# Comparatif anti-trojans

1. **Tests 1 - conduits des 22 Janvier au 10 Février 2005 :**
   Tests des capacités « On Access » et « On Boot » poursuivis par un test « On Demand »
   Observation d'une installation de Kazaa V 3.0 US


**http://assiste.free.fr - *ASAP***

**Réactions, suggestions, remarques, idées**
**http://assiste.forum.free.fr/viewforum.php?f=95**

***Remerciements :***
*NickW, modératrice et Vazkor, Le Gromleux et Jim Rakoto, modérateurs sur **les forums d'Assiste**.*

***Dédicace :***
*A Pierre-Henri, mon fils, 7 ans, qui ne m'a pas beaucoup vu durant la réalisation du comparatif et aux membres **ASAP**.*

# 1. Table des matières

# 2. Table des illustrations

# 3. Utilitaires comparés

Nous avons retenu l'intégralité des produits anti-trojans [51] phare actuels, gratuits ou commerciaux, ainsi que la version Bêta 1 de l'anti-spywares de Microsoft (Microsoft AntiSpyware, anciennement « Giant AntiSpyware ») et un antivirus gratuit. Cette sélection par le haut pourra être étendue, par la suite, à d'autres anti-trojans [51] ainsi qu'à des antivirus [52] puisque ces derniers commencent à s'intéresser aux « trojans » [40].

## A propos des termes « trojans » et « anti-trojans »

Rappelons que les parasites appelés, d'une manière générique, et à tort, « trojans » [40], sont beaucoup plus nombreux que les virus.

La popularité du terme « trojans » [40] fait que tous les anti-quelque-chose-de-non-viral sont, désormais, classés à « anti-trojans » [51].

Les éditeurs d'antivirus entrent dans la chasse aux parasites non viraux. Puisqu'il n'existe pas de convention de nommage des parasites non viraux, ils les classent tous, en vrac, à trojan-quelque-chose. Il existe pourtant une classification « forte » organisant en une trentaine de classes les parasites non viraux:

- Adware [55]
- Backdoor [56]
- Binder [57]
- Dialer [58]
- Hijacker [59]
- Keylogger [60]
- Killer [61]
- Packer [62]
- Password Stealer [63]
- Password Attacker [64]
- Password Cracker [65]
- Probe tools [66] - [67]
- RAT – Remote Administration Tool [68]
- Spyware [69]
- …

« Anti-spywares », « anti-adwares » etc. … et « anti-trojans [51] » sont devenus des synonymes et seule la dénomination « anti-trojans [51] » reste. Le terme de « Anti-Spywares » serait préférable car le trojan (le Cheval de Troie) est le véhicule d'une ou plusieurs charges actives. Seules ces dernières nous intéressent et sévissent, d'une manière ou d'une autre, dans une forme d'espionnage.

Lorsque les charges actives ont uniquement une activité parasitaire, existent dans leurs propres objets (fichiers…) et sont installables seules, à la main, ou déployées par un véhicule, elles ne doivent jamais être appelées « Trojan ». Le « Trojan » est le véhicule qui a servi à les déployer. Ce fonctionnement en cheval de Troie peut être choisi délibérément par son éditeur (Kazaa…) ou l'être à son insu (cas de sites de téléchargement de logiciels qui accolent aux utilitaires téléchargés une ou des charges actives, se servant de ce que vous téléchargez comme de chevaux de Troie pour faire pénétrer des parasites dans votre machine).

Lorsque la charge active est intimement liée au code de l'activité apparente du programme hôte (typiquement, presque tous les économiseurs d'écran, les générateurs de clés de licence de logiciels…) il y a ambiguïté car il s'agit d'un cheval de Troie ET keylogger simultanément ou d'un cheval de Troie ET Backdoor simultanément ou d'un cheval de Troie ET d'un RAT etc. … Le parasite n'est pas dissociable du véhicule écrit spécifiquement pour le déployer et la suppression de l'un entraîne la suppression de l'autre. Notre préférence irait à l'appellation directe dans leur classe.

Sur cette page [54], une liste de chevaux de Troie (trojans) au sens véritable du terme.

## Les utilitaires rejetés :

Les utilitaires de sécurité trompeurs, frauduleux ou crapuleux, figurant dans l'anti-logithèque [(46)], ne font et ne feront pas partie de ce comparatif, quand bien même ils auraient cessé, sous la dénonciation de travaux comme ceux de Eric L. Howes [(46)] ou les notres [(46)] et la pression des internautes, leurs activités illicites.

## Les utilitaires comparés :

- A² Free (gratuit) (17)
- Ad-aware se Personal (gratuit) (18)
- Intermute SpySubTract (19)
- Microsoft Antispyware (anciennement Giant Antispware) (beta 1) (20)
- PestPatrol version 4 (21)
- Pestpatrol version 5 corporate (22)
- Spy Sweeper
- Spybot Search & Destroy (gratuit) (23)
- Tauscan (24)
- TDS-3 (25)
- The Cleaner (26)
- AVG Antivirus (gratuit)

# 4. Tests conduits des 22 Janvier au 10 Février 2005

## *Introduction*

Les tests portent essentiellement sur les 2 fonctions les plus importantes des utilitaires de sécurité de type analyseurs (scanners anti-trojans [51] et scanners antivirus [52]) : leurs capacités de réaction « On access » (Accès à un objet) et « On boot » (Démarrage du système). Ces deux fonctions, lorsqu'elles sont implémentées, agissent en temps réel (ou pseudo temps réel), les rapprochant ainsi des outils de contrôle d'intégrité, sans en atteindre les méthodes et résultats. Ces 2 fonctions n'ont rien à voir avec la fonction ordinairement utilisée et comparée : l'analyse périodique, à la demande (« On demand »).

## *A propos des choix*

### Choix des parasites à opposer aux utilitaires testés

Le choix des parasites à « offrir » en pâture s'est porté sur Kazaa et ses « compagnons » pour plusieurs raisons :

- Kazaa est le pourvoyeur de parasites le plus connu au monde (c'est l'archétype des Chevaux de Troie[40]).
- Kazaa est réputé pour être truffé de parasites ce qui nous fait une collection de parasites facile à constituer et à opposer aux utilitaires testés.
- 100% des charges actives transportées devraient être découverts par la totalité des anti-trojans [51] testés et Kazaa lui-même, es-qualité Cheval de Troie et es-qualité outil de P2P, doit également être détecté.
- Les outils qui faillissent à ce test sont mal partis pour figurer dans le haut des comparatifs.
- Kazaa utilise obligatoirement un téléchargeur [47] maison (un downloader [47]) qui s'installe préalablement sur nos machines afin d'y déployer la totalité du premier niveau du colis. Ce téléchargeur [47] pourrait constituer une difficulté pour les utilitaires testés puisque, par obligation, nous allons l'autoriser à s'exécuter.
- Kazaa implante des parasites à fonctionnement pyramidal. Ils vont à leur tour en télécharger et implanter d'autres.
- Kazaa est réputé pour ne plus fonctionner après éradication de certaines de ses charges actives. Certains anti-trojans [51] seraient assez malins pour, non pas éradiquer purement et simplement les charges actives mais les remplacer par des leurres inactivés, Kazaa continuant alors de fonctionner.

2 versions de Kazaa sont disponibles pour la communauté francophone, à la date du test, depuis le site de Kazaa à http://www.kazaa.com/fr/products/downloadKMD.htm :

- Version française 2.6.7
- Version US 3.0

La page US accroche notre attention par cette déclaration « **NO SPYWARE** » ! Sachant que cette version sera disponible en français prochainement, c'est celle-ci que nous avons installée et testée.

Kazaa déclare lui-même :
notre traduction du texte sur http://www.kazaa.com/us/products/downloadKMD.htm :

- **Qu'est-ce que vous installez avec Kazaa v3.0 (version gratuite):**
  **Kazaa** – application principale qui vous permet de chercher, télécharger et partager des fichiers.
  **TopSearch** - affiche des fichiers de meilleure qualité et avec gestion des droits numériques (identifiés par des icônes Or dans les résultats de la recherche). Développée par Altnet.
  **Altnet Peer Points Manager** – C'est un gestionnaire de récompenses pour partager des fichiers marqués avec les icônes Or. Comprend
    **My Search Tool bar**
    **Joltid P2P Networking**
    **Altnet Peer Points Components**
  **BullGuard P2P** – 'BullGuard P2P' fournit une protection antivirus lorsque vous utilisez Kazaa.
  **Publicités** - envoyées par
    **Cydoor** [1]
    **GAIN Network** [2]
  **InstallFinder** – procure des résultats de recherches alternatifs lorsque vous naviguez.

Cette sélection de parasites sera étendue, par la suite, à d'autres parasites afin d'avoir une base de données au spectre assez large. Les tests seront alors reconduits sur une plus grande échelle.

# 5. Préparation de la machine de tests

## *Introduction*

Pour ce test, on se met dans un contexte utilisateur final « normal-haut », pas trop protégé mais pas complètement laxiste. Nous allons donc utiliser le firewall de Microsoft Windows SP2 et l'antivirus gratuit AVG.

Nota
Quelques « promenades », ces derniers jours (décembre 2004 et janvier 2005), à Paris, dans des rayons informatiques de magasins comme la FNAC, le BHV, DARTY etc. … ou chez Surcouf, nous ont permis d'entendre, horrifié, ce conseil constant et criminel des vendeurs : ne pas utiliser de pare-feu (firewall) avec Kazaa !

## *Préparation*

Le but est de préparer une machine totalement propre et proche, en terme de niveau de sécurisation, de la machine de monsieur tout le monde, c'est à dire « niveau zéro » ou peu s'en faut. Elle disposera donc du pare-feu « gratuit » de Windows SP2 et d'AVG, un antivirus gratuit.

### Plate-forme matérielle utilisée :

- Boîtier Thermaltake Xaser III
- Alimentation 550 Watts
- Asus A7N8X deluxe
- Athlon 2700+
- 1 GO ram
- ATI Radeon 9700 Pro
- Lecteur CD
- 1 disque dur 80 GO Maxtor, vierge (neuf) monté sur un canal IDE
- 1 disque dur 250 GO Maxtor, contenant notre bibliothèque d'outils, en USB.
- ADSL Wanadoo 1024
- Moniteur 17 pouces

### Outils logiciels divers

Pour cette préparation, sachant que l'espérance de survie d'une machine non protégée sur le Net est de moins de 4 minutes avant attaque réussie, nous irons le moins possible sur le Net. Nous avons donc, préalablement, téléchargé ou mis à jour la totalité de ce dont nous allons avoir besoin.

