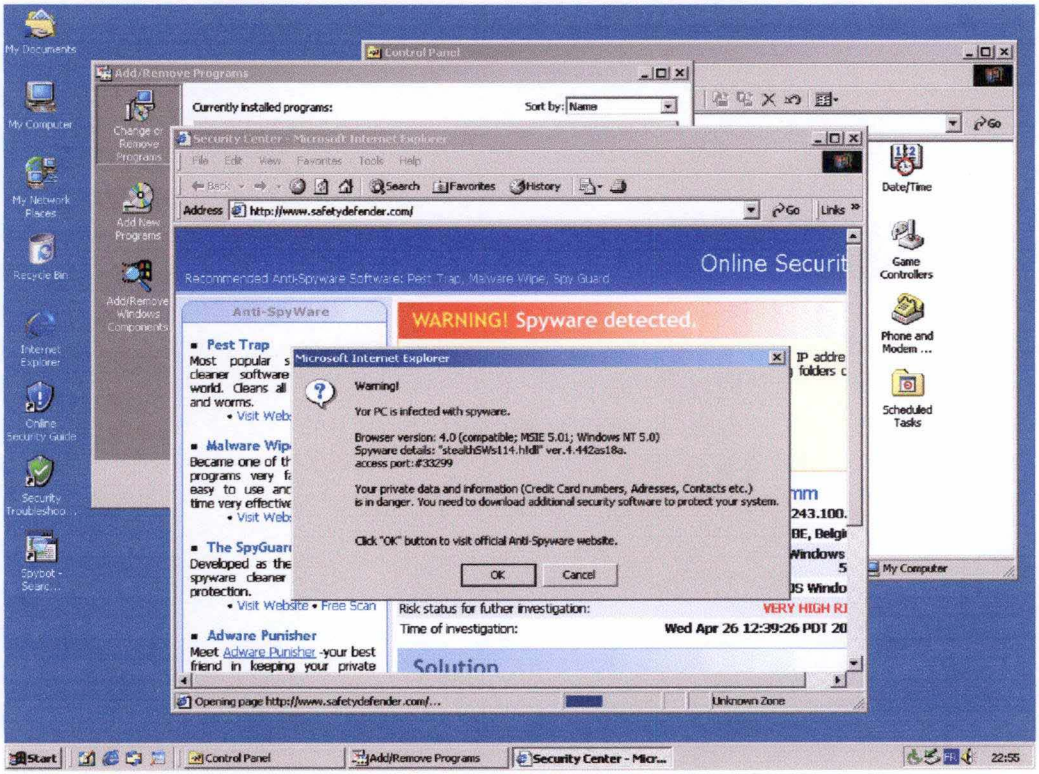


Figure 98 : eMedia Codec, Internet Explorer après nettoyage Spybot

Spybot S&D est démarré, il fait une analyse du système. On peut constater que le module de téléchargement Vcodec est toujours installé.

Figure 99 : vCodec après nettoyage par Spybot S&D

Vcodec installe des fichiers dans C:\Windows\System32 et quelques autres répertoires temporaires dont le nom est aléatoire et change à chaque exécution. Il est impossible de les supprimer manuellement car ils sont verrouillés par un processus système. Quand bien même il serait possible d'en supprimer quelques uns, ils se réinstallent automatiquement avec un nom différent.

3.5.6 Résumé de l'expérience

Compte tenu de la longueur de la démonstration, résumons les étapes de l'expérimentation.

1. **SpywareQuake**
    - Réinitialisation du système.
    - Installation du codec vidéo eMedia.
    - Installation et scan SpywareQuake.
2. **Spybot Search & Destroy**
    - Réinitialisation du système.
    - Installation eMediaCodec.
    - Installation et scan de Spybot Search &Destroy.
    - Nettoyage du système par Spybot Search & Destroy.

3.5.7 Conclusion

L'expérience n'a pas suivi le tracé prévu au départ. Chaque étape a eu son lot de surprises qui ont conduit au changement de choix d'expérimentation. L'idée de départ était de comparer la capacité de différents outils anti-spywares face à un produit contenant du code malicieux choisi arbitrairement : eMedia codec. Le choix d'eMedia codec est venu par hasard lors de son installation sur une autre machine[105]. Le logiciel anti-virus (Kaspersky Anti-Virus en l'occurrence) avait immédiatement réagit en stoppant l'action du code malicieux et en avertissant de la présence d'un cheval de Troie et d'un espion. C'est alors qu'eMedia Codec est devenu le sujet de cette démonstration. La combinaison de Kazaa et eMedia codec à conduit à une installation inopinée de SpywareQuake qui s'est avéré être un bon sujet d'étude, étant lui-même un outil anti-spywares malicieux.

Les logiciels anti-spywares (Spybot S&D et Spyware Quake) ont mis en évidence la présence de code malicieux dans ce décodeur vidéo.

Ce codec a lui-même engendré l'installation d'un anti-spywares suspect : Spyware Quake. Il n'y a pas eu d'installations en chaîne de spywares, mais un manque de vigilance d'un utilisateur aurait pu avoir le même effet. Il aurait suffit d'un clic de souris sur les différents pop-ups proposés pour démarrer l'installation de produits malicieux.

L'analyse Spybot S&D a révélé que les composants d'eMedia Codec réunissent les caractéristiques d'un cheval de Troie, d'un spyware et d'un adware. Spybot S&D est incapable de se débarrasser du cheval de Troie, tout comme il est impossible de le faire de manière manuelle. Après la suppression de tous les fichiers liés à ce produit, il se réinstalle automatiquement de lui-même à chaque réinitialisation du système, ou même avant, tant qu'un processus spécifique (impossible à tuer par l'utilisateur en session) est logé en mémoire. La seule manière pour s'en défaire a été de télécharger un script qui exécute une tâche de nettoyage de ce code malicieux durant la phase de démarrage des processus systèmes, avant même de donner la main à l'utilisateur.

[105] PC hors laboratoire équipé des logiciels suivants : Spybot Search and Destroy (et son module résident), Kaspersky Anti-Virus et le pare-feu Windows XP.

3.6 Démonstration 3 : Les anti-spywares

3.6.1 Introduction

Notre utilisateur a pu constater que les résultats affichés lors de son expérience spyware pouvaient varier de manière importante selon la solution anti-spyware adoptée. Il a également entendu parler de l'existence de vrais et de faux anti-spywares. Il se pose donc des questions quant à la qualité des différentes solutions sélectionnées. Il décide de les mettre en concurrence en espérant que les meilleurs logiciels anti-espions supplanteront et révèleront les faux anti-spywares ou les moins bons d'entre eux.

3.6.2 Méthode

Dans les scenarios invoqués, on imagine trois anti-spywares qu'il aurait trouvé en faisant une recherche sur mots clés dans un moteur de recherche. Il n'a pas envie de débourser de l'argent pour une solution anti-spyware. Il décide donc d'installer les outils proposés gratuitement sur l'Internet.

3.6.3 Diagramme de séquence

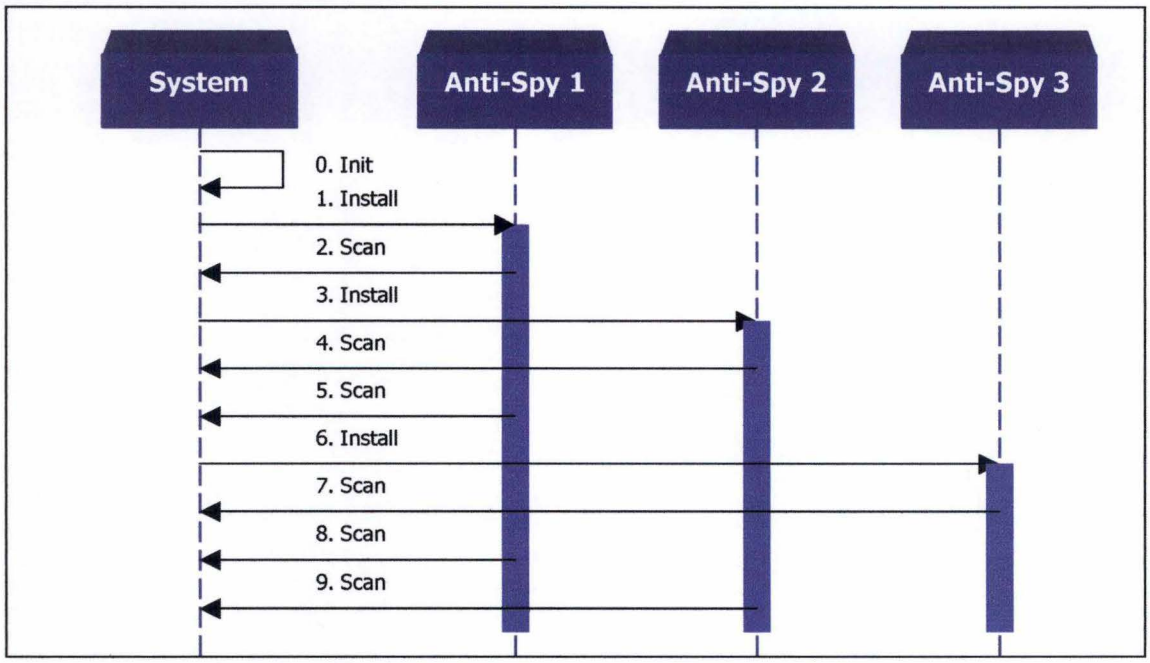


Figure 100 : Diagramme de séquence, test anti-spywares

3.6.4 Scénarios

Chaque scénario suit le diagramme de séquence, la seule variable est liée aux acteurs figurant dans le schéma.

Pour cette expérience, trois outils anti-spyware ont été sélectionnés. Il s'agit d'un « vrai » anti-spyware réputé fiable par les spécialistes dans le domaine : SpyBot Search and Destroy. Les deux autres sont répertoriés malicieux, trompeurs ou douteux [SPW06] : SpywareStrike et AdwareSpy.

SpywareQuake , le logiciel anti-spywares testé lors de l'expérience précédente, est un produit dérivé de SpywareStrike. Le moteur de recherche est identique, seule l'interface a changé ainsi que la base de signatures. SpywareStrike est un produit identique (mis à part l'habillage), directement dérivé ou successeur des produits suivants : AdwareDelete, AntiVirus Gold, SpyAxe, SpyFalcon, et Spyware Sheriff[SPW06].

Les scénarios de tests suivent la combinatoire représentée dans le tableau suivant :

Scénario	Anti-Spy 1	Anti-Spy 2	Anti-Spy 3
1	Spybot S&D	SpywareStrike	AdwareSpy
2	SpywareStrike	AdwareSpy	Spybot S&D
3	SpywareStrike	Spybot S&D	AdwareSpy
4	Spybot S&D	AdwareSpy	SpywareStrike
5	AdwareSpy	SpywareStrike	Spybot S&D
6	AdwareSpy	Spybot S&D	SpywareStrike

Figure 101 : table des scenarios de tests anti-spywares

Pour l'illustration, deux scenarios sont présentés afin de démontrer la différence de résultats en installant l'un ou l'autre logiciel anti-spywares dans des ordres différents. Cette séquence est déterminante pour un utilisateur néophyte qui se fie aux résultats des logiciels anti-espions pour sélectionner celui qui gagnera sa confiance.

Pour l'exercice, seuls les deux premiers scenarios du tableau seront présentés (libre au lecteur de tester davantage de combinaisons). L'importance ici est la démarche de la démonstration.

Notons que dans ce laboratoire, on ne fait que de l'analyse anti-spywares afin de mettre les différents outils en concurrence. Il ne s'agit pas de mesurer la qualité de résolution des problèmes.

Un « faux » anti-spyware ne signifie pas forcément qu'il n'effectue pas de recherche de logiciels espions mais qu'il peut faire autre chose en sus. Cette autre chose étant :

- de l'espionnage étant lui-même un spyware,
- de la fausse alerte spyware afin d'inciter à l'achat dudit produit anti-spyware,
- toute autre activité suspecte, généralement non documentée.

0. Init

L'étape appelée Init correspond à la mise en place du système de base à partir de l'image du disque préalablement copiée sur CD-Rom dans la phase de pré-installation.

- Démarrage à partir d'un CD d'installation de Linux (Mandriva 2005),
- redémarrage à partir du CD de démarrage de TrueImage,
- chargement de l'image de Windows 2000,
- redémarrage du système en Windows.