- Les utilitaire testés
  - oA² Free (gratuit) [17]
  - oAd-aware SE Personal (gratuit) [18]
  - oIntermute SpySubTract [19]
  - oMicrosoft Antispyware (anciennement Giant Antispware) (beta) [20]
  - oPestPatrol version 4 [21]
  - oPestpatrol version 5 corporate [22]
  - oSpy Sweeper
  - oSpybot Search & Destroy (gratuit) [23]
  - oTauscan [24]
  - oTDS-3 [25]
  - oThe Cleaner [26]

- Divers outils
  - oPhotoImpact pour d'éventuelles captures d'écran
  - oOpen Office pour la rédaction de cette étude
  - oTotal Uninstall (15) – un moniteur d'installation
  - oProcessGuard [16] – un moniteur d'exécution

oMRU Blaster – un nettoyeur de traces

- Un antivirus gratuit
  oAVG
- Pilotes
  oLa dernière version des pilotes du modem ADSL Sagem

## Installation de Windows

- Entrée dans le BIOS de la machine
- Paramétrage du BIOS pour assurer un démarrage à partir du lecteur de CD-ROM
- Le disque dur utilisé est totalement vierge

- Re-Démarrage à partir du CD d'installation de Windows XP Pro.
- Formatage en NTFS du disque dur.
- Installation de Windows XP Pro version française (Licence légale)
- Installation des correctifs du SP2 (CD de Microsoft France)

- Entrée dans le BIOS de la machine
- Paramétrage du BIOS pour assurer un démarrage à partir du disque dur (Disk-0)
- Redémarrage sous un Windows XP Pro SP2 tout neuf.

Remarque : les pilotes de la carte graphique et les pilotes de la carte mère ne sont pas installés. Nous sommes 100% sous un Microsoft Windows pur et les pilotes livrés avec.

## Paramétrage du centre de sécurité :

- Le pare-feu de Windows est activé
- Les mises à jour automatiques sont désactivées
- Pas d' antivirus [(52)] (le centre de sécurité de Windows verra, après son installation, l'antivirus AVG)

## Création d'une connexion

- Installation « à la main » des pilotes du modem, sans passer par le kit du fournisseur d'accès Internet
- Paramétrage d'une connexion Internet avec l'assistant de Windows (Démarrer > Connexion > Afficher toutes les connexions > Créer une nouvelle connexion), sans utiliser le kit du fournisseur d'accès fourni sur un cd-rom, toujours suspect, donc sans implanter ses spywares qui polluent l'ouverture de la connexion par un énorme trafic suspect.

## Windows Update

- Connexion sur Windows Update
- Téléchargement et installation des nouveaux correctifs depuis la publication du SP2
  - KB 980175
  - KB 890830
  - KB 885836
  - KB 873339
  - KB 885835
  - KB 886185
  - KB 834707
- Déconnexion

## Préparation de la surveillance du système

- Installation de Total Uninstall
  Surveiller toutes les traces de chaque installation et de chaque navigation. Toutes les actions qui suivent se passent sous Total Uninstall [(15)]
- Installation de ProcessGuard Free [(16)]
  C'est une application en temps réel [(27)] chargée de surveiller tout lancement de processus et de

signaler si son lancement ou son activité n'est pas conforme à certaines règles (autorisation de se lancer, interdiction pour un processus de tuer un autre processus etc. …). Pour l'instant, ProcessGuard est paramétré en mode apprentissage durant toute la phase d'installation des autres outils.

- La surveillance système sera complétée du Tea-Timer, processus pseudo temps réel [27] de Spybot Search & Destroy qui, lui, signale certaines modifications apportées à la base de registre.

## Installation de l'antivirus gratuit AVG

- Installation de AVG.
- Connexion
- Mise à jour
- Déconnexion
- Paramétrage
  Tous les paramètres d'origine + « Scan all files »
- Analyse du système
- Ok – Le système est propre d'après AVG

Nota : AVG utilise une ADS [42] attachée au fichier (pour la version actuelle) avg70free_300a419.exe

# *Installation et paramétrage des anti-trojans*

## Installation de Spybot Search & Destroy [23]

Installation avec ses modules SDHelper et TeaTimer.
Le TeaTimer est installé pour sa capacité à signaler en temps pseudo réel [27] certains changements apportés à la base de registre de Windows et aussi pour être comparé aux autres modules temps réel [27] des autres anti-trojans [51] dans sa capacité à bloquer l'implantation de certains parasites ou à la signaler pour que l'utilisateur prenne une décision.

Connexion
Mise à jour de Spybot S&D
Déconnexion.
L'immunisation, outil purement préventif de Spybot, n'est pas appliquée afin de ne pas bloquer l'implantation des parasites contenus dans le logiciel à tester et que nous souhaitons révéler.
Réglages de Spybot :

- Modules additionnels : tous
- Mode « Avancé »
- Mouchards Exclus :
  - DSO Exploit est coché (exclu - il s'agit d'un bug dans Spybot et il faut exclure ce test)
  - Toutes les exclusions paramétrées d'origine dans Spybot doivent être décochées
    - LSP.New.net
    - MySearch
    - New.Net
    - SideStep
- Cookies Exclus
  - Aucun cookie ne doit être coché afin d'assurer leur destruction lors du nettoyage des traces, avant de lancer la surveillance du logiciel à tester.

Analyse du système
Il y a un cookie de DoubleClick détecté et quelques traces de type MRU [28] normales et sans importance pour notre test.

## Installation de A² [17]

Installation
Connexion
Mise à jour

- La mise à jour est obligatoire
- Nécessite la création d'un compte chez l'éditeur de A²
- Nécessite le paramétrage d'un client de messagerie (Outlook Express) pour recevoir un e-mail à lire.

Déconnexion
Analyse du système
OK – Le système est propre d'après A² Free qui ne signale pas la présence du cookie traceur de DoubleClick.

## Installation de Ad-Aware SE Personal [18]

Installation
Connexion
Mise à jour
Déconnexion
Paramétrage

- Forcer l'analyse des fichiers archives (fichiers compressés)

Analyse du système (Full system scan)
Ok – Le système est propre d'après Ad-Aware
Il y a un cookie de DoubleClick détecté et quelques traces de type MRU [28] normales et sans importance pour notre test.

## Installation de InterMute SpySubTract [19]

InterMute est la société qui a acquis le petit utilitaire gratuit de l'étudiante Merijn, CWShredder, bien connu dans le monde de la sécurité sur Internet,
Installation. L'utilitaire optionnel préventif « Venus » est installé.
Connexion
Mise à jour
Déconnexion
Paramétrage

- La taille maximale au delà de laquelle un fichier n'est pas analysé est mise à zéro afin que tous les fichiers soient analysés.

Analyse du système (Full scan)
Ok – Le système est propre d'après InterMute SpySubTract
Il y a un cookie de DoubleClick détecté

## Installation de Microsoft AntiSpyware (ex Giant AntiSpyware) [20]

Installation
AutoUpdate : Non [14]
Protection Temps Réel [27] : Oui
SpyNet : Non (principe de « push » qui constitue une faille majeure de sécurité)
Connexion
Mise à jour
Déconnexion
Analyse du système (Full Scan)
Ok – Le système est propre d'après Microsoft AntiSpyware
Nota : bien que les cookies soit analysés par Microsoft AntiSpywares et bien qu'un cookie de DoubleClick soit installé actuellement sur le système, cookie bien connu pour donner des boutons à tous les internautes, Microsoft AntiSpyware ne le signale pas.

## Installation de PestPatrol V4 [21]

Installation
Il faut donner un nom, prénom, adresse e-mail mais l'envoi pour enregistrement n'est pas obligatoire (si une connexion n'est pas préalablement établie, l'envoi échoue et le processus d'installation se poursuit normalement)
Paramétrage :

- Where to Search ?
  - All Files
  - Desktop
  - Thorough
  - Show Hidden
- What to Search ?
  - Tout sélectionner
- What to Exclude
  - Ne rien exclure de l'analyse, en particulier supprimer les 2 exclusions par défaut (corbeille de Windows et System Volume Information)

Connexion
Mise à jour
Déconnexion
Analyse du système
Ok – Le système est propre d'après PestPatrol V4
Il y a un cookie de DoubleClick détecté

## Installation de PestPatrol V5 Corporate [22]

Installation
Nécessite l'installation de Microsoft .NET FrameWork
Connexion
Téléchargement et installation de Microsoft .NET FrameWork pris en charge automatiquement par l'installateur de PestPatrol V5 Corporate

Mise à jour de PestPatrol V5
Paramétrage :

- Active Protection : Enable
- Mémoire
- Cookies
- Base de registre
- Emplacement courants
- All Hard Drives

Analyse du système (Scan Now)
Ok – Le système est propre d'après PestPatrol V5
Nota : bien que les cookies soit analysés par PestPatrol V5 Corporate, le cookie de DoubleClick, actuellement sur le système, n'est pas signalé.

## Installation de Spy Sweeper

Installation avec « Run at Startup » et « Add to Windows Explorer Context Menu »
Connexion
Update Program
Update Definitions
Déconnexion
Paramétrage

- Program Options
  - Automatic check for Updates est désactivé
- Sweep option
  - L'option « Do not sweep restore folder… » est décochée : on veut analyser également le contenu des points de restauration du système [41].
  - Sweep all folders

Analyse du système
Ok – Le système est propre d'après Spy Sweeper
Nota : Spy Sweeper utilise une ADS [42] attachée au fichier (pour la version testée) ssfsetup1_1780952792.exe

## Installation de Tauscan [24]

Installation
Connexion
Mise à jour
Déconnexion
Paramétrage

- All Files

Nota : Advanced Trojan Analyser ne doit être activé que si vous avez plusieurs heures devant vous. Ce paramètre peut être activé / désactivé en cours de scan sans avoir besoin de tuer Tauscan et de le relancer.
Analyse du système
Ok – Le système est propre d'après Tauscan
Nota : Tauscan n'analyse pas les cookies
Nota : Tauscan utilise une ADS [42] attachée au fichier taubase.exe

## Installation de TDS-3 [25]

Installation
Configuration :

- Scan Control > Scan Option
  - Tout coché
- Scan Task Configuration
  - Memory Mutexes
  - Scan All Hard Drives
  - Registry & Files traces
  - System files CRC32

Connexion
Mise à jour

Déconnexion
Analyse du système
Ok – Le système est propre d'après TDS-3
Nota : TDS-3 n'analyse pas les cookies. TDS-3 est un cauchemar à paramétrer, surtout si on ne lit pas l'anglais. Il dispose de plusieurs petits outils d'aide à l'utilisateur avancé mais qui n'ont rien à voir avec l'analyse anti-trojans [51] et finissent d'enfoncer l'utilisateur « normal » dans la perplexité la plus totale.
Nota : TDS-3 utilise une ADS [42] attachée au fichier radius.td3.