Toutes les étapes de l'initialisation du laboratoire sont illustrées en annexe sous la rubrique « Initialisation ». Cette phase est identique pour chaque scénario.

3.6.5 Scenario 1 : Spybot Search & Destroy – SpywareStrike - AdwareSpy

1. Install Anti-Spy 1

Description Téléchargement et installation de Spybot Search & Destroy.

Tâches Démarrage du navigateur,
navigation sur la page de téléchargement de l'anti-spyware (http://www.safer-networking.org),
lancement de l'installation du produit.

Les étapes de téléchargement et d'installation de Spybot S&D sont illustrées en annexe sous la rubrique « Installation de Spybot S&D ».

2. Scan Anti-Spy 1

Description Analyse du système par Spybot Search & Destroy.

Tâches
- Démarrage de Spybot S&D,
- configuration de l'outil pour une analyse approfondie[106],
- vaccination du système[107],
- analyse du système.

Résultats et observations

Figure 102 : Alexa, analyse par Spybot

Au premier scan, l'analyse du disque révèle un élément qualifié de spyware, le lien d'Alexa. Les autres éléments ne sont que des traces d'activités laissées par l'utilisateur sur le système, ainsi que des identificateurs de produits installés sur le système tels que Windows Media Player, la liste des derniers fichiers ouverts par MS Paint, les journaux d'activités de différentes applications, etc.

```
12.03.2006 13:30:50 - ##### check started #####
12.03.2006 13:30:50 - ### Version: 1.4
12.03.2006 13:30:50 - ### Date: 12/03/2006 13:30:50
12.03.2006 13:31:16 - ##### checking bots #####
12.03.2006 13:54:27 - found: Alexa Related  Link
12.03.2006 14:02:08 - ##### checking usage tracking #####
12.03.2006 14:02:08 - found: Common Dialogs History 20 files
12.03.2006 14:02:09 - found: Log  Activity: COM+.log COM+.log
12.03.2006 14:02:09 - found: Log  Activity: SchedLgU.Txt SchedLgU.Txt
12.03.2006 14:02:09 - found: Log  Activity: imsins.log imsins.log
12.03.2006 14:02:09 - found: Log  Activity: mmdet.log mmdet.log
12.03.2006 14:02:09 - found: Log  Activity: ModemDet.txt ModemDet.txt
12.03.2006 14:02:09 - found: Log  Activity: OEWABLog.txt OEWABLog.txt
12.03.2006 14:02:09 - found: Log  Install: comsetup.log comsetup.log
12.03.2006 14:02:09 - found: Log  Install: iis5.log iis5.log
12.03.2006 14:02:10 - found: Log  Install: ocgen.log ocgen.log
12.03.2006 14:02:10 - found: Log  Install: ockodak.log ockodak.log
12.03.2006 14:02:10 - found: Log  Install: setupact.log setupact.log
12.03.2006 14:02:10 - found: Log  Install: setupapi.log setupapi.log
12.03.2006 14:02:10 - found: Log  Install: setuplog.txt setuplog.txt
12.03.2006 14:02:10 - found: Log  Shutdown: System32\wbem\logs\mofcomp.log System32\wbem\logs\mofcomp.log
12.03.2006 14:02:10 - found: Log  Shutdown: System32\wbem\logs\wbemcore.log System32\wbem\logs\wbemcore.log
12.03.2006 14:02:10 - found: Log  Shutdown: System32\wbem\logs\wbemsnmp.log System32\wbem\logs\wbemsnmp.log
12.03.2006 14:02:11 - found: Log  Shutdown: System32\wbem\logs\winmgmt.log System32\wbem\logs\winmgmt.log
12.03.2006 14:02:11 - found: Log  Shutdown: System32\wbem\logs\wmiprov.log System32\wbem\logs\wmiprov.log
12.03.2006 14:02:21 - found: Internet Explorer Typed URL list 2 files
12.03.2006 14:02:21 - found: Internet Explorer User agent
12.03.2006 14:02:22 - found: Internet Explorer User agent
12.03.2006 14:02:24 - found: MS Management Console Recent command list 1 files
12.03.2006 14:02:25 - found: MS Media Player Client ID
12.03.2006 14:02:25 - found: MS Media Player Client ID
12.03.2006 14:02:33 - found: MS Fax Last country ID
12.03.2006 14:02:33 - found: MS Fax Last country ID
12.03.2006 14:02:34 - found: MS Paint Recent file list 4 files
12.03.2006 14:02:41 - found: Windows Drivers installation paths
12.03.2006 14:02:44 - found: Windows.OpenWith Open with list - .BMP extension 2 files
12.03.2006 14:02:47 - found: Windows Explorer Stream history 4 files
12.03.2006 14:02:47 - found: Windows Explorer User Assistant history IE 8 files
12.03.2006 14:02:47 - found: Windows Explorer User Assistant history files 48 files
12.03.2006 14:02:48 - found: Windows Explorer Last visited history 2 files
12.03.2006 14:02:48 - found: Windows Explorer Recent file global history
12.03.2006 14:02:50 - found: Cookie Cookie (4)
12.03.2006 14:02:50 - found: Cache Cache (93)
12.03.2006 14:02:50 - ##### check finished #####
```

Figure 103 : Résultat du premier scan appronfondi par Spybot S&D

[106] Les impressions d'écran de la configuration de Spybot S&D sont disponibles en annexe.

[107] La vaccination correspond à l'inscription d'une liste de clés de blocages dans la base de registre (sites Internet et CLSID).

3. Install Anti-Spy 2

Description Téléchargement et installation de SpywareStrike.

Tâches Connexion Internet Explorer sur la page de SpywareStrike (http://www.spywarestrike.com).

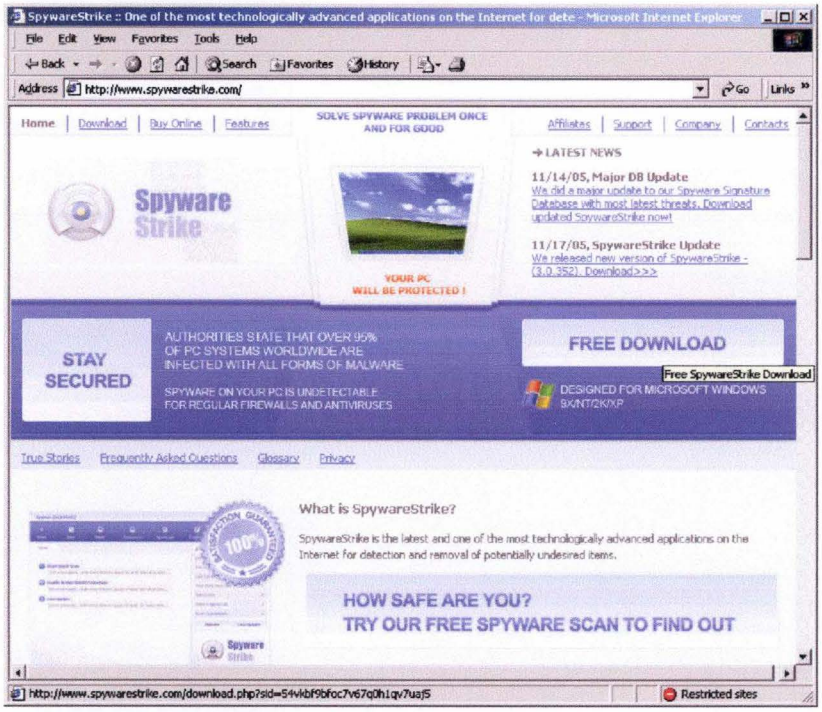


Figure 104 : Page d'accueil de SpywareStrike

Observations - Lorsqu'on clique sur le lien de téléchargement, l'accès est refusé,

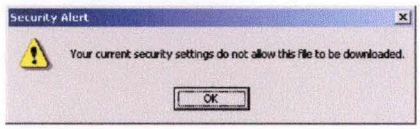


Figure 105 : SpywareStrike, blocage Spybot

- La navigation sur la page de SpywareStrike est une zone à accès restreint. En supposant que cette interdiction est légitime, l'utilisateur néophyte est donc protégé à ce stade car il n'arrive pas à télécharger le fichier.
Cette restriction est imposée par Spybot S&D dans la phase intitulée « vaccination ».
Les utilisateurs expérimentés peuvent contourner cette règle en changeant un paramètre du navigateur. Il suffit d'enlever les URL relatives à SpywareStrike de la liste des sites à accès restreint.

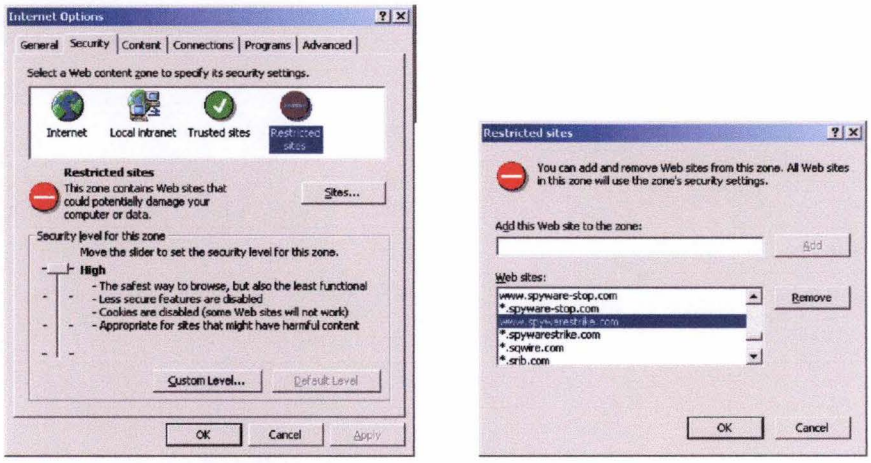


Figure 106 : Paramètres Internet Explorer, les zones à accès restreint

Après avoir accepté ces paramètres, le site de SpywareStrike est considéré comme zone Internet au même titre que les autres sites par défaut.

Figure 107 : Internet Explorer, les zones

- Une fois le fichier téléchargé, l'installation de SpywareStrike se déroule sans problème. Les impressions d'écran du processus d'installation se trouvent dans les annexes sous la rubrique « Installation de SpywareStrike ». Notons cependant qu'un changement dans la base de registre est signalé par SpyBot S&D. Celui-ci demande une confirmation pour accepter cette modification.

A ce stade, l'utilisateur a l'option de faire confiance à SpywareStrike et de mettre en œuvre les moyens d'autoriser son installation, ou faire confiance à Spybot et ne pas installer le produit. Pour l'expérimentation, jouons l'utilisateur obstiné qui fait le nécessaire pour autoriser son installation et son exécution.

4. Scan Anti-Spy 2

Description Analyse du système par SpywareStrike.

Tâches - Démarrage de SpywareStrike,
- lancement d'une analyse approfondie.

Figure 108 : Analyse SpywareStrike

Résultats l'outil ne décèle absolument aucun élément suspect et revient très rapidement sur l'écran principal.

5. Scan Anti-Spy 1

Description Analyse du système par Spybot Search & Destroy.

Résultats Spybot détecte 12 éléments suspects liés à SpywareStrike.

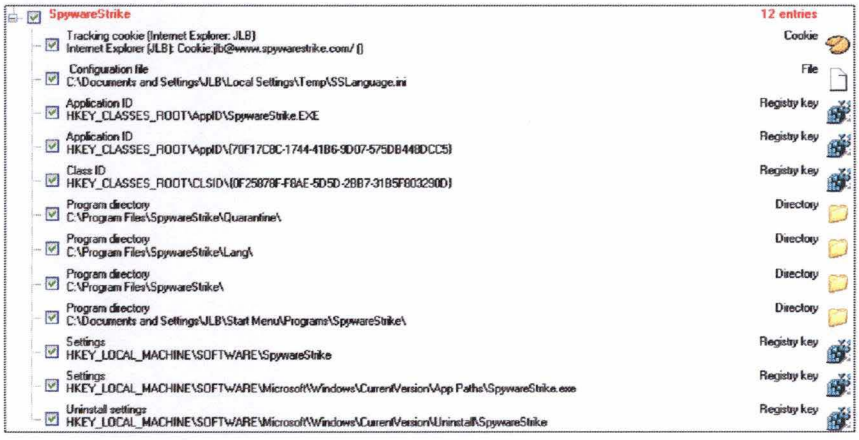


Figure 109 : SpywareStrike, analyse Spybot

6. Install Anti-Spy 3

Description Téléchargement et installation d'AdwareSpy.

Tâches - Démarrage InternetExplorer,
- connexion à l'adresse http://www.adwarespy.com,

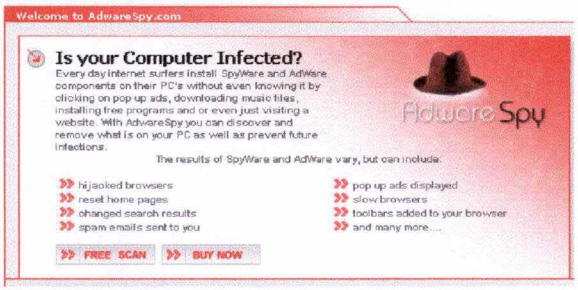


Figure 110 : Page d'accueil AdwareSpy

- installation de l'outil en cliquant sur le bouton « Free Scan ». Les écrans successifs de téléchargement et d'installation sont en annexe dans la rubrique « Installation d'AdwareSpy ».

Résultats et observations

L'installation d'AdwareSpy se déroule sans problème.

7. Scan Anti-Spy 3

Description Analyse du système par AdwareSpy

Résultats et observations

L'analyse du système est lancée avec AdwareSpy.

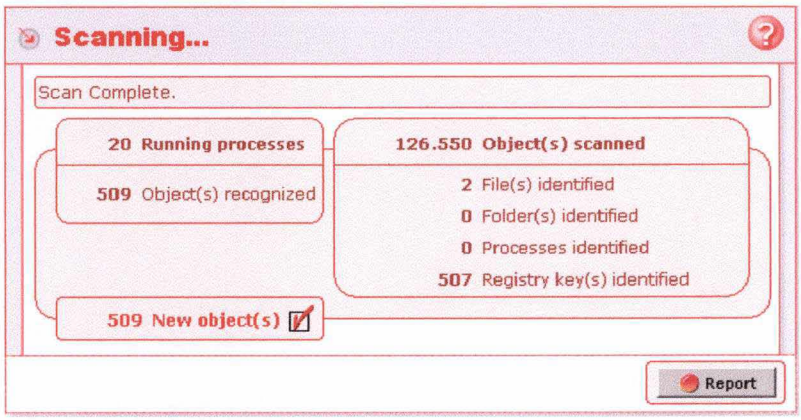


Figure 111 : AdwareSpy, analyse du système

Après une heure d'analyse, le résultat est impressionnant en terme de nombre d'éléments suspects trouvés :
- 2 fichiers,
- 507 entrées dans la base de registre.

Les 2 fichiers correspondent à :
- un cookie de la page de démarrage d'Internet Explorer identifié en tant que « Tracking cookie »,
- le fichier C:\Program Files\Spybot – Search & Destroy\SDHelper.dll, le module résident pour Internet Explorer de Spybot (identifié en tant que « Spybot-S&D IE Browser plugin).

Les entrées de la base de registre :

- AdwareSpy reconnait également une série de clés de registre liées à Spybot (CLSID et BHO), sans donner plus de précisions,

- Il trouve également trois éléments de la base de registre identifiés comme dialers « TinTel dialer » et « Instant Access (Adware) / Instant Access is a Premium Rate Dialer »,

- 4 entrées localisées dans les clés « HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\ », identifiés en tant que « I-LookUp », « SearchCentrix » et « TrafficHog »,

- Tous les autres éléments (près de 500) concernent des entrées dans la base de registre liées à la clé HKLM\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility. Toutes ces clés correspondent à la liste de blocages imposée par Spybot S&D.

8. Scan Anti-Spy 1

Description Analyse du système par Spybot Search & Destroy

Tâches - Fermeture de AdwareSpy ainsi que de SpywareStrike,
- analyse par Spybot

Résultats et observations
Spybot ne décèle aucun nouvel élément par rapport à l'analyse précédente.

9. Scan Anti-Spy 2

Description Analyse du système par SpywareStrike

Tâches - Fermeture de Spybot S&D, ainsi que du résident IE de Spybot,
- démarrage de SpywareStrike,
- analyse par SpywareStrike.

Résultats et observations
Le scan comme à chaque fois avec cet outil ne dure pas plus de trente secondes et ne décèle absolument rien de suspect sur le système.

Conclusion du premier scenario

Du point de vue de l'utilisateur, la confusion est totale. Spybot S&D accuse SpywareStrike, AdwareSpy accuse Spybot et SpywareStrike ne trouve jamais rien. En procédant par élimination logique, on peut imaginer que les « mauvais » anti-spywares sont d'abord SpywareStrike, et ensuite Spybot S&D. Il reste alors en course AdwareSpy car il n'a jamais été incriminé.

Le système est réinitialisé.

3.6.6 Scenario 2 : SpywareStrike – AdwareSpy – Spybot Search & Destroy

1. Install Anti-Spy 1

Description Téléchargement et installation de SpywareStrike.

Tâches - Connexion IE sur la page de SpywareStrike (http://www.spywarestrike.com),
- téléchargement et exécution de l'installation de l'outil.

Résultats et observations

L'installation se déroule sans problème.

Notons l'avertissement sur une signature manquante.

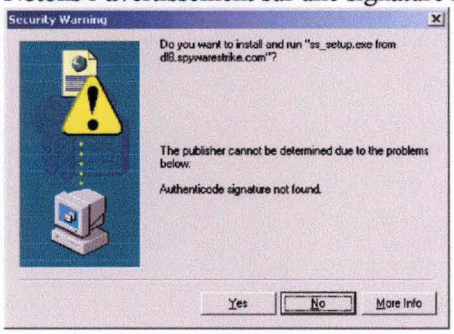


Figure 112 : SpywareStrike, avertissement de signature manquante

2. Scan Anti-Spy 1

Description Analyse du système par SpywareStrike.

Résultats SpywareStrike exécute son « Full System Scan » en quelques secondes et n'affiche absolument aucun résultat. Le retour sur l'écran d'accueil se fait immédiatement.

3. Install Anti-Spy 2

Description Téléchargement et installation de AdwareSpy.

Tâches - Connexion IE sur la page de AdwareSpy (http://www.adwarespy.com),
- téléchargement et exécution de l'installation de l'outil.

Résultats et observations

L'installation se déroule correctement.

L'écran d'avertissement relatif à la signature authenticode apparait lors du téléchargement :

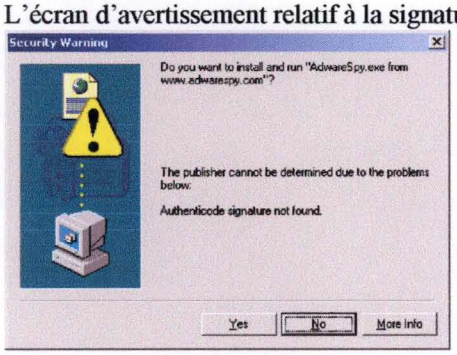


Figure 113 : SpywareStrike, avertissement authenticode

4. Scan Anti-Spy 2

Description Analyse du système par AdwareSpy.

Tâches - Démarrage d'AdwareSpy,
- paramétrage de l'outil,
- analyse complète du système.

Le paramétrage se fait conformément à la figure suivante :

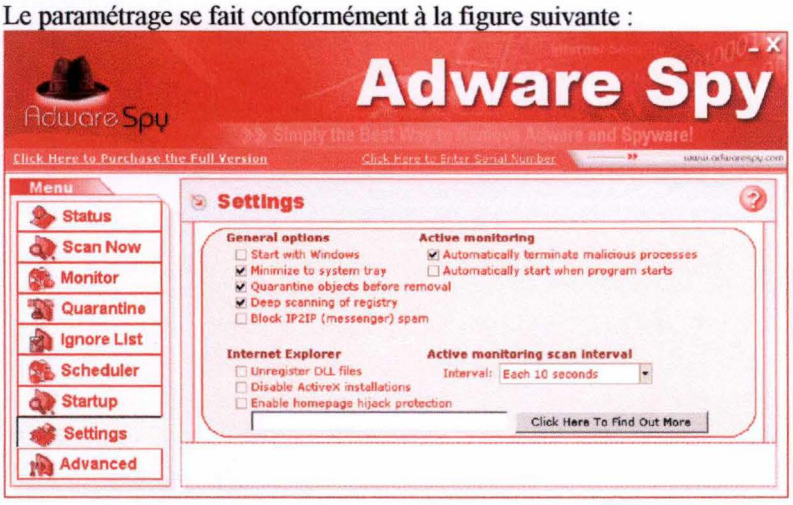


Figure 114 : AdwareSpy, paramétrage de l'outil

Analyse complète du système :

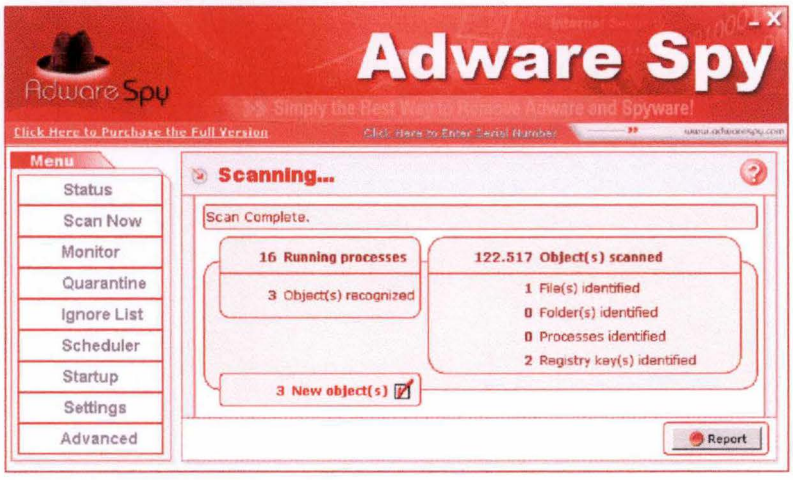


Figure 115 : AdwareSpy, analyse en cours

AdwareSpy trouve un cookie est deux dialers.

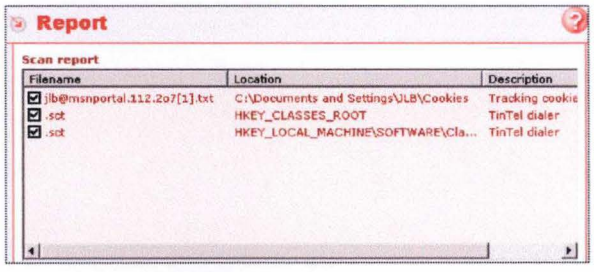


Figure 116 : AdwareSpy, rapport d'analyse

L'analyse du système prend beaucoup plus de temps que celle réalisée par SpywareStrike. Ce qui laisse supposer que l'examen se fait de manière plus approfondie et plus « sérieuse ».
Les éléments trouvés correspondent à un cookie de la page d'Internet Explorer par défaut sur le site Microsoft (portail MSN), les deux éléments « .sct » correspondent à l'association faite dans la base de registre aux fichiers .sct (de type « scriptlet »).

5. Scan Anti-Spy 1

Description Analyse du système par SpywareStrike.

Résultats et observations

Le résultat est toujours identique, rien de suspect n'a été décelé.

6. Install Anti-Spy 3

Description Téléchargement et installation de Spybot S&D.

Tâches - Ouverture d'une session Internet Explorer à l'adresse http://www.safer-networking.org,
- téléchargement et installation de Spybot S&D.

Résultats et observations

La page de démarrage par défaut d'Internet Explorer a changé. Au lieu de se connecter sur le portail Microsoft MSN, l'adresse de démarrage est http:/// ce qui débouche sur une page d'erreur.
Durant les étapes de téléchargement et d'installation, les instances des anti-spywares précédents ne sont pas fermées. Lors de l'installation de Spybot, les produits AdwareSpy et SpywareStrike sont toujours actifs en mémoire.

L'installation se déroule sans aucun problème.