## Installation de The Cleaner [26]

Installation avec TCActive et TCMonitor
Connexion
Mise à jour
Déconnexion
Paramétrage

- Scan in archives
- Scan for hidden executables

Analyse du système
Ok – Le système est propre d'après The Cleaner
Nota : The Cleaner n'analyse pas les cookies

## Installation de Ulead PhotoImpact

Pour les captures d'écrans

# 6. Le comparatif anti-trojans

## *Bavardage entre un utilitaire et son serveur*

### But de la mesure

On cherche à savoir s'il y a du « bavardage » lors d'une connexion d'un utilitaire vers son serveur de mise à jour alors qu'aucune mise à jour n'est disponible.

### Mesure

Les utilitaires ont été mis à jour dimanche 23 janvier 2005 au matin. L'après midi même, nous entreprenons de mesurer la quantité de caractères envoyés / reçus, lors d'une demande de mise à jour, alors qu'il ne doit pas y avoir de trafic puisque les produits sont à jour.

Nous avons ouvert une connexion par Démarrer > Connexion > Nom de la connexion, lancé un utilitaire, demandé sa mise à jour, relevé les chiffres du trafic puis fermé la connexion pour passer à l'utilitaire suivant.

Ces chiffres sont des ordres de grandeur car, dès qu'une connexion est établie, des paquets sont envoyés et reçus ne serait-ce que pour permettre au fournisseur d'accès d'authentifier la demande, mesurer la vitesse etc. … puis d'autres serveurs envoient des « ping » …Il y a quelques centaines de caractères ainsi envoyés / reçus.

Ce qu'il faut observer est le différentiel entre les uns et les autres. 3 utilitaires sortent du lot (plus un cas particulier) :

- Spybot reçoit beaucoup de caractères (probablement l'emprunte de chaque fichier dans chaque langue ce qui fait beaucoup de fichiers – c'est normal). Ce nombre est constant si on recommence plusieurs fois la manipulation.

- A² Free reçoit également un peu plus de caractères que la moyenne.

- Microsoft AntiSpyware, lui, en envoie beaucoup plus que les autres. Il faudrait analyser le contenu de ces paquets sortants (à condition qu'ils ne soient pas cryptés).

- PestPatrol v4, entre dimanche matin et dimanche après-midi, bénéficiait d'une mise à jour (300Ko) en plein week-end. Ces gens-là ne se reposent donc pas ! Nous avons recommencé le test juste après pour avoir des mesures comparables. PestPatrol est un peu plus lent car il prend la peine de fermer tous ses modules avant de lancer la mise à jour éventuelle, incluant celle du code, puis il relance tout. Les autres utilitaires n'assurent automatiquement que la mise à jour des bases de signatures et se reposent sur l'utilisateur s'il y a une mise à jour des binaires à faire.

Le temps de mise à jour, dans notre test durant lequel il n'y a pas de mise à jour, n'est pas mesurable. Il est, à ce stade, fonction de la vitesse des doigts sur les touches du clavier ou la vitesse du poignet déplaçant la souris ! Nous l'avons arrondi à 5 secondes chaque fois.

### Notation : formule de calcul pour obtenir une notation /10

Il n'est pas tenu compte de ces mesures dans le comparatif final.

### Notation : prise en compte dans la note finale

Sans objet.

| Bavardages | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Octets envoyés | 4000 | 4000 | 5000 | 12000 | 5080 | 6000 | 4000 | 4700 | 5200 | 4500 | 4600 | 3500 |
| Octets Reçus | 10000 | 3500 | 3000 | 5500 | 4721 | 3000 | 3500 | 30000 | 3200 | 3200 | 4200 | 3000 |
| Durée (en secondes) | 5 | 5 | 5 | 5 | 20 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |

*Figure 1 – Tableau - Bavardages entre un utilitaire et son serveur*

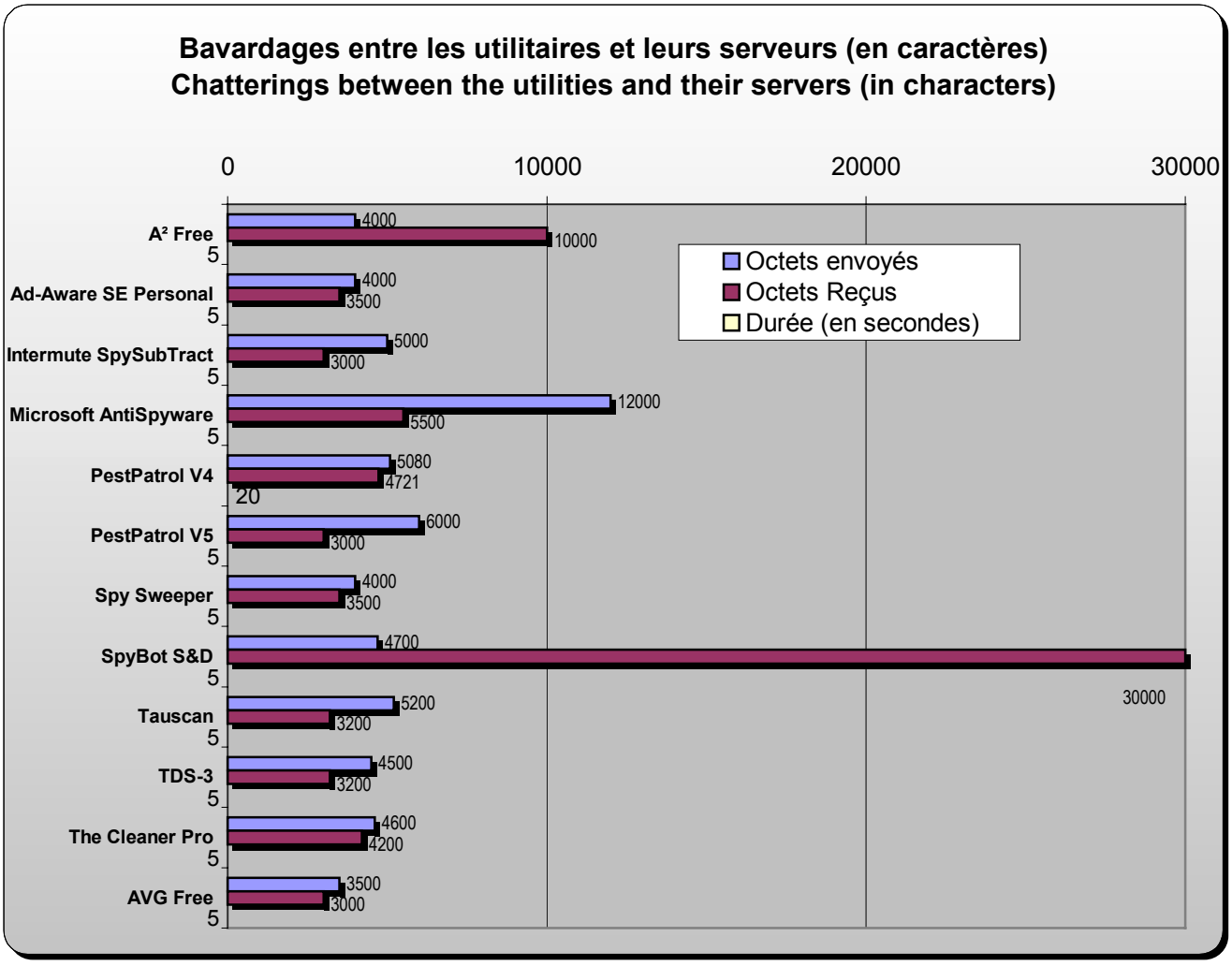


*Figure 2 – Graphique - Bavardages entre un utilitaire et son serveur*

## *Durée d'exécution des analyses à la demande (Scan « On demand »)*

### But de la mesure

La durée d'exécution des analyses à la demande est un élément de confort. Cette mesure de durée est relativement peu importante en terme de sécurité, mais, corrélée avec la charge processeur mobilisée, elle permet de se rendre compte de la possibilité réaliste d'usage d'un utilitaire durant l'exploitation normale de l'ordinateur (par exemple, de jour durant les heures de travail). Peut-il être réalistement exécuté en concurrence avec d'autres applications ? Est-il raisonnablement « employable » ou « écroule » t'il complètement une machine ?

### Mesure

Cette mesure est prise, sachant que les utilitaires ont été réglés à leur maximum et que le disque analysé contient uniquement Windows XP Pro SP2, les utilitaires cités et une implantation de Kazaa avec ses parasites associés. Ce n'est pas tant le temps brut qu'il faut regarder mais plutôt le différentiel entre les scanners les plus rapides et les plus lents.

Le nombre le plus petit est le meilleur : il signe le scanner le plus rapide.

- PestPatrol V5 Corporate est imbattable et certains modules de PestPatrol V4 commencent à bénéficier de la technologie de la V5 Corporate.

- Spybot est un cas particulier. Sa vitesse est magique mais ce n'est pas un scanner de fichiers. Vous pouvez copier une collection de 100.000 parasites tous plus dangereux les uns que les autres, sur un disque système. Spybot n'en verra strictement aucun. A fortiori sur des disques ou des partitions secondaires dont il se fiche comme de sa première chemise. Spybot ne s'intéresse pas aux parasites présents mais aux parasites installés, ce qui est totalement différent.

- Tauscan est complètement hors jeu en matière de vitesse d'analyse. Ici, le temps donné est celui d'un scan « normal » afin que Tauscan reste dans des temps comparables aux autres. Si on le règle à son maximum, comme pour les autres scanners de ce test, il va mettre 8h53' pour faire le même travail soit 31.980 secondes ! On ne sait pas ce qu'il fait durant tout ce temps (sand-boxing (simulation d'exécution dans une machine virtuelle appelée « bac à sable »…) de chaque exécutable ?…).