7. Scan Anti-Spy 3

Description Analyse du système par Spybot S&D

Résultats et observations

Spybot détecte 2 malveillances :
- Alexa tout comme dans le premier scenario,
- SpywareStrike (13 entrées)

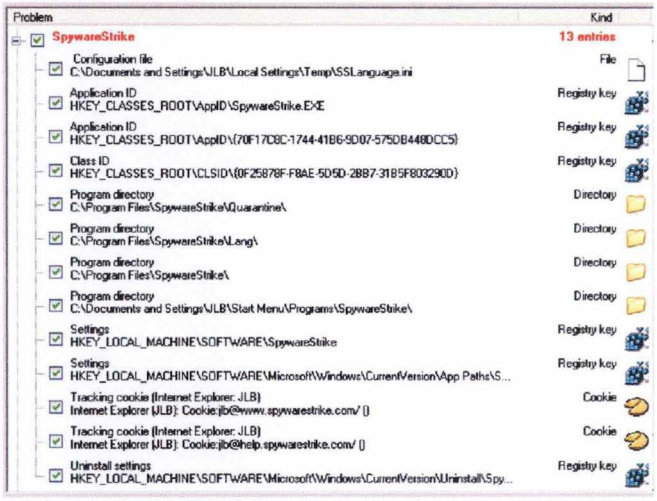


Figure 117 : SpywareStrike analysé par Spybot

Spybot affiche les informations suivantes : « SpywareStrike est un logiciel malveillant supposé être un anti-spyware. Il s'intalle avec SmitFraud-C, trouve des problèmes inexistants pour forcer l'utilisateur à payer pour une désinfection ».

8. Scan Anti-Spy 1

Description Analyse du système par SpywareStrike

Résultats et observations

Le résultat est toujours identique, rien de suspect n'a été décelé.

9. Scan Anti-Spy 2

Description Analyse du système par AdwareSpy

Résultats et observations

Tout comme dans le scenario précédent, le scan a décelé 509 éléments.

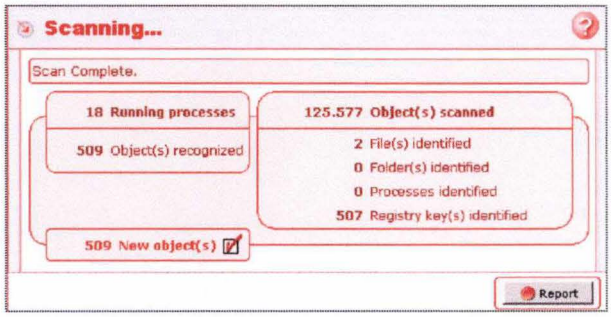


Figure 118 : AdwareSpy, analyse du système

L'explication de ces éléments est identique que pour le premier scenario.

Conclusion du second scenario

SpywareStrike ne décèle jamais d'élément suspect.

Avant l'installation de Spybot S&D, AdwareSpy fait trois détections dont deux sont erronées. Après l'installation de Spybot S&D, il interprête mal les entrées de la base de registre et incrimine Spybot S&D.

Spybot S&D quant à lui détecte deux malveillances justifiées, dont SpywareStrike.

En procédant par élimination logique, on peut imaginer que les « mauvais » anti-spywares sont :

- SpywareStrike à en juger son incapacité de détection,
- AdwareSpy ou Spybot S&D selon qu'on accorde du crédit à la quantité de détections ou pas.

3.6.7 Conclusion

La quantité de spywares frauduleux, inadaptés ou inutiles est impressionnante. Plusieurs d'entre eux, identiques, sont disponibles sous différents noms. De nombreux anti-spywares sont dotés d'un moteur de recherche médiocre, qui interprète les éléments (fichiers, clés de la base de registre et processus) de manière erronée, C'est ainsi qu'ils peuvent détecter des quantités invraisemblables d'éléments suspects. Ce qui ôte toute crédibilité à l'outil.
Il en existe également qui génèrent volontairement de fausses alertes et détections (désignés en anglais par les termes « false positive ») dans un but d'incitation à la vente. Dans ce cas, les résultats, parfois plausibles, sont à examiner avec circonspection.

L'utilisateur « naïf » voulant mettre en évidence les bons logiciels anti-espions des mauvais, constate que selon la manière dont il orchestre la séquence des installations des anti-spywares, les résultats sont différents. Dans le premier cas, en considérant l'utilisateur non expertisé dans la configuration de Windows, il arrivera aux constatations suivantes :

- Spybot S&D s'installe correctement et semble bien faire son travail,
- Spybot S&D empêche l'installation de SpywareStrike,
- AdwareSpy s'installe et incrimine Spybot S&D.

Il reste par conséquent en course AdwareSpy qui semble être le plus sûr.

Dans le second scenario, les constatations sont les suivantes :

- Les trois logiciels sont installés correctement,
- SpywareStrike semble ne pas faire grand-chose, tandis que Spybot S&D et AdwareSpy font un scan approfondi,
- Spybot S&D incrimine SpywareStrike et AdwareSpy incrimine Spybot S&D.

Dans les deux cas, AdwareSpy apparait comme le plus accusateur et pourrait remporter la confiance de l'utilisateur néophyte.

Du point de vue expert, il ressort de ces scenarios que la quantité ne prime pas sur la qualité. La qualité de l'outil peut être jugée sur la pertinence des détections. L'exhaustivité des détections est le critère le plus difficile à déterminer. Seule la comparaison des résultats d'outils avérés est en mesure de mettre en évidence les lacunes de ceux-ci. Même l'association des meilleurs logiciels anti-espions ne garantit pas une détection totale des espions existants. Afin de s'assurer de la fiabilité d'un outil anti-spywares, il existe des sites et des forums spécialisés dans le domaine de la sécurité (Computer Associates, McAfee, SpywareWarrior, Kaspersky, etc.). On y trouve généralement des listes de produits fiables. On ne peut donc que conseiller aux utilisateurs de prendre leurs renseignements sur un outil anti-spywares avant de l'installer.

3.7 Critique de la démarche

La démarche adoptée consiste en une succession de démonstrations destinées à montrer :

- l'existence de logiciels espions,
- la forme et le mode de propagation des logiciels espions,
- la fiabilité des logiciels anti-spywares disponibles gratuitement sur Internet.

Les produits de test choisis sont des logiciels gratuits, disponibles au grand public, afin d'être le plus proche de la réalité car tout internaute est susceptible de rencontrer une situation similaire. C'est donc volontairement qu'aucun outil spécifique n'a été développé. Le système de base n'a pas fait non plus l'objet d'une configuration particulière. De ce fait, il est loisible au lecteur de reproduire ces expériences dans des conditions identiques.

Le choix des logiciels pourrait cependant être critiqué. En effet, seul Spybot Search & Detroy a été présenté comme logiciel anti-spyware fiable, or il en existe d'autres qui n'ont pas été mis en présence. On peut justifier ce choix par l'objectif de l'étude. Celui-ci n'est pas de comparer la qualité des logiciels anti-espions réputés, car cela est fait régulièrement par divers magazines. Cette expérience aurait été sans réel intérêt.

Les résultats des expériences ont été partiellement inattendus.

Le premier scenario visait à mettre en évidence la présence de l'espion Gator dans deux produits choisis arbitrairement : Kazaa et Claria ScreenScenes. Kazaa, contrairement à ce qui était prévu ne contenait plus Gator dans la version testée, mais il était cependant bien dans l'économiseur d'écran ScreenScene.

La deuxième expérience centrée sur un décodeur vidéo malicieux (eMedia Codec) visait à le confronter à des outils anti-spywares différents et d'en comparer les résultats. Le Codec était muni d'un installateur de programmes malicieux, ce que l'expérience a mis en évidence mais il n'a cependant pas été possible de montrer une prolifération de code malveillant. De plus, cette expérience a révélé l'existence d'outils anti-spywares suspects, et a ainsi déterminé la troisième partie du laboratoire.

La dernière expérience met en confrontation trois logiciels anti-espions dont un seul d'entre eux est fiable. Le résultat est une fois de plus inattendu. Un des outils s'est révélé complètement inutile, les deux autres jetant un doute sur leur crédibilité respective, le « mauvais » anti-spyware affichant une suspicion sur le « bon » outil anti-espions. La séquence des installations des outils change la manière dont l'utilisateur pourrait interpréter le résultat, semant ainsi une incertitude sur leur fiabilité.

La démarche atteint une limite dans la vérification des informations. On est tenu de faire confiance aux outils reconnus fiables mais on ne peut vérifier s'ils font effectivement et complètement leur travail de détection. De même pour les outils suspects, l'absence de développement spécifique ne permet pas de vérifier l'existence ou non d'un transfert d'informations « personnelles » à l'un ou l'autre serveur et l'usage qui en serait fait. Pour ce dernier point, il aurait été très difficile de suivre ses informations et leurs destinations, cette étude nécessitant une approche totalement différente.

Conclusion

Le projet initial était la réalisation d'un spyware didactique. Celui-ci, à l'inverse des autres, agissant de manière visible, en affichant une description explicative de chaque action d'espionnage effectuée. Le but de la réalisation était d'intégrer les fonctionnalités des spywares les plus répandus (espionnage des habitudes de navigation, recherche d'informations d'identification, traçage, etc.). Le reproche que l'on peut faire à l'égard de ce genre d'outil est son manque de crédibilité, car c'est un logiciel espion créé de toutes pièces dont il est difficile de prouver la pertinence. Tout utilisateur peut nier son reflet de la réalité vis-à-vis des logiciels espions réels. Il aurait cependant une vraie valeur pédagogique.

La deuxième version du projet consistait en l'écriture d'un observateur du trafic réseau lié à Gator. Cet outil aurait eu la forme d'une extension d'un serveur proxy en code libre ou d'une méthode faisant appel à des outils de type « renifleurs ». La complexité de mise en œuvre dans les délais impartis, ainsi que la faisabilité ont écarté cette méthodologie. Quand bien même on pourrait lire les paquets sur le réseau, il serait quasi impossible d'en décoder le contenu, celui-ci pouvant être crypté (algorithmes de chiffrement, stéganographie ou références externes). L'avantage d'une telle solution, aurait été de permettre une étude sur un spyware concret largement répandu.

L'approche choisie en définitive a été l'expérimentation de divers scénarios de manière progressive en se basant sur des outils et des logiciels malveillants existants sur le marché. Le but étant de livrer aux utilisateurs une expérience réaliste, concrète et reproductible. Toutes les expériences sont menées sur un ordinateur sans protection spécifique et connecté sur Internet. Ce genre de configuration basique est celle que pourrait employer tout utilisateur néophyte en matière de sécurité.

Afin de montrer la présence de logiciels espions, Kazaa et Claria ScreenScene (deux produits réputés pour la distribution de spywares) sont soumis à Spybot S&D (un détecteur avéré fiable). Cette expérience montre effectivement la présence de l'espion Gator pour ScreenScene mais pas avec Kazaa où il était attendu. Les produits testés ne cachent pas l'existence des modules externes, dont Cydoor livré avec Kazaa, un autre espion, et Gator, ceux-ci figurent dans les conditions de licence des produits. La plupart des logiciels publient des conditions générales de licence plus ou moins détaillées où la rubrique consacrée à la protection de la vie privée y est plus souvent présente qu'auparavant. Sans avoir étudié l'aspect juridique complexe du problème, on a pu malheureusement constater que la subtilité de la notion de « données personnelles » profite aux éditeurs. Les logiciels espions sont généralement présentés dans les conditions de licence de manière détournée, sous la forme d'un adware par exemple, l'aspect spyware n'y est jamais explicitement exprimé. Un aspect envisagé mais non exploré est l'analyse des conditions générales de licences des logiciels frauduleux. Cela permettant une interprétation correcte du texte et un décodage des activités suspectes sous-entendues.

La deuxième expérience tente de montrer la prolifération de logiciels malveillants par l'intermédiaire d'un décodeur vidéo malicieux, doté d'un module de téléchargement et d'installation. Le codec est soumis à deux anti-spywares dont l'un d'eux s'est révélé suspect. Cela introduisant le doute sur la crédibilité des logiciels anti-espions disponibles gratuitement sur Internet. Cette expérience a également permis de montrer qu'un logiciel espion ne vient jamais seul, il n'est qu'un élément d'un paquetage. Il accompagne le logiciel justifiant son existence, et éventuellement d'autres modules tels qu'un ou plusieurs adwares (l'espion pouvant être lui-même un adware), une barre d'outils ou encore un cheval de Troie (comme un gestionnaire de téléchargement). L'expérience n'a pas permis de révéler une installation en chaîne de spywares comme on le présumait, mais un manque de vigilance d'un utilisateur aurait pu avoir le même effet. Il aurait suffit d'un clic de souris sur les différents pop-ups proposés pour démarrer l'installation de produits malicieux.