### Notation : formule de calcul pour obtenir une notation /10

Ces mesures sont prises en compte dans le comparatif final.
La note est attribuée au différentiel entre le plus rapide et le plus lent et est calculée par
A=durée mesurée
B=durée la plus courte
C=Durée la plus longue
10-((A-B)/(C-B)*10)
Le plus petit différentiel obtient 10, le plus grand 0

### Notation : prise en compte dans la note finale

La mesure de la durée (vitesse) d'exécution d'une analyse totale (réglage maximum et application sur l'intégralité des objets) n'est pas très importante en terme de sécurité. C'est un élément de confort qui doit peu influer sur le résultat final. Le résultat de cette mesure est donc affecté du coefficient « 1 ».

| Durée d'un scan "on demand" | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Durée d'un scan "on demand" | 776 | 270 | 511 | 390 | 400 | 77 | 254 | 103 | 640 | 830 | 994 | 568 |

*Figure 3 – Tableau - Durée d'exécution des analyses (scan) à la demande*

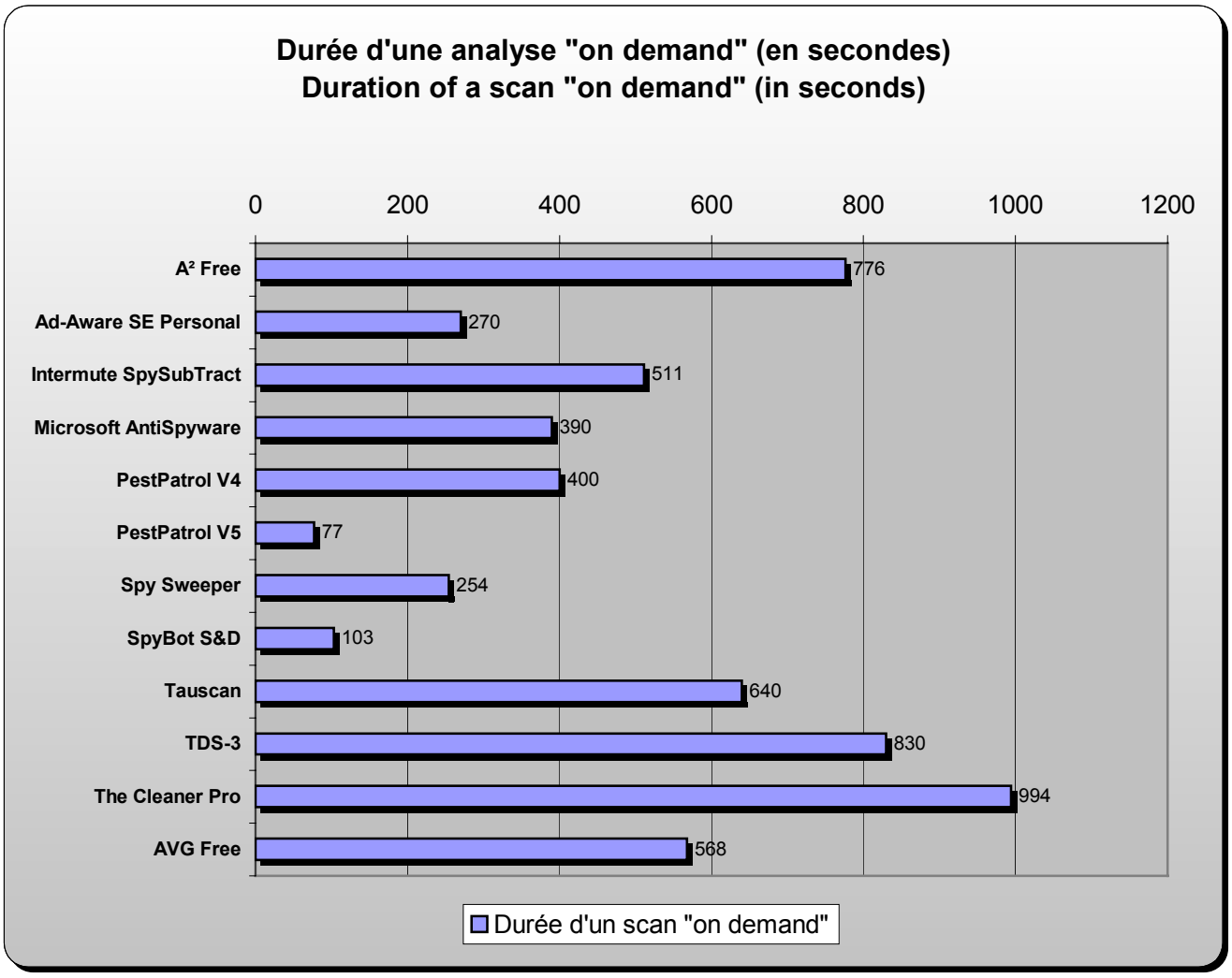


*Figure 4 – Graphique - Durée d'exécution des analyses (scan) à la demande*

## *Nombre d'objets analysés*

### But de la mesure

Nous cherchons à savoir si l'utilitaire mesuré prend bien en compte la totalité des objets présents ou s'il fait des impasses.

### Mesure

Cette information est impossible à avoir « sérieusement » ! Elle est crétinisée par la politique de communication des éditeurs. Ils s'imaginent plus crédibles en gonflant les chiffres. Certains comptent les items de la base de registre. Lorsqu'ils commencent à analyser leur premier fichier, ils sont déjà à 30.000 ou 40.000 prétendus objets analysés !

Il y a exactement 34.469 objets de type fichiers ou répertoire, y compris les répertoires et les fichiers cachés et système, sur la machine de test. Il y a également 32.876 items dans la base de registre.

Certains outils excluent (ne testent pas) certains types de fichiers qui ne peuvent être pollués, d'autres n'excluent rien pensant qu'un innocent .gif peut cacher un .exe dont on a changé le suffixe. On estime les scanners annonçant entre 20.000 et 30.000 objets scannés sur la machine de tests comme honnêtes. Les scanners annonçant dans les 50.000 objets analysés ajoutent aux 20.000 fichiers environ qu'ils doivent réellement analyser, les 32.876 items de la base de registre.

- PestPatrol v5 ne donne pas d'information.
- Tauscan, The Cleaner ou AVG semblent analyser réellement le plus grand nombre de fichiers.
- TDS et A² Free font d'importantes impasses.
- Microsoft AntiSpyware est l' anti-trojans [(51)] qui analyse le moins de fichiers.
- Ad-aware SE Personal, avec ses 85.605 objets analysés, est complètement délirant, surréaliste. Ce nombre relève d'une pure paranoïa commerciale, ce produit étant gratuit pour servir d'appel à la version payante. Ce nombre doit décompter tous les items de la base de registre + tous les cookies + tous les contenus des archives (les .zip, .cab etc. …) et d'autres encore…

### Notation : formule de calcul pour obtenir une notation /10

En théorie, le plus grand nombre serait le meilleur mais, à cause de la fantaisie des chiffres annoncés, il ne peut être tenu compte de ces mesures dans le comparatif final.

### Notation : prise en compte dans la note finale

Sans objet.

| Nombre d'objets analysés | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nombre d'objets analysés | 25800 | 85605 | 49435 | 23177 | 50723 | ? | 32876 | 25607 | 32207 | 24099 | 31703 | 33211 |
| Dont items en mémoire | | | | | | | 1770 | | | | | |
| Dont items en base de registre | | | | | | | 32876 | | | | | |
| Dont items fichiers/répertoires | | | | | | | 25027 | | | | | |

*Figure 5 – Tableau - Nombre d'objets analysés par les scanners*

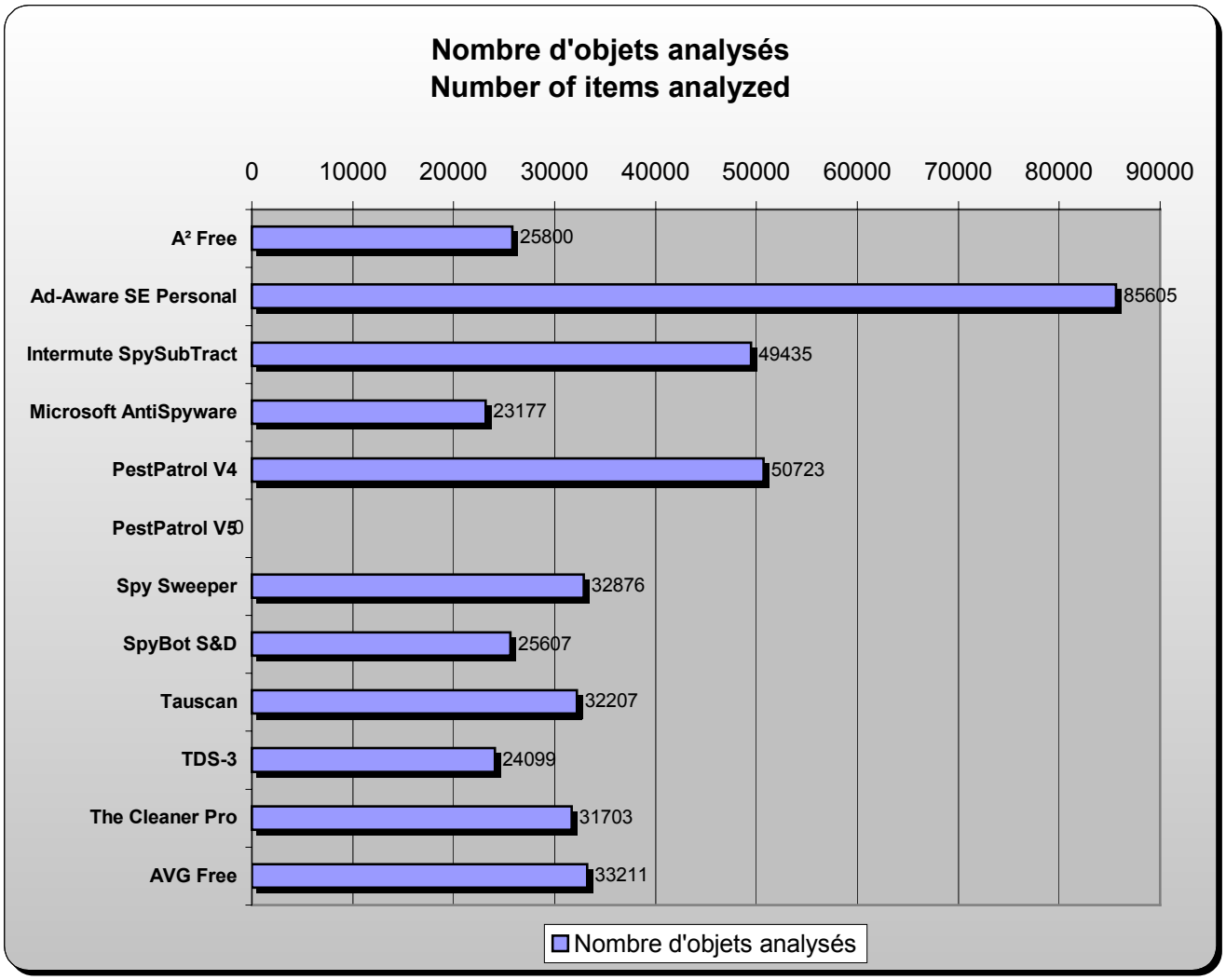


*Figure 6 – Graphique - Nombre d'objets analysés par les scanners*

# *Tailles des processus d'analyse (scanners) en mémoire*

## But de la mesure

C'est une information sensible car sur des machines à taille mémoire « normale », les pics de consommation sont souvent la cause de plantages.

## Mesure

Il y a deux mesures :

- Pic de consommation
  Donnée directement par le gestionnaire de tâches de Windows. C'est la mesure la plus intéressante.
- Consommation moyenne
  Ressource moyenne consommée, approximative. Nous n'avons pas trouvé d'outil gratuit permettant de nous donner cette mesure.

Les nombres les plus petits sont les meilleurs.

## Notation : formule de calcul pour obtenir une notation /10

Seul le pic de consommation mémoire est pris en compte dans le comparatif final.
La note est attribuée au différentiel entre le plus grand et le plus petit et est calculée par
A=pic mesuré
B=pic le plus faible
C=pic le plus élevé
10-((A-B)/(C-B)*10)
Le plus petit différentiel obtient 10, le plus grand 0

## Notation : prise en compte dans la note finale

La mesure du pic mémoire d'un processus, lors d'un scan total (réglage maximum et application sur l'intégralité des objets) n'est pas très importante en terme de sécurité. C'est plus une mesure d'usage réaliste des produits. Le résultat de cette mesure doit donc peu influer sur le résultat final et est donc affecté d'un coefficient 1

| Taille des processus | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Taille moyenne | 13750 | 19500 | 39800 | 38500 | 32000 | 37500 | 32000 | 31000 | 9600 | 21000 | 21500 | 22000 |
| Pic de taille | 20724 | 25332 | 47308 | 42468 | 38392 | 38840 | 37380 | 33856 | 12528 | 35888 | 23072 | 28908 |

*Figure 7 – Tableau - Pic de taille et taille moyenne des processus en mémoire*

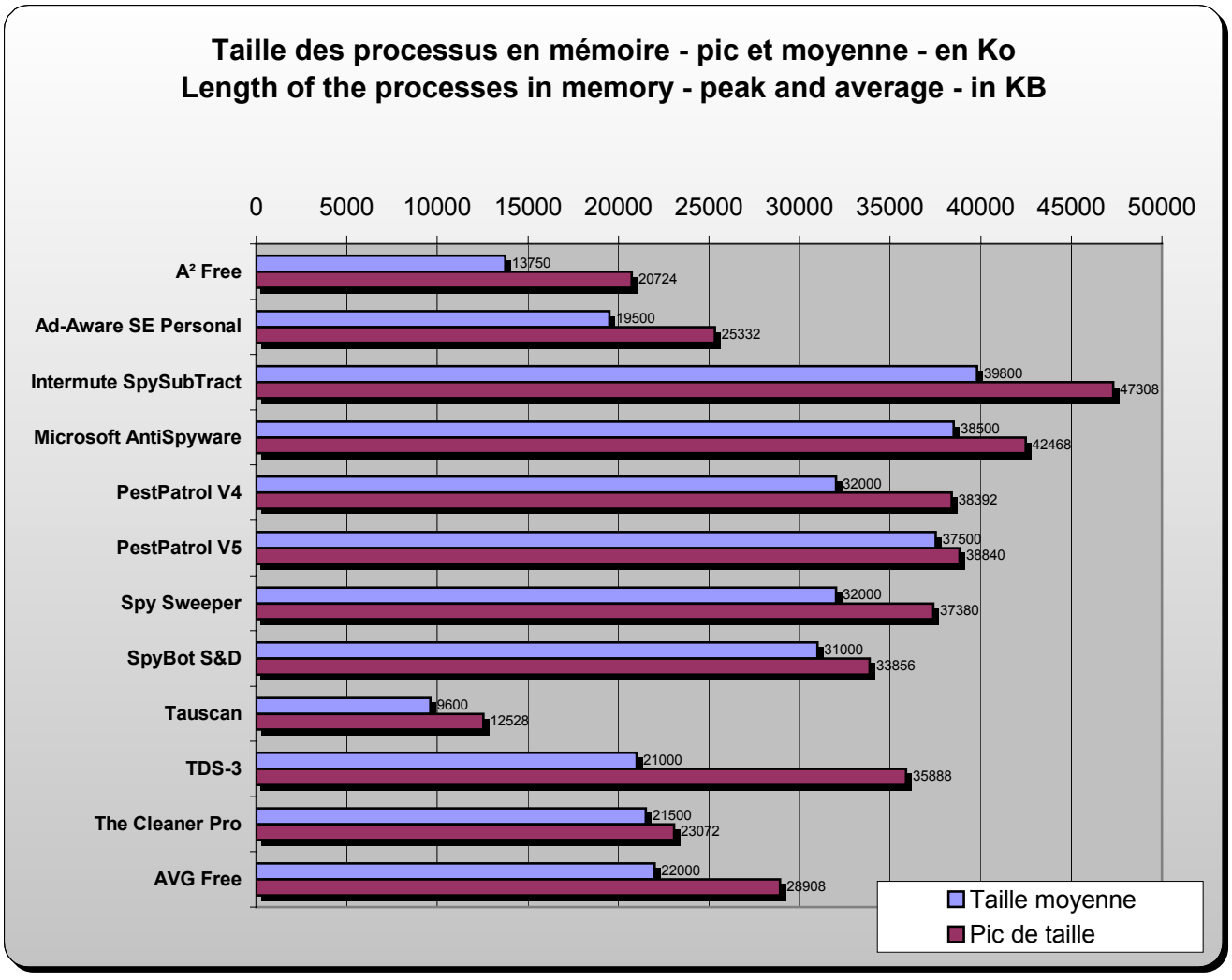


*Figure 8 – Graphique - Pic de taille et taille moyenne des processus en mémoire*

## *Charge d'utilisation de la puissance du processeur*

### But de la mesure

La charge processeur des analyses à la demande est un élément de confort. Cette mesure permet, corrélée avec la durée d'exécution des analyses, de se rendre compte de la possibilité réaliste d'usage d'un utilitaire durant l'exploitation normale de l'ordinateur (par exemple, de jour durant les heures de travail). Peut-il être réalistement exécuté en concurrence avec d'autres applications ? Est-il raisonnablement « employable » ou « écroule » t'il complètement une machine.

### Mesure

Pourcentage des ressources processeur mobilisées par le processus. Chiffre moyen, du début à la fin du processus d'analyse. Peut connaître des pics à 100% et des périodes de « calme ». Ces mesures sont approximatives : nous n'avons pas trouvé d'outil gratuit, utilisable par tous, permettant de donner cette mesure.

Le nombre le plus petit est le meilleur.

Le résultat de PestPatrol V5 Corporate laisse tous les autres loin derrière alors que la pertinence de ses résultats (parasites trouvés) est bonne. C'est extrêmement étonnant. Nous avions déjà testé l'analyse en ligne par PestPatrol, il y a plusieurs mois. Elle utilisait alors la future technologie de la V5 actuelle (uniquement sur les processus en mémoire) et nous avions même demandé à PestPatrol si l'analyse analysait réellement quelque chose tant sa vitesse est phénoménale.

### Notation : formule de calcul pour obtenir une notation /10

Ces mesures sont prises en compte dans le comparatif final.
La note est attribuée au différentiel entre la plus haute charge CPU et la plus faible et est calculée par
A=charge mesurée
B=charge la plus basse
C=charge la plus haute
((A-B)/(C-B)*10)
L'utilitaire chargeant le moins le processeur obtient 10, celui le chargeant le plus obtient 0

### Notation : prise en compte dans la note finale

La mesure de la charge processeur d'un processus, lors d'un scan total (réglage maximum et application sur l'intégralité des objets) n'est pas très importante en terme de sécurité. C'est beaucoup plus un élément de confort et d'usage réaliste du produit. Le résultat de cette mesure influe donc peu sur le résultat final et est affecté d'un coefficient 1.

| Utilisation du processeur (%) | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| % CPU utilisé (moyenne) | 70 | 50 | 50 | 30 | 45 | 2 | 55 | 100 | 40 | 75 | 80 | 50 |