La troisième expérience met en concurrence trois outils anti-spywares entre eux. La combinaison de ces outils fait apparaître la présence d'outils douteux. Profitant de la notoriété des logiciels espions, de nombreux outils anti-spywares suspects ont trouvé leur place sur le marché. Les utilisateurs mal informés peuvent tomber facilement sur ces outils, généralement payant, qui sont inadaptés, malicieux ou complètement inutiles. L'expérience en laboratoire a montré combien ces logiciels anti-spywares peuvent semer la confusion chez les utilisateurs, ceux-ci s'incriminant mutuellement.

Il est important d'adopter une attitude défensive à l'égard de toutes les offres de logiciels « gratuits », notamment en lisant toutes les conditions générales et en étant attentif à toutes les étapes d'acceptation des clauses. Une installation proposée à un utilisateur fait généralement appel à son consentement. La propagation des logiciels espions profite donc en majeure partie de l'ignorance, de la naïveté ou du manque d'attention de ceux-ci. Une lecture attentive et avertie permet parfois de soupçonner une activité suspecte. Les éditeurs de logiciels espions sont conscients de cet état de fait, et comptent sur ce principe pour assurer la propagation et la pérennité de leurs malveillances.

La vigilance des utilisateurs est un premier pas mais cette bonne volonté nécessite d'être épaulée par des outils adéquats. Plusieurs solutions techniques on été présentées, des plus élémentaires aux plus élaborées. Tout utilisateur quelques soient ses compétences peut se prémunir, dans une certaine mesure, de la plupart des spywares en installant des outils spécifiques. Il n'existera malheureusement jamais de produit miraculeux qui protège l'utilisateur de tout risque. La protection ne peut être assurée que par une combinaison de moyens informatiques (une configuration réactive du système et des outils adaptés et mis à jours) et d'un discernement de la part de l'utilisateur.

Bibliographie

[ADW05] iOpus Software GmbH, Quick reference on Adware and Spyware Software, http://www.adware.info/ (consulté le 25 mai 2005)

[ALA04] Aladdin Knowledge Systems, Epidémie de Spyware – Comment détecter du code malveillant sous les apparences de la « légalité », http://www.aladdin.com , http://www.afina.fr/upload/Fournisseur/Aladdin/esafe_spyware_French_wp.pdf (publié en 2004), (consulté le 20 janvier 2005)

[ARI01] Ariase, Les outils pour surfer l'esprit tranquille sur Internet, http://www.ariase.com/fr/observatoire/outils/?TYPEID=5 (consulté le 18 janvier 2005)

[ARQ06] Arquin Geoffroy, Droit de la vie privée, http://www.copropriete-ejuris.be/protection-de-la-vie-privee-commission.shtml (consulté le 5 mai 2006)

[ASC01] Anti-Spyware Coalition, ASC Risk Model Description http://www.antispywarecoalition.org/documents/RiskModelDescription.htm (consulté le 14 janvier 2006)

[BEA04] Beal Vangie, The Difference Between Adware & Spyware, http://www.webopedia.com/DidYouKnow/Internet/2004/spyware.asp, (mise à jour le 11 novembre 2004) (consulté le 25 mai 2005)

[BOL01] Boline John, Malware: Do You Know What's Running On Your Computer? http://newsletters.hagerman.com/newsletters/ebul13-WP.htm (consulté le 29 mai 2005)

[BRA04] Brandt Adrew, Poor defenders, http://pcworld.com/resource/printable/article/0,aid,118362,00.asp (publié en décembre 2004) (consulté le 26 janvier 2005)

[CER01] CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), Risque de divulgation de données personnelles/confidentielles par des produits Microsoft http://www.certa.ssi.gouv.fr/site/CERTA-2001-ALE-014/index.html (mis à jour le 19 octobre 2001) (consulté le 14 janvier 2006)

[CON04] Condo Jean-Charles, Un logiciel espion qui désinstalle ses concurrents, http://www.branchez-vous.com/actu/04-12/08-353104.html (publié le 9 décembre 2004) (consulté le 25 janvier 2005)

[COR04] Corteggiano Maxime, Logiciel espion, http://www.laboratoire-microsoft.org/def/9537/ (publié le 24 novembre 2004) (consulté le 19 janvier 2005)

[COU01] Coutaz & Fanti, Cookies: projet de directive européenne restreignant leur utilisation, http://www.cyber-avocat.ch/e-business.html (consulté le 11 novembre 2005)

[DIF01] Internetdiffusion, Les moteurs de recherche, http://www.lesmoteursderecherche.com (consulté le 26 novembre 2005)

[DUB00] Dubois Denis, Le mouchard d'Amazon, http://www.anonymat.org/archives/amazon.htm, (mise à jour le 23 janvier 2000) (consulté le 3 mars 2005)

[GRE03] Gregoire Hubert, La technologie ActiveX, http://www.ac-nancy-metz.fr/services/monxp/activex.htm (mise à jour le 26 mars 2003) (consulté le 27 février 2005)

[GUI05] Guillemin Christophe, L'appât du gain est désormais au coeur de la cybercriminalité, http://www.zdnet.fr/actualites/internet/0,39020774,39198290,00.htm, (mise à jour le 14 janvier 2005) (consulté le 22 mars 2005)

[HOW04] Howes Eric L., "Junkware": A New Name for "Spyware" https://netfiles.uiuc.edu/ehowes/www/junkware.htm (mise à jour le 29 mars 2004) (consulté le 29 mai 2005)

[HUR01] Hurst Mark, Microsoft's Smart Tags Threaten the User Experience, http://www.goodexperience.com/columns/01/0621smart.html (mise à jour le 21 juin 2001) (consulté le 1er mars 2005)

[IDN03] Infos-du-Net (David), Télécommunications : Les dialers, outils de détournements http://www.infos-du-net.com/actualite/576-dialers.html (publié le 3 février 2003) (consulté le 22 juin 2005)

[IEE06] Felten Edward W. et Halderman Alex J., « Rootkits », *IEEE Security & Privacy*, The IEEE Computer Society, vol.4 n°1, page 20, Janvier-février 2006

[ILL04] Illett Dan (traduit de l'anglais par Guillemin Christophe), Kazaa représenterait la première menace en matière de "spyware", http://www.zdnet.fr/actualites/telecoms/0,39040748,39185531,00.htm (publié le 26 novembre 2004) (consulté le 12 janvier 2005)

[JUD02] Jud Emmanuel, Spywares : ces logiciels à votre écoute, http://www.secuser.com/dossiers/spywares_generalites.htm (publié le 2 décembre 2002) (consulté le 17 janvier 2005)

[LEO01] Léonard Th., « Le nouveau contexte des traitements de cyber-marketing sur Internet » in *Commerce et protection des données à caractère personnel*, C.R.I.D., Namur, 2001 disponible à l'adresse http://www.droit.fundp.ac.be/Textes/Leonard1.pdf

[LEY05] Leyden John, Zombie bots fuel spyware boom http://www.theregister.co.uk/2005/07/11/malware_report_mcafee (mis à jour le 11 juillet 2005) (consulté le 2 janvier 2005)

[MAN03] Manach Jean-Marc, Le logiciel espion Lover Spy cacherait une arnaque, http://www.transfert.net/a9409 (publié le 9 octobre 2003) (consulté le 12 janvier 2005)

[MIC03] Microsoft Corp., Microsoft Internet Explorer Privacy Statement http://www.microsoft.com/windows/longhorn/ieprivacy.mspx (mise à jour le 24 octobre 2003) (consulté le 29 mai 2005)

[MKB05] Microsoft, Article KB240797 : "How to stop an ActiveX control from running in Internet Explorer", http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q240/7/97.asp&NoWebContent=1&NoWebContent=1 (mise à jour le 4 avril 2005) (consulté le 28 juin 2005)

[PIN05] Pinard Pierre, Convergence anti-spyware, http://assiste.free.fr/index.html (mise à jour le 27 février 2005) (consulté le 28 février 2005)

[PIS05] Piscitello Dave, What's The Difference Between Spyware And Viruses?, http://www.securitypipeline.com/56900521 (mise à jour le 4 janvier 2005) (consulté le 8 mai 2005)

[REU05] Reuters, Un éditeur de logiciel espion doit changer ses pratiques, http://www.liberation.fr/page.php?Article=265863 (publié le 4 janvier 2005) (consulté le 16 janvier 2005)

[SAL04] Salsmann Flavien, Les spywares, http://www.supinfo-projects.com/fr/2004/spywares_fr/2/ (mise à jour le 14 février 2004) (consulté le 5 juin 2005)

[SAN01] Santorin Jean-Luc, Avenue A,
interview pour « Le Journal du Net », propos recueillis par Florence Santrot,
http://www.journaldunet.com/itws/it_petorin.shtml (publié le 25 janvier 2001),
(consulté le 11 avril 2006)

[SMI99] Smith Richard M., The Web Bug FAQ
http://www.eff.org/Privacy/Marketing/web_bug.html (mis à jour le 11 novembre 1999)
(consulté le 17 janvier 2006)

[SPW06] SpywareWarrior, The Spyware Warrior List of Rogue/Suspect Anti-Spyware Products & Web Sites,
http://www.spywarewarrior.com/rogue_anti-spyware.htm (mis à jour le 9 mars 2006)
(consulté le 12 mars 2006)

[SQU05] Centre de Ressources Informatiques de l'Université de Toulouse, SquidGuard,
http://cri.univ-tlse1.fr/documentations/cache/squidguard.html (mise à jour le 12 mai 2005)
(consulté le 28 juin 2005)

[VER01] Verbiest Thibault, Wéry Etienne, « La protection des données personnelles » in *Le droit de l'internet et de la société de l'information*, Ed. Larcier, Bruxelles, Belgique, pages 411-430, 2001

[VIN04] Vinatier Emmanuel, « Protéger sa vie privée » in *Hacking*, Micro Application, Paris, France, pages 137-147, 2004

[WAG01] Agility Systems Inc., Smart Tags FAQ,
http://www.ourfaqsite.com/faqs/Details/FAQ_997969056.html, (mise à jour le 16 août 2001)
(consulté le 3 mars 2005)

[WAZ05] Azimut, Logiciel espion (spyware), "BHO" et autres programmes nuisibles,
http://www.fsa.ulaval.ca/azimut/logiciels/spy/default.asp
(consulté le 12 janvier 2005)

[WBB05] BugBrother – Security Tao, Keyloggers, Troyens et Backdoors,
http://www.bugbrother.com/security.tao.ca/keylog.html
(consulté le 13 mars 2005)

[WCE02] Commission de la protection de la vie privée, La collecte de données à caractère personnel sur Internet,
http://www.privacy.fgov.be/publications.htm, (mise à jour le 29 août 2002)
(consulté le 16 avril 2005)

[WCF01] CheckFlow, Liste des spywares,
http://www.flowprotector.com/fr/spywarelist/echelle_risque.asp
(consulté le 30 janvier 2005)

[WEB01] auteur inconnu, Les logiciels espions, un fléau qui affecte aussi le monde des affaires,
http://benefice-net.branchez-vous.com/nouvelles/04-10/08-314901.html (publié le 18 octobre 2004)
(consulté le 12 janvier 2005)

[WEB03] auteur inconnu, Espionnage sur Internet,
http://eservice.free.fr/espionnage-internet.html (mise à jour le 15 septembre 2004)
(consulté le 13 janvier 2005)

[WEB04] auteur inconnu, Etes-vous le maillon faible de votre sécurité ?,
http://eservice.free.fr/failles-securite-humaines.html (mise à jour le 19 septembre 2004)
(consulté le 13 janvier 2005)

[WEB05] auteur inconnu, Les risques des cookies,
http://eservice.free.fr/cookies.html (mise à jour le 27 septembre 2003)
(consulté le 13 janvier 2005)