*Figure 9 – Tableau - Ressources processeur utilisées*

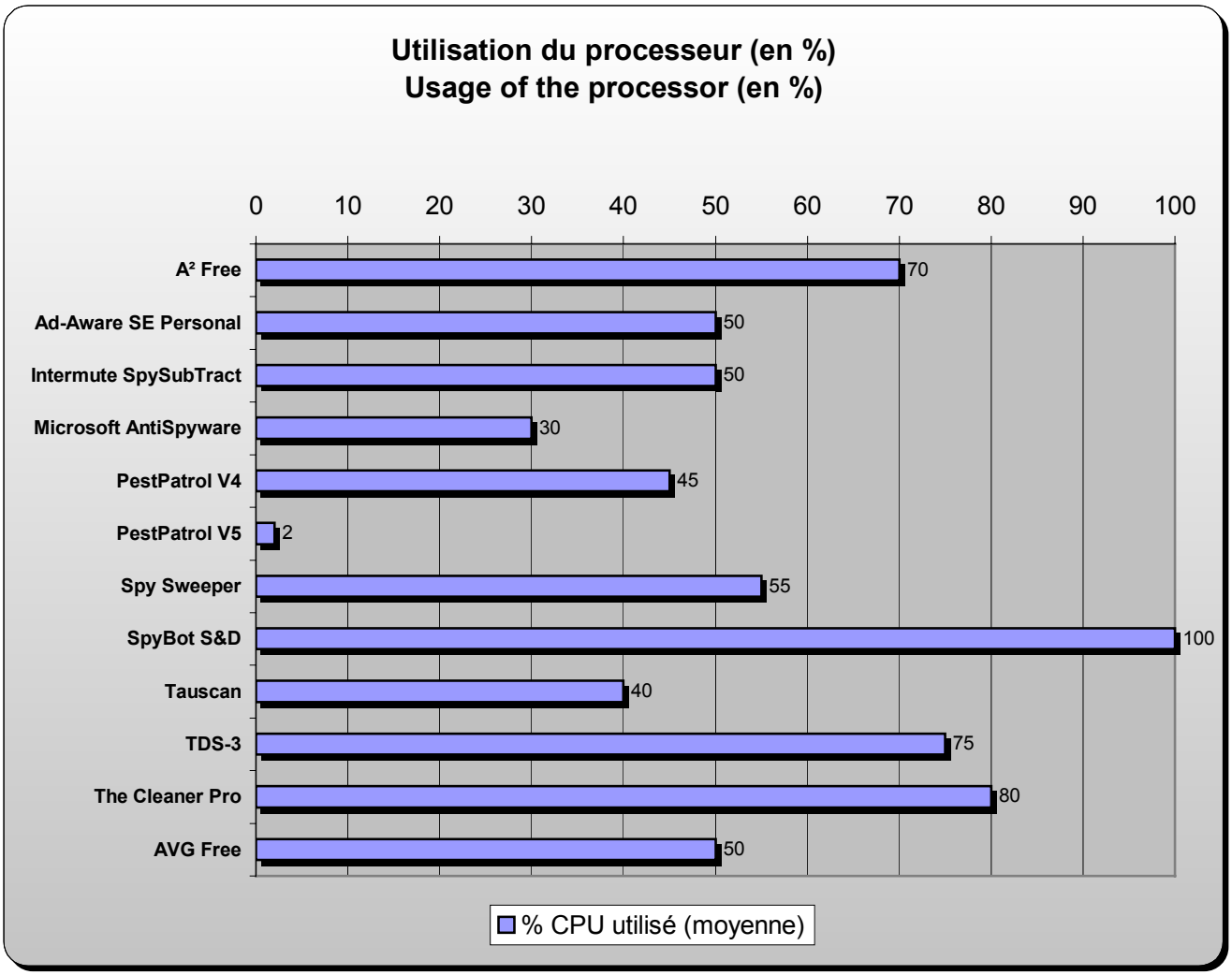


*Figure 10 – Graphique - Ressources processeur utilisées*

Sur les graphiques suivants, les échelles de temps (axes horizontaux) et de charge processeur (axes verticaux) sont strictement identiques. La lecture des courbes est directement comparative – elles peuvent être superposées.