[WHV01] TechConnect Security – par H. Vincent, 64% des ordinateurs auraient des spywares,
http://www.pcinpact.com/actu/news/64_des_ordinateurs_auraient_des_spywares.htm (publié le 24 novembre 2004)
(consulté le 12 janvier 2005)

[WHV02] Branchez-vous – par H. Vincent, TOP 10 des spywares les plus intrusifs,
http://www.pcinpact.com/actu/news/TOP_10_des_spywares_les_plus_intrusifs.htm (publié le 13 décembre 2004)
(consulté le 12 janvier 2005)

[WHV03] Ars Technica – par H. Vincent, La police australienne va utiliser des spywares, http://www.pcinpact.com/actu/news/La_police_australienne_va_utiliser_des_spywares.htm (publié le 14 décembre 2004) (consulté le 12 janvier 2005)

[WWP01] Webopedia, GUID, http://www.webopedia.com/TERM/G/GUID.html, (mise à jour le 20 juin 2002) (consulté le 13 mars 2005)

[ZAT01] Zataz News (D.B.), Le spyware : simple gène ou réelle menace http://www.zataz.com/reportages-securite/7004/spyware--adware--espiongiciel.html (mis à jour le 21 avril 2004) (consulté le 15 janvier 2006)

1. Table des annexes

2. Table de correspondance des termes français-anglais

Bannière	Banner
Cheval de Troie / Troyen	Trojan
Chien de garde	Watchdog
Enregistreur de frappe au clavier	Keylogger
FAI	ISP
Fenêtre surgissante	Pop-up
Graticiel	Freeware
Logiciel espion / Espiogiciel	Spyware
Numéroteur	Dialer
Pare-feu	Firewall
Partagiciel	Shareware
Pirate de navigateur	Hijacker
Porte dérobée	Backdoor
Poste à poste	Peer-to-peer
Pourriel	Spam
Programme nuisible	Malware
Publiciel	Adware
Référent	Referrer
Reniffleur	Sniffer
Traçage	Tracking
Vers	Worm

3. Laboratoire

3.1 Initialisation

Les impressions d'écran de l'initialisation représentent 90 photos qui, pour des raisons évidentes, ne sont pas imprimés dans ces annexes. Les images sont disponibles sur le CD-Rom accompagnant.

3.2 Installation de Spybot Search & Destroy

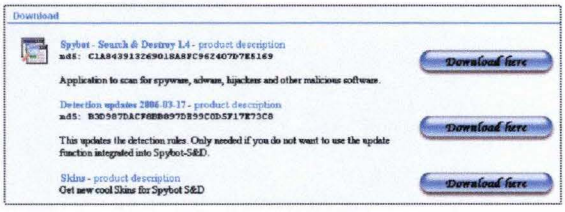


Figure 1 : Téléchargement de Spybot S&D

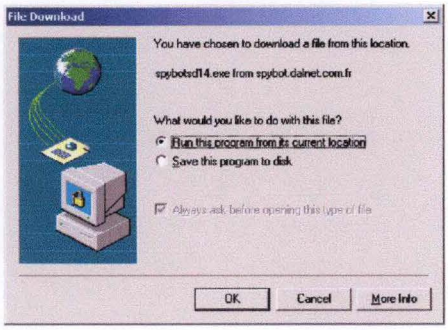


Figure 2 : Installation de Spybot S&D (1)

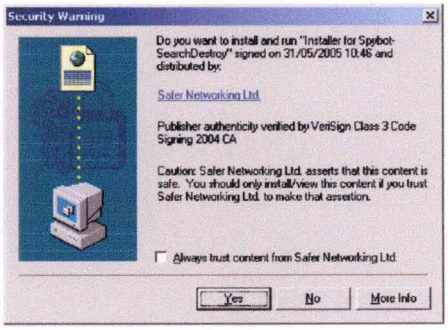


Figure 3 : Installation de Spybot S&D (2)

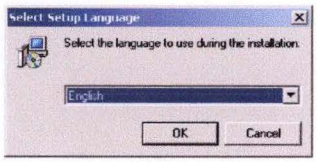


Figure 4 : Installation de Spybot S&D (3)

Figure 5 : Installation de Spybot S&D (4)

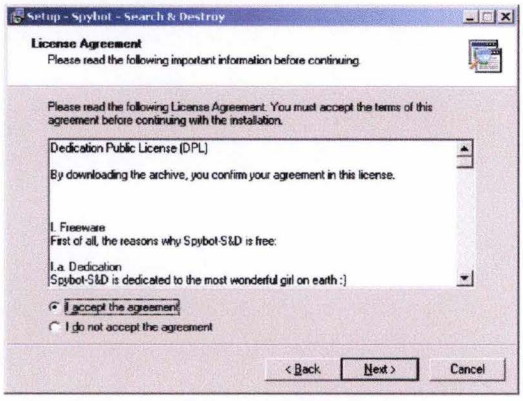


Figure 6 : Installation de Spybot S&D (5)

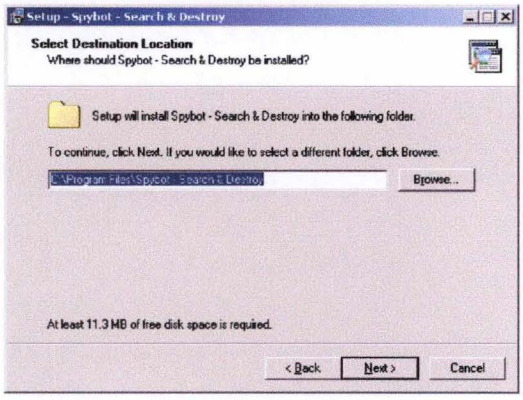


Figure 7 : Installation de Spybot S&D (6)

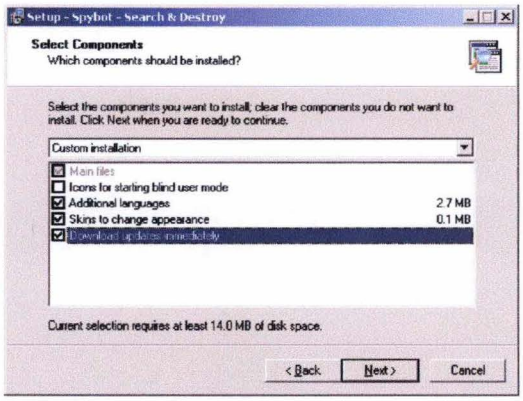


Figure 8 : Installation de Spybot S&D (7)

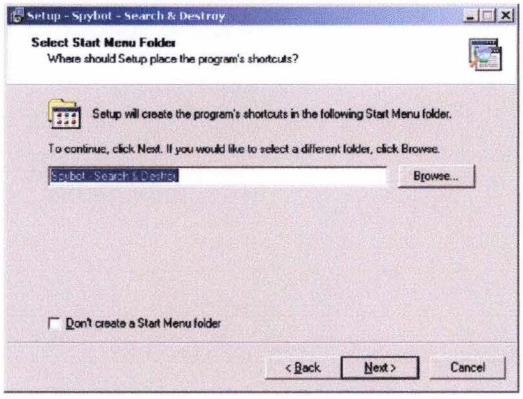


Figure 9 : Installation de Spybot S&D (8)

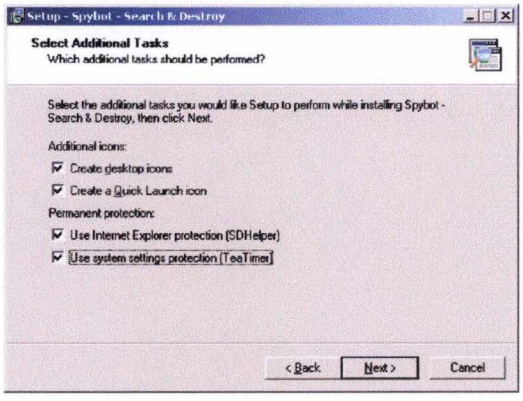


Figure 10 : Installation de Spybot S&D (9)

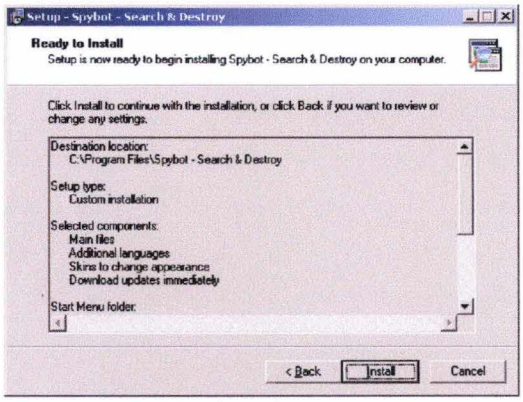


Figure 11 : Installation de Spybot S&D (10)

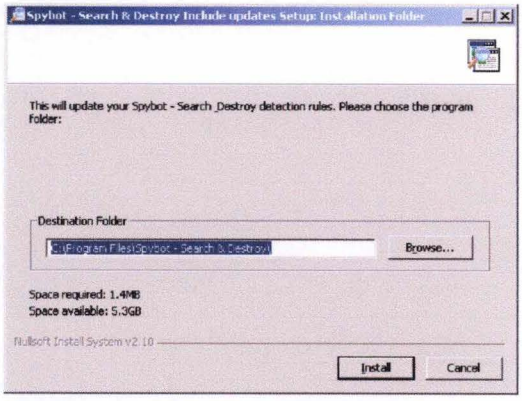


Figure 12 : Installation de Spybot S&D (11)

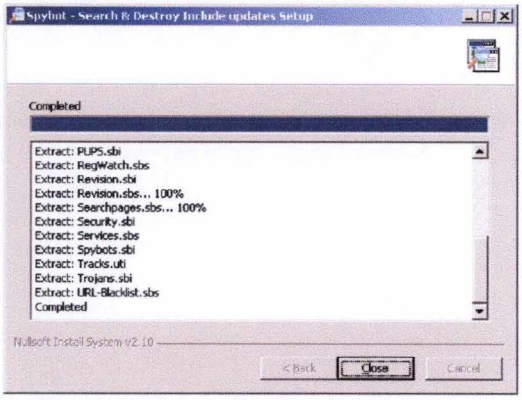


Figure 13 : Installation de Spybot S&D (12)

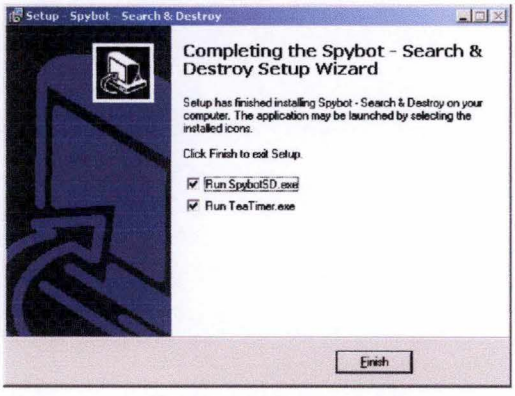


Figure 14 : Installation de Spybot S&D (13)

Figure 15 : Installation de Spybot S&D (14)

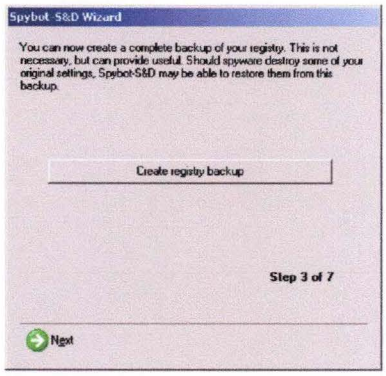


Figure 16 : Installation de Spybot S&D (15)

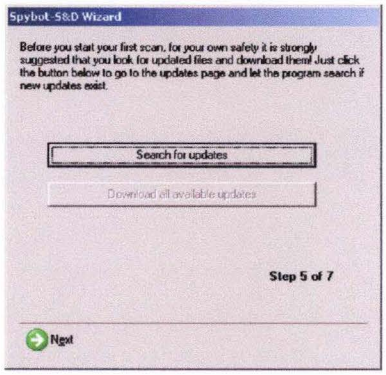


Figure 17 : Installation de Spybot S&D (16)