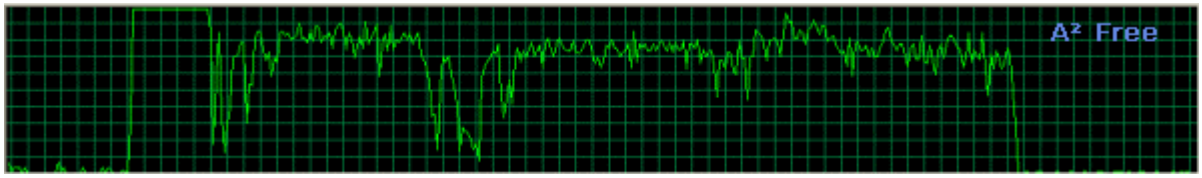


*Figure 11 – Courbe de charge et de durée – A² Free*

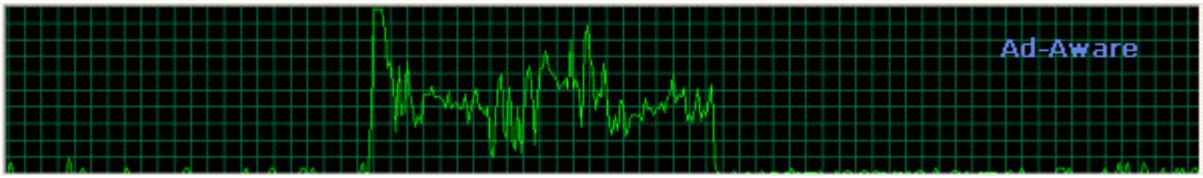


*Figure 12 – Courbe de charge et de durée – Ad-aware*

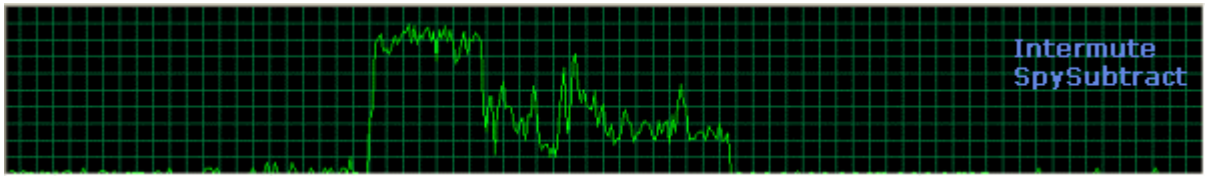


*Figure 13 – Courbe de charge et de durée – Intermute SpySubtract*

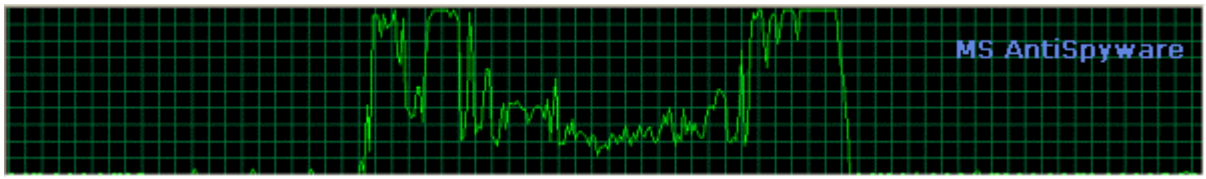


*Figure 14 – Courbe de charge et de durée – Microsoft AntiSpyware*

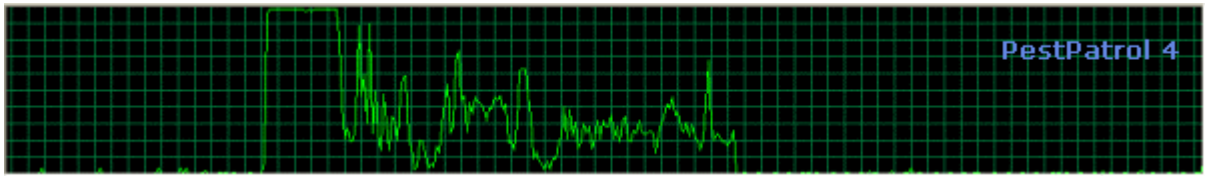


*Figure 15 – Courbe de charge et de durée – PestPatrol 4*

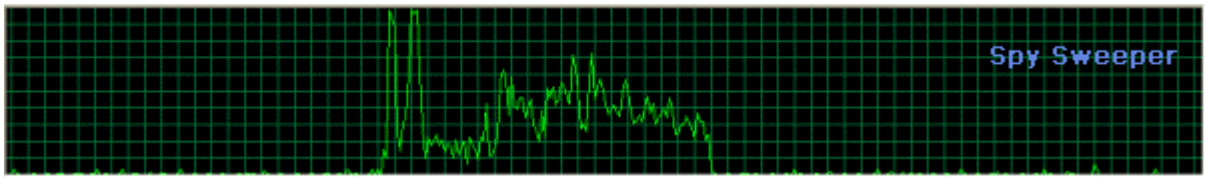


*Figure 16 – Courbe de charge et de durée – Spy Sweeper*

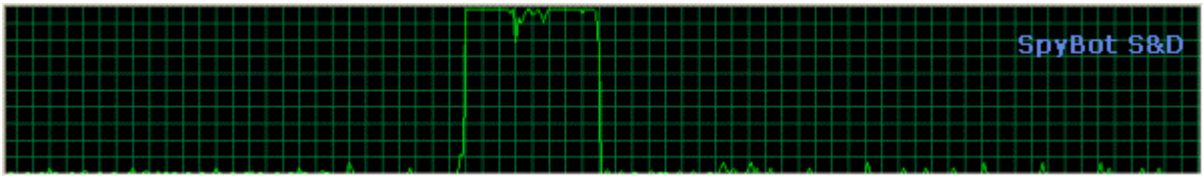


*Figure 17 – Courbe de charge et de durée – SpyBot Search and Destroy*

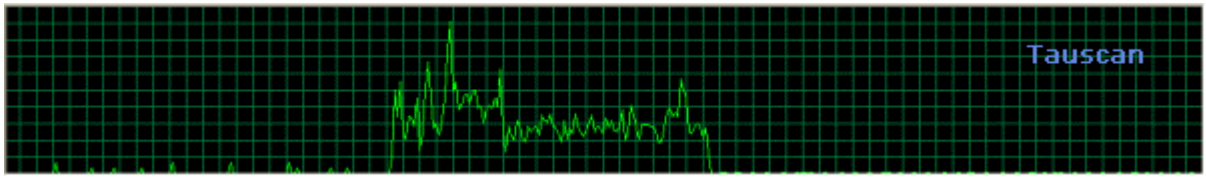


*Figure 18 – Courbe de charge et de durée – Tauscan*

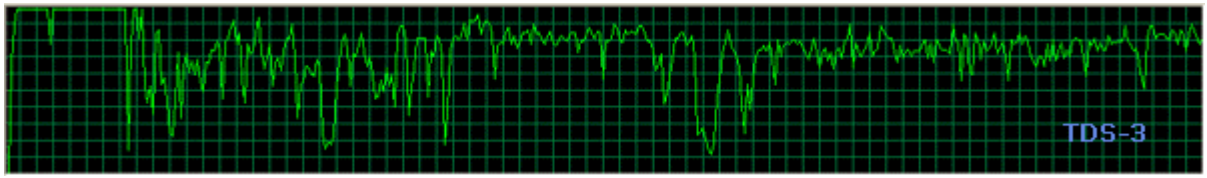


*Figure 19 – Courbe de charge et de durée – TDS-3*

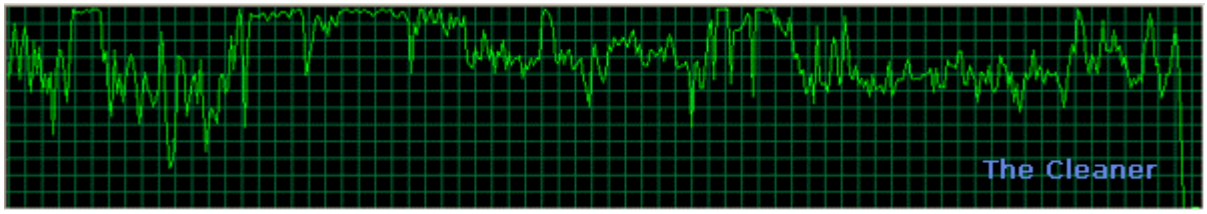


*Figure 20 – Courbe de charge et de durée – The Cleaner*

## *Réactivité « On access » - Parasites trouvés*

### But de la mesure

La fonction « On access » est la plus importante des outils de sécurisation « classiques » (antivirus [52] et anti-trojans [51]) et rapproche ces outils de ceux dit de « contrôle d'intégrité », sans en avoir les caractéristiques de prévention et de temps réel pur [27]. Les fonctions « on access » permettent d'obtenir une réaction immédiate d'un utilitaire de sécurité dès l'accès à un objet parasité, même s'il s'agit de simplement le « regarder » sans l'exécuter. Ainsi, le simple fait de se promener sur son disque avec l'explorateur de Windows et de faire un clic droit (bouton droit de la souris) sur un objet parasité, ou de passer dessus avec les flèches de déplacement, doit déclencher les foudres des utilitaires de sécurité bien faits. Les fonctions « On access » ne sont jamais testées lors des tests comparatifs classiques à cause de la difficulté et du temps nécessaire à mettre ces tests en œuvre et les conduire.

### Mesure

Cette mesure s'est faite en installant Kazaa sur une machine sur laquelle les utilitaires à tester sont préalablement installés.

Cette mesure, la plus importante, s'est révélée être un casse-tête. L'information fournie par les utilitaires est complètement différente de l'un à l'autre et n'est pas directement comparable. En sus, elle est parasitée par l'inflation « commerciale » des nombres. Certains affichent, avec intelligence, la découverte des parasites précis et bien nommés, même si cela recouvre des centaines de fichiers et clés de registre. D'autres explosent ces nombres en comptant, non pas les parasites, mais les moindres objets appartenant aux parasites et les moindres choses tournant autour de ces parasites. Ainsi, lorsque nous avons vu les chiffres annoncés par Intermute SpySubTract, la première réaction a été de dire : « Centaines de faux positifs pour acheter leur produit – Hop ! direction l'anti-logithèque avec tous les interdits et faux utilitaires de sécurité ». Il a fallu regarder les objets désignés pour comprendre que, pour Intermute, la moindre icône en .gif ou le moindre fichier en .txt, à partir du moment où il est dans le répertoire d'un parasite, est compté comme un parasite ! C'est stupide !

Il nous a fallu beaucoup de temps pour réduire les « trouvailles » des uns et des autres à un corpus exhaustif de parasites (Gator [3] = 1 parasite et non pas 700 parasites avec 36 noms comme se plaisent à le déclarer certains utilitaires !).

En l'occurrence, une installation de Kazaa se solde par l'implantation de 13 parasites dont 11 doivent être décelés durant l'installation si l'utilitaire dispose d'un module « temps réel » (et si celui-ci est bien fait).

Les modules temps réel fonctionnent avec un sous-ensemble de la base de signatures. Ce sous-ensemble, qui permet de ne travailler que sur un spectre réduit de parasites afin de ne pas prendre trop de temps calcul, est choisi avec soin par les responsables sécurité des éditeurs d'utilitaires et peut signer la qualité ou l'insignifiance d'un utilitaire.

L'installation de Kazaa a donc déclenché diverses réactions de la part de certains outils dotés d'un module « On access » temps réel [27] ou pseudo temps-réel [27]. Les autres n'ont rien vu.

- **A² Free** ne dispose pas de module temps réel [27]. On trouve cette fonctionnalité dans A² Personal (payant).
- **Ad-aware SE Personal** ne dispose pas de cette fonctionnalité. Elle existe dans la version payante.
- **PestPatrol v5 Corporate** est un scanner temps différé (« on demand") administrable à distance et déployable sur un réseau.
- **Tauscan** : il n'a pas été possible d'obtenir le moindre résultat de Tauscan, un excellent outil normalement, probablement à cause d'une erreur de manipulation indéterminée.
- **TDS-3** ne dispose pas de module temps réel [27]. On nous promet un TDS-4 depuis plus de 2 ans.
- **AVG** n'a rien vu malgré son module temps réel [27]. C'est un antivirus [52] pur et pas un anti-trojans [51]. Il ne verra d'ailleurs rien, non plus, durant l'analyse en temps différé (scan « on demand »).

### Notation : formule de calcul pour obtenir une notation /10

Ces mesures sont prises en compte dans le comparatif final.
La note est attribuée au ratio entre parasites trouvés et parasites à trouver. Il y avait 11 parasites à trouver « On access ».

Parasites trouvés/Parasites à trouver*10
Celui qui ne trouve rien obtient 0, celui qui les trouve tous obtient 10.

## Notation : prise en compte dans la note finale

La mesure de réactivité « On access » des utilitaires de type scanners (antivirus [52] et anti-trojans [51]) est la plus importante de toutes. Le résultat de cette mesure influe considérablement sur le résultat final et est affecté du coefficient de pondération le plus élevé : 10.

## Les parasites signalés « On access »

| | A² Free | Ad-aware se Personal | Intermute SpySubtract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner | Avg | Windows SP2 | ProcessGuard |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Lancement de l'installation de Kazaa (Kazaa_setup.exe) | | | ✓ | | | | | | | | | | ✓ | ✓ |
| P2Psetup.exe (Web - P2P Installer - Trojan Downloader) | | | ✓ | ✓ | | | | ✓ | | | | | | ✓ |
| ActiveX 1D6711C8-7154-40BB-3DEA45B69CBF P2P Networking | | | ✓ | | ✓ | | | ✓ | | | ✓ | | | ✓ |
| Asm.exe | | | ✓ | | | | | | | | | | | ✓ |
| Kazaa | | | | | | | ✓ | | | | | | | |
| Kazaa Adware Bundler (Kazaa300_en.exe) | | | | ✓ | | | | ✓ | | | ✓ | | | ✓ |
| Xmltest.exe | | | | | | | | | | | | | | ✓ |
| Fsg.exe | | | | | | | | | | | | | | ✓ |
| Setup.exe | | | | | | | | | | | | | | ✓ |
| Fsg_4203.exe (GAIN Network [2] Trickler) | | | | ✓ | | | ✓ | ✓ | | | | | | ✓ |
| Amd4005.exe | | | ✓ | | | | | | | | | | | ✓ |
| Point Manager.exe | | | ✓ | | ✓ | | ✓ | ✓ | | | ✓ | | | ✓ |
| MySetp.exe (MyWay ToolBar - MyWay Search Bar) | | | | ✓ | | | | | | | ✓ | | | ✓ |
| Pdpsetup5105.exe | | | | | | | | | | | | | | ✓ |
| BullGuardOptIn (bulldownload.exe) | | | | | | | | ✓ | | | ✓ | | | ✓ |
| CMESys.exe (CMEII - CME II Client Application) | | | | | ✓ | | | ✓ | | | ✓ | | | ✓ |
| gmt.exe (Gator [3] / GAIN Network [2] / Claria) | | | | ✓ | ✓ | | | | | | | | | ✓ |
| 0494D0D9-F8E0-41ad92A3-14154ECE70AC 0494D0D1-F8E0-41ad92A3-14154ECE70AC Bho MyWay SpeedBar | | | | | | | | ✓ | | | | | | |
| Totaux parasites trouvés « On access » | 0 | 0 | 6 | 5 | 4 | 0 | 3 | 8 | 0 | 0 | 6 | 0 | 1 | 16 |

*Figure 21 – Récapitulation des parasites signalés « On access »*

Selon les conventions de nommage ou les objets qui servent à identifier « on access » un parasite, ce sont 11 parasites différents que les utilitaires devraient signaler, d'une manière ou d'une autre, à ce moment-là car ils sont installés ET lancés par le téléchargeur [47] (downloader [47]) de Kazaa.

Win SP2 est là pour mémoire. A partir du moment où on autorise Kazaa_setup.exe à s'exécuter, le SP2 ne sert plus à rien – ce n'est d'ailleurs pas sa finalité.

ProcessGuard [16] est le plus rapide de tous en vitesse de réaction et voit la totalité des tâches activées. Il est cité en référence ici mais son activité n'est pas du tout de même nature que celles des anti-trojans [51] et des antivirus [52] et il ne fait pas partie du comparatif.