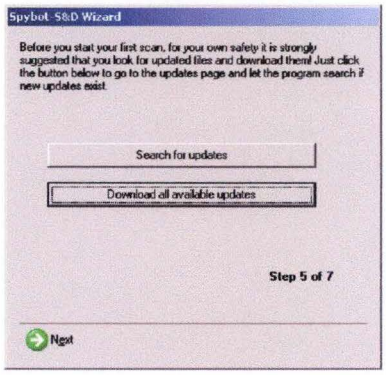


Figure 18 : Installation de Spybot S&D (17)

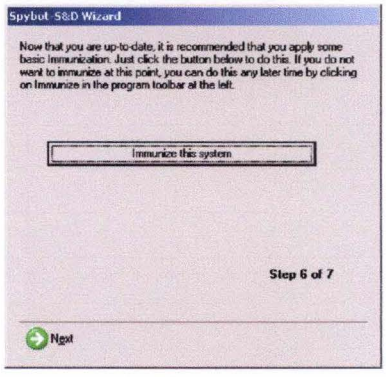


Figure 19 : Installation de Spybot S&D (18)

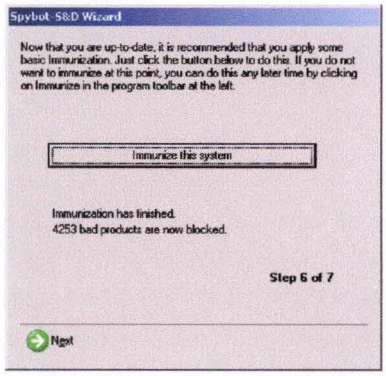


Figure 20 : Installation de Spybot S&D (19)

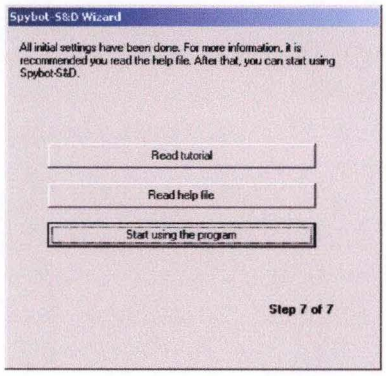


Figure 21 : Installation de Spybot S&D (20)

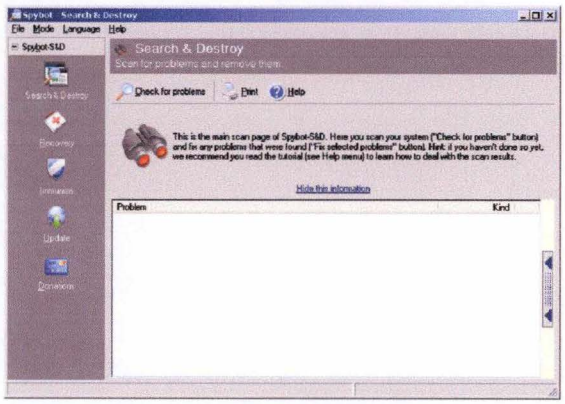


Figure 22 : Installation de Spybot S&D (21)

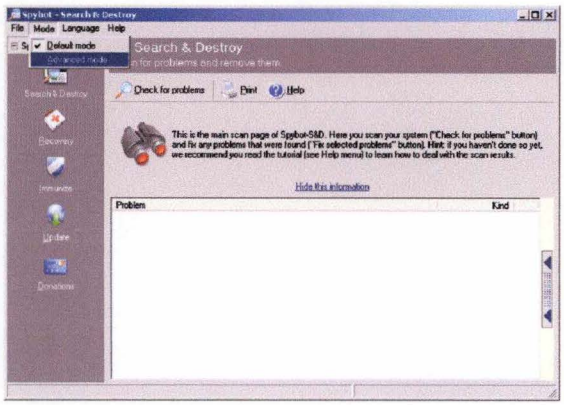


Figure 23 : Installation de Spybot S&D (22)

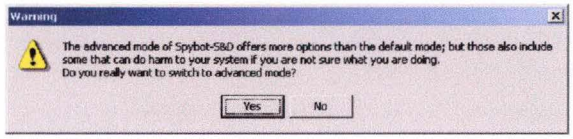


Figure 24 : Installation de Spybot S&D (23)

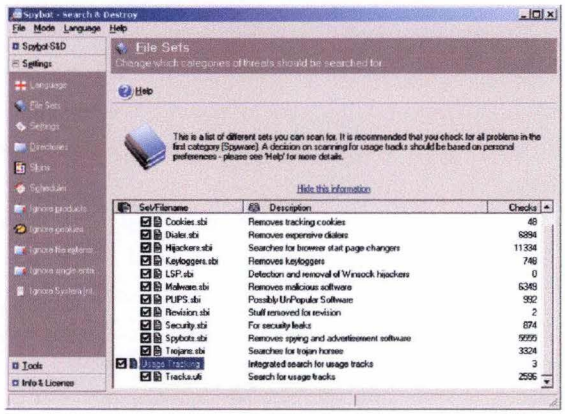


Figure 25 : Installation de Spybot S&D (24)

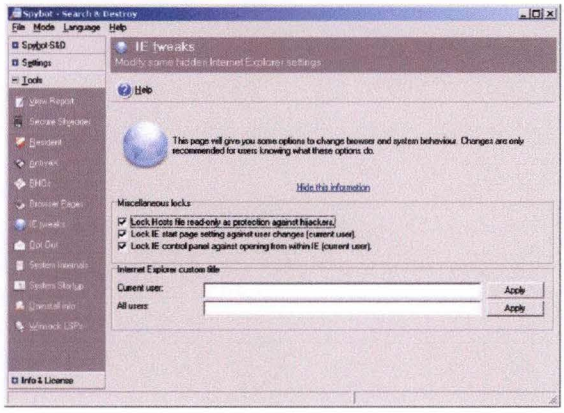


Figure 26 : Installation de Spybot S&D (25)

Figure 27 : Installation de Spybot S&D (26)

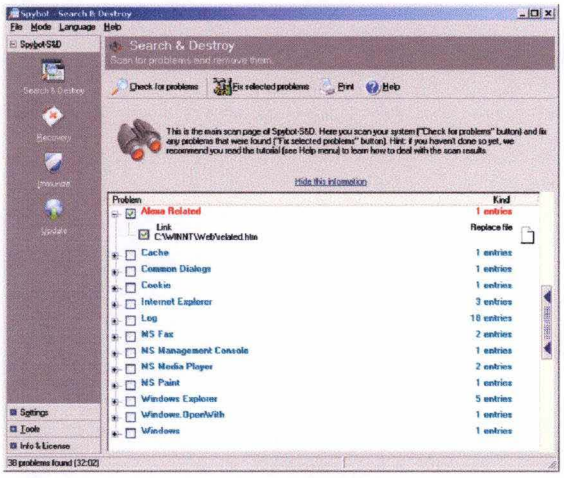


Figure 28 : Installation de Spybot S&D (27)

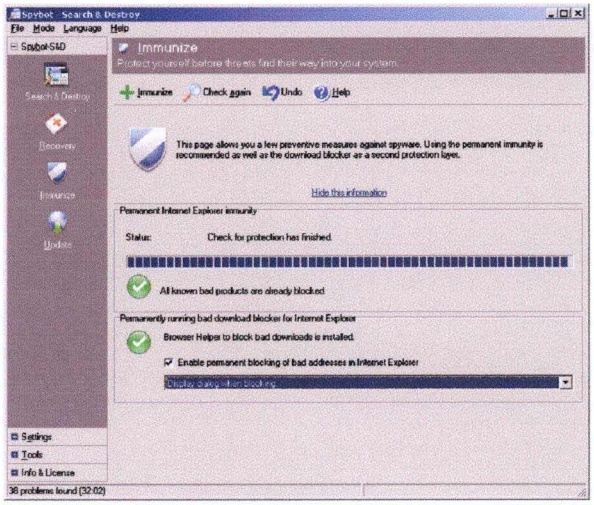


Figure 29 : Installation de Spybot S&D (28)

3.3 Installation de eMedia Codec

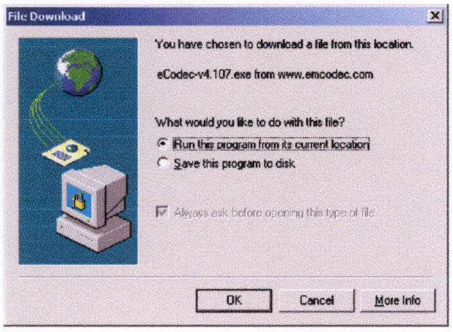


Figure 30 : Installation de eMedia Codec (1)

Figure 31 : Installation de eMedia Codec (2)

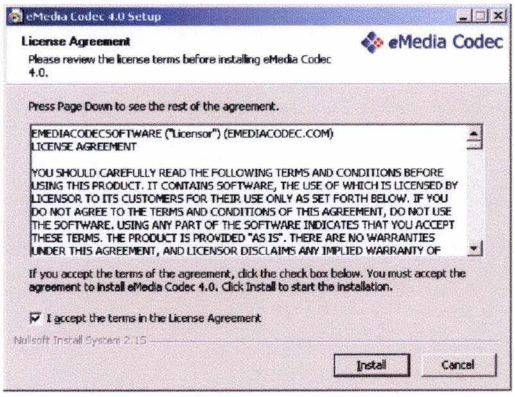


Figure 32 : Installation de eMedia Codec (3)

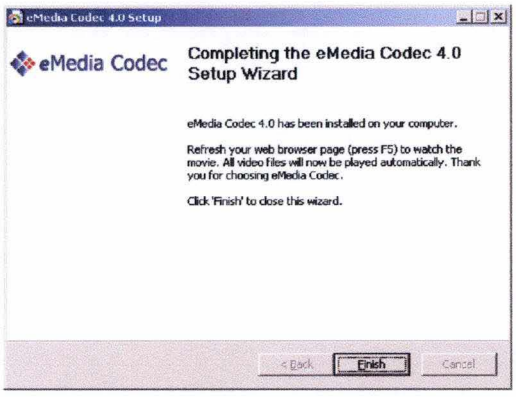


Figure 33 : Installation de eMedia Codec (4)

3.4 Installation de SpywareStrike

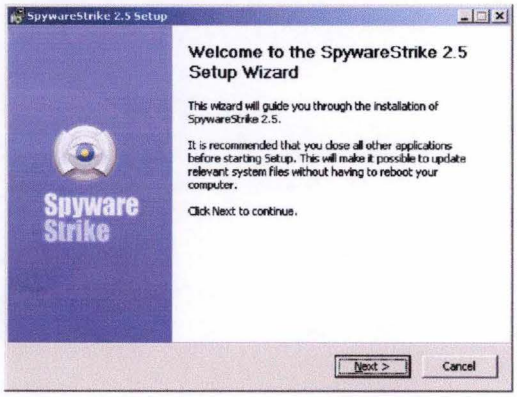


Figure 34 : Installation de SpywareQuake (1)

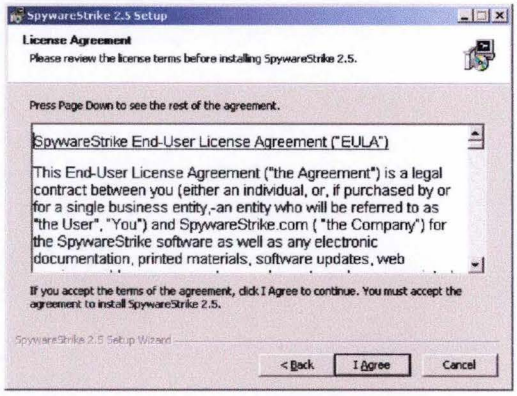


Figure 35 : Installation de SpywareQuake (2)

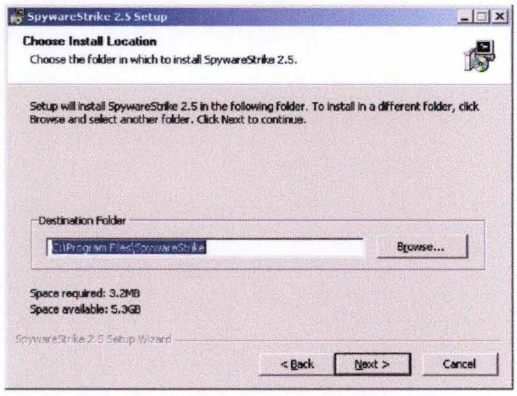


Figure 36 : Installation de SpywareQuake (3)

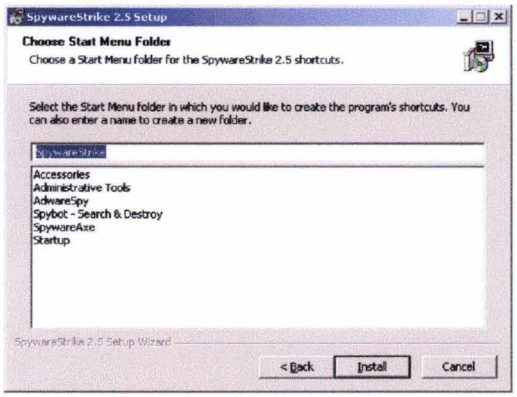


Figure 37 : Installation de SpywareQuake (4)

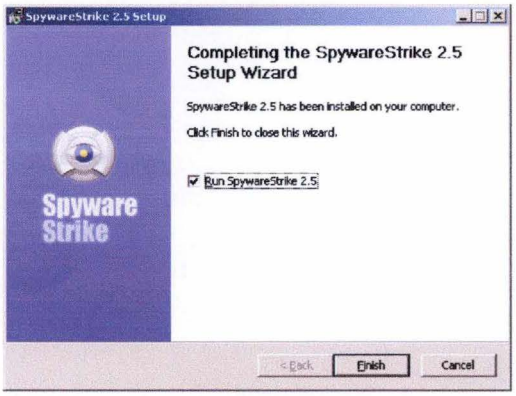


Figure 38 : Installation de SpywareQuake (5)

3.5 Installation d'AdwareSpy

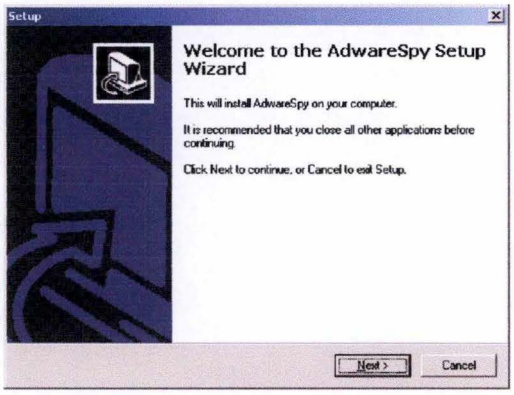


Figure 39 : Installation d'AdwareSpy (1)

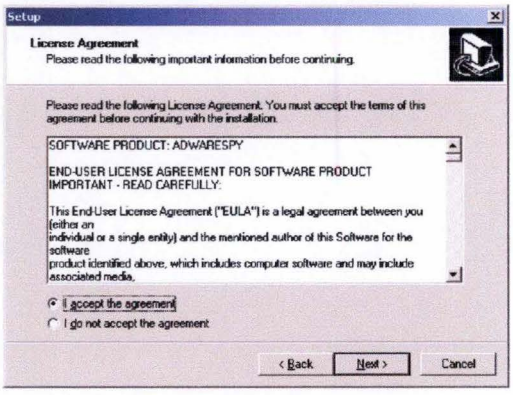


Figure 40 : Installation d'AdwareSpy (2)

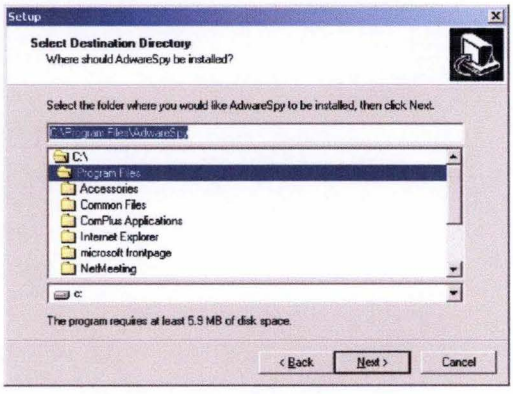


Figure 41 : Installation d'AdwareSpy (3)

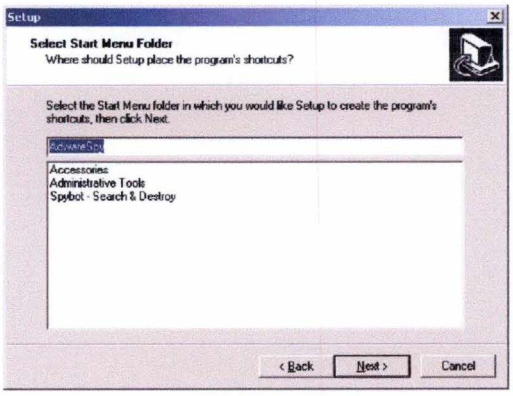


Figure 42 : Installation d'AdwareSpy (4)

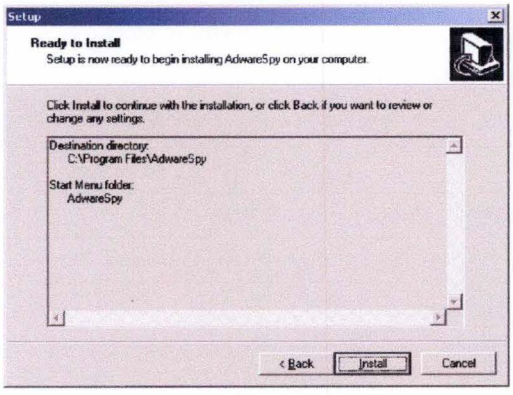


Figure 43 : Installation d'AdwareSpy (5)

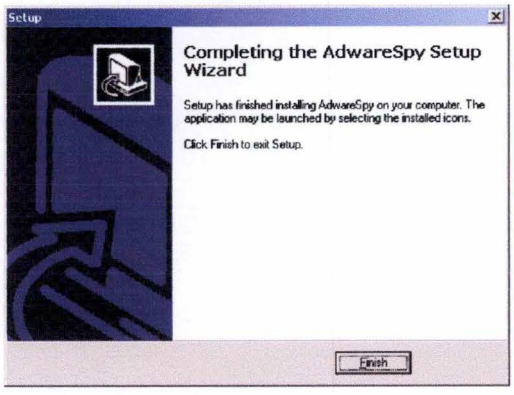


Figure 44 : Installation d'AdwareSpy (6)

3.6 Installation de GAIN Magic Waterfall ScreenScene

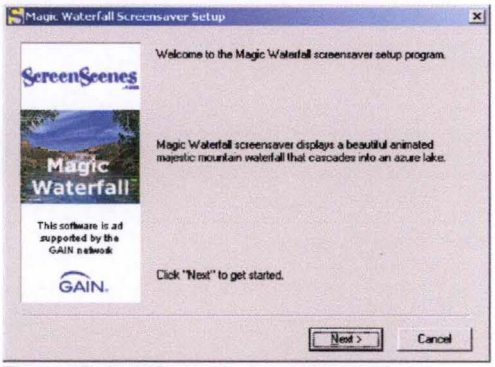


Figure 45 : Installation du ScreenScene (1)

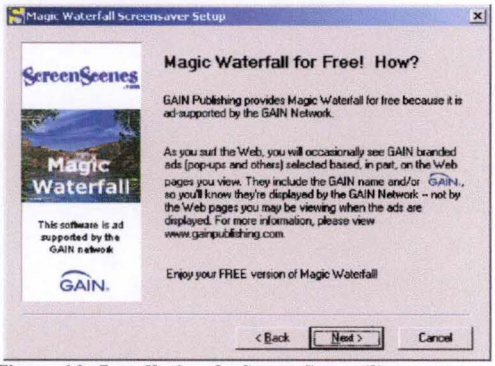


Figure 46 : Installation du ScreenScene (2)

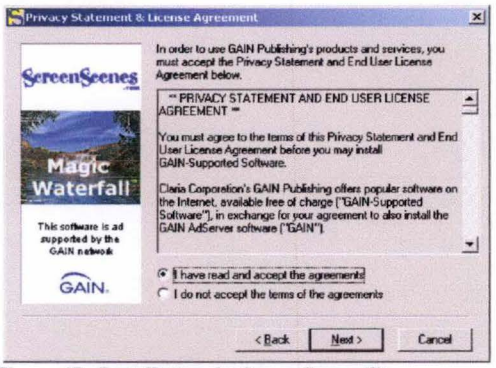


Figure 47 : Installation du ScreenScene (3)

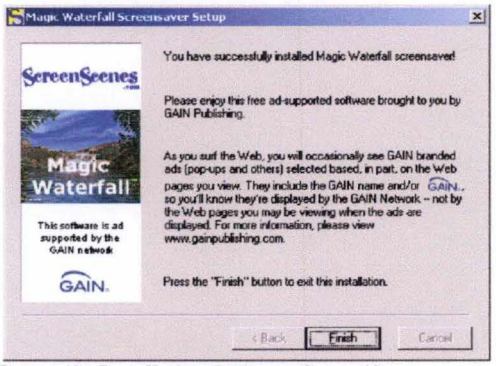


Figure 48 : Installation du ScreenScene (4)

4. Informations spyware de Spybot S&D

4.1 SmitFraud.C

Description
This program installs itself through the internet and creates new desktop wallpaper. This wallpaper looks like a Windows 98 blue screen and contains a warning that the computer is infected with viruses, that one should download run a virus scanner and that the computer wouldn't work in normal mode. In addition to this one gets a desktop icon leading to a pretended anti virus application named PSGuard. Scanning the computer with this software will return a virus found (that was installed by this software itself). In order to remove this virus one has to download the full version for about 20 EUR.
Another unpleasant effect of Smitfraud-C is that some configuration options in the Control Panel will no longer be available. This way it stops the user from changing the wallpaper and forces him to keep the blue screen. Overall Smitfraud-C is a very sneaky software trying to sell PSGuard by frightening less experienced users.

4.2 SpywareQuake

Description
official demoversion appears to install normally but finds a lot of false positives, most likely intentional to make user buy the full product. stealthinstall version gets installed with Vcodec/ Zlob, also capable of reinstall via winlogon hijack and viruswarning popup

4.3 Vcode.eMedia

Functionality
"eMedia Codec" aka "Stream Video Codec" is a multimedia compressor / decompressor.

Description
Malware downloader. Installs Malware like SpyGuard, WinFixer, WinAntiVirus Pro,...

Privacy Statement

SOFTWARE INSTALLATION: Components bundled with our software may report to Licensor and/or its affiliates the installation status of certain marketing offers, such as toolbars, and also generalized installation information, such as language preference and operating system version, to assist Licensor in its product development. No personal information will be communicated to EMEDIACODECSOFTWARE or its affiliates during this process. Licensor may offer additional components through our version checking/update system. These components include: Toolbar, Popup advertising solution, Commercial homepage manager, Commercial messenger.

4.4 Vcodec

Functionality
VCodec is new generation multimedia compressor/decompressor which registers into the Windows collection of multimedia drivers.

Description
Malware Downloader. Changes Zonemaps. Installs Malware like SpyAxe, PSGuard, AV-Gold and Smitfraud-C.

4.5 Zlob.Downloader

Functionality
Malware Downloader

Description
Trojan, which downloads and install various third-party spyware and malware to infected computers: SpyAxe, SpywareStrike, SpyTrooper, Vcodec, ...

5. Liens utiles

5.1 Outils anti-spyware fiables

Spybot Search & Destroy ..... http://www.safer-networking.org
Ad-aware ..... http://www.lavasoft.de
Pest Patrol ..... http://www.ca.com/products/pestpatrol
Spy Sweeper ..... http://www.webroot.com/wb/products/spysweeper/index.php
Spyware Doctor ..... http://www.pctools.com/spyware-doctor
Windows Defender ..... http://www.microsoft.com/athome/security/spyware/software/default.mspx
Mac Scan ..... http://macscan.securemac.com

5.2 Sites d'informations fiables sur les anti-spywares

Spyware Warrior ..... http://www.spywarewarrior.com/rogue_anti-spyware.htm
Spyware Info ..... http://www.spywareinfo.com
Castle Cops ..... http://www.castlecops.com
Dox Desk ..... http://www.doxdesk.com
Ben Edelman Spyware Research . http://www.benedelman.org
Spyware Guide ..... http://www.spywareguide.com
Campaign Against Spyware ..... http://www.cdt.org/action/spyware
Zero Realm ..... http://www.zerorealm.com
CounterExploitation ..... http://www.cexx.org