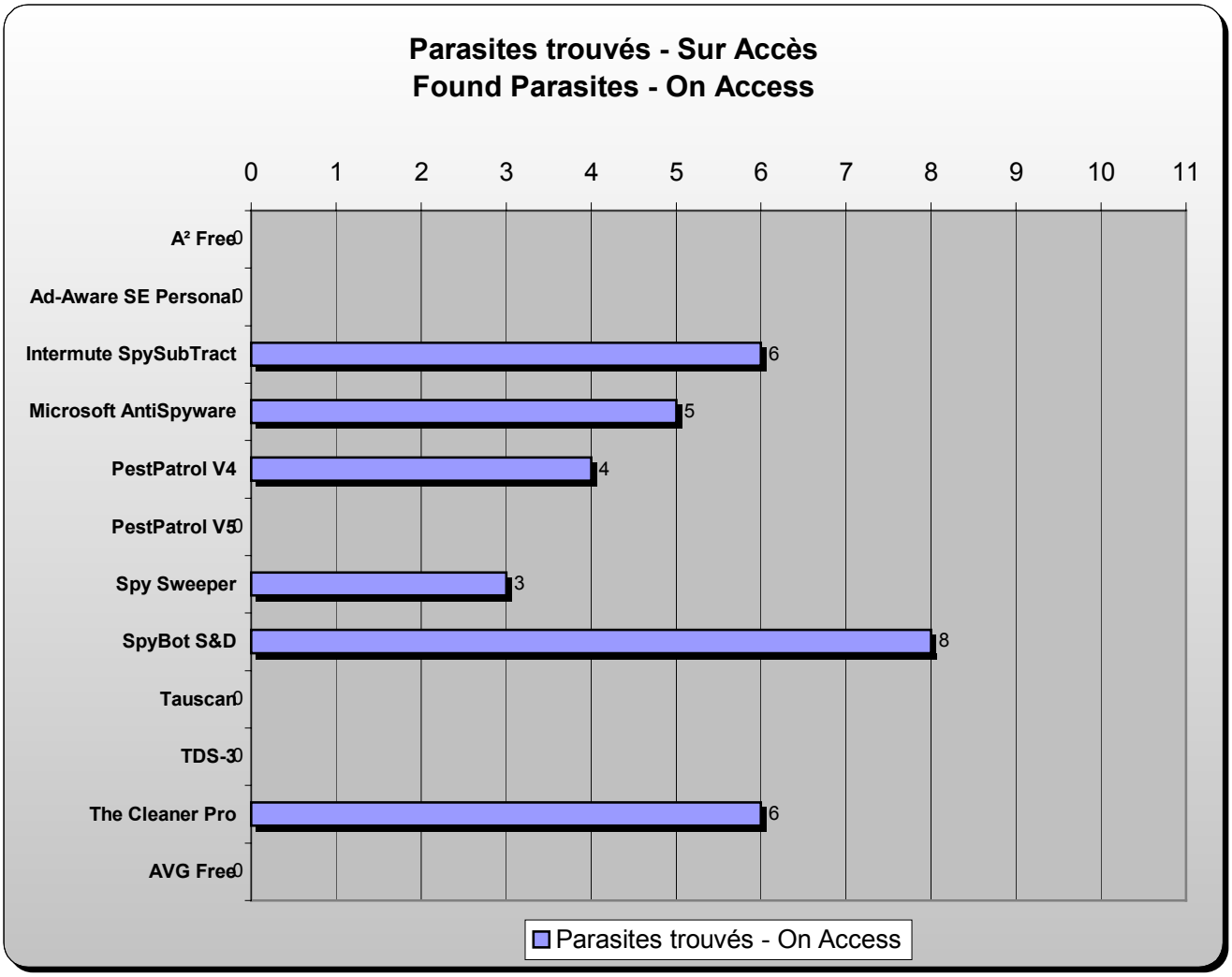


*Figure 22 – Parasites trouvés par les fonctions "On access"*

## *Réactivité « On boot » - Parasites trouvés*

### But de la mesure

Nous avons voulu savoir comment réagissent les utilitaires de sécurité au démarrage de Windows (On Boot) et alors que les parasites sont déjà installés. Nous nous attendions à ce que les réactions au démarrage de Windows soient strictement les mêmes que celles « On Access », avec utilisation du même module « On Access ». Et bien non ! Pas du tout ! En réalité, nous avions de sérieux doutes compte tenu du moment très tardif où sont lancés ces utilitaires dans la séquence de démarrage de Windows.

### Mesure

En démarrant / redémarrant Windows, certains utilitaires de sécurité surveillent ce qui se lance mais, à priori, ce n'est pas leur tasse de thé.

Il y a 11 parasites à découvrir. Voir le tableau récapitulatif.

### Notation : formule de calcul pour obtenir une notation /10

Ces mesures sont prises en compte dans le comparatif final.
La note est attribuée au ratio entre parasites trouvés et parasites à trouver.
Parasites trouvés/Parasites à trouver*10
Celui qui ne trouve rien obtient 0, celui qui les trouve tous obtient 10.

### Notation : prise en compte dans la note finale

La mesure de réactivité « On Boot » des utilitaires de type scanners (antivirus [52] et anti-trojans [51]) est aussi importante que la mesure « On access ».. Le résultat de cette mesure influe considérablement sur le résultat final et est affecté d'un coefficient 10.

### Les parasites signalés « On Boot »

| | A² Free | Ad-aware se Personal | Intermute SpySubtract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner | Avg | Windows SP2 | ProcessGuard |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P2P Networking.exe (Altnet) | | | ½(1) | | ✓ | | ½(2) | | | | | | | |
| TOPicks (Points Manager) | | | ½(1) | | ✓ | | | | | | | | | |
| Gator(3)/GAIN Network(2)/Claria | | | | | ✓ | | ½(2) | | | | ✓ | | | |
| MySearchBar | | | | | | | | | | | ✓ | | | |
| Totaux parasites trouvés « On boot » | | | 1 | | 3 | | 1 | | | | 2 | | | |

*Figure 23 – Récapitulatif : Parasites signalés lors d'un démarrage du système*

½(1)=Venus de Intermute SpySubtract
SpySubTract dispose d'un module que l'on a classé ici, Venus, car on ne sait pas où le classer. Il se situe entre les modules temps réel, lancés au démarrage, « On boot », et les scanners « On demand ».
Ce module est bien lancé au démarrage mais il ne détecte pas immédiatement les parasites qui se lancent au démarrage, en même temps que lui. Ce n'est pas du tout un module temps réel [27]. On ne peut même pas dire qu'il s'agisse de pseudo temps réel [27], comme c'est le cas pour Spybot S&D, beaucoup plus réactif. Il effectue,

en réalité, une analyse en arrière-plan qui boucle indéfiniment, en priorité basse, sur un sous-ensemble de la base de signatures, et affiche les quelques parasites éventuellement trouvés. On peut alors, soit ignorer ses avertissements et poursuivre, soit lancer une analyse « normale » pour pouvoir accéder aux fonctions d'éradication. Si l'on clique sur « Don't scan » (ignorer), Venus recommence son analyse et ré-affiche ses résultats, indéfiniment, à moins de désactiver ce module.

½ [(2)]=Spy Sweeper

Spy Sweeper dispose d'un module qui se lance au démarrage et détecte assez rapidement quelques parasites en mémoire mais il a fallu complètement désactiver tous les autres processus de sécurité se lançant au démarrage, pour le laisser démarrer tout seul puis, même, désactiver une partie des parasites eux-mêmes avec Spy Sweeper (AltnetPointsManager, CMESys et GMT). Nous avons pu alors démarrer, de temps en temps seulement, sans problème pour Spy Sweeper. Dans tous les autres cas, Spy Sweeper se lance, affiche une fenêtre déclarant que 2 paramètres entrent en conflit avec quelque chose (sans doute un parasite) et attend une action de l'utilisateur tandis que le démarrage de Windows et des parasites lancés au démarrage se poursuit normalement. Cette intermittence est un problème.

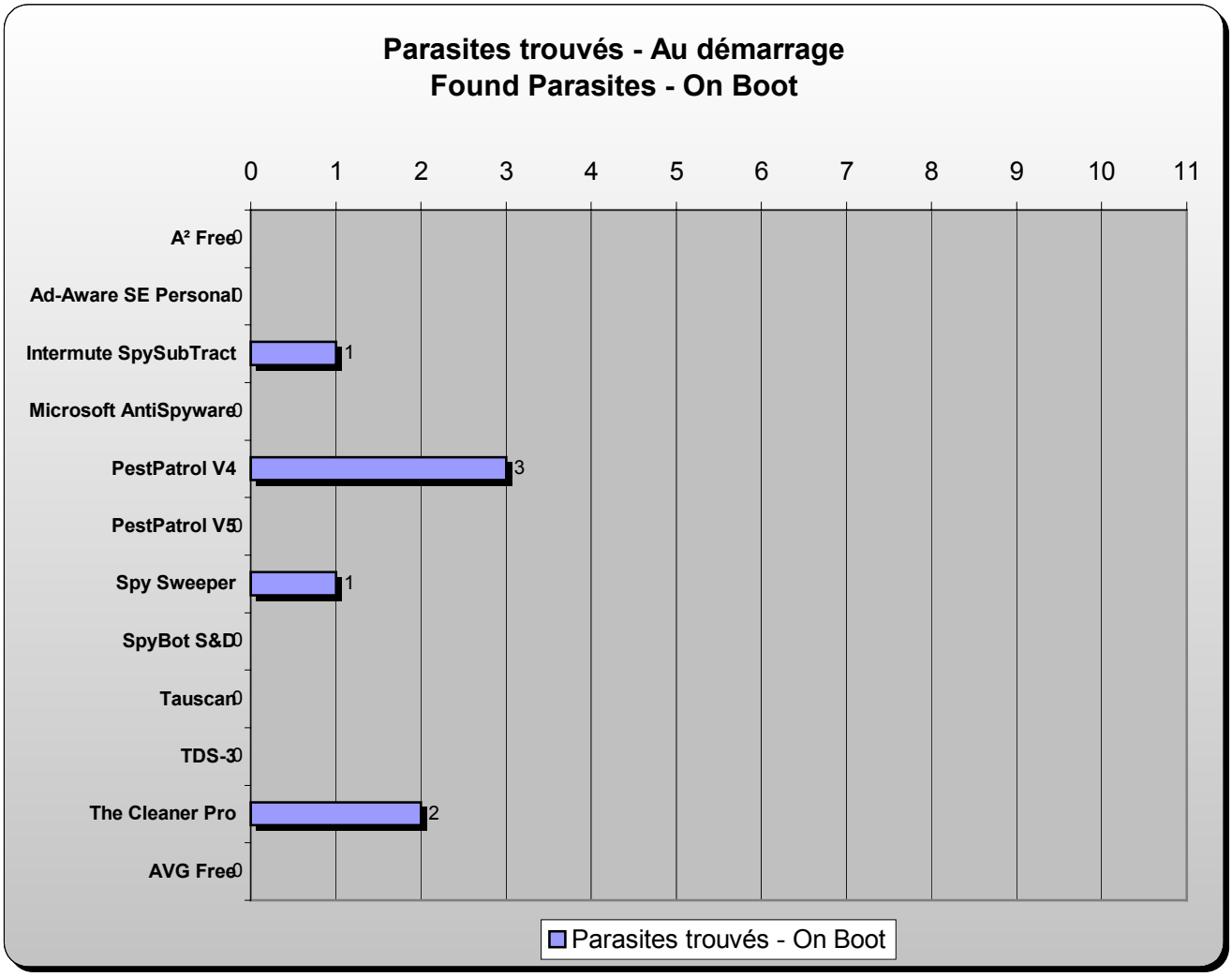


*Figure 24 – Comparatif : Parasites signalés lors d'un démarrage du système*

## *Analyse « On demand » - Parasites trouvés*

### But de la mesure

Il s'agit du test classique des anti-trojans [(51)] et des antivirus [(52)]. Moins significatif que les tests « On access » et « On boot », ce test permet de sonder le spectre de la base de signatures.

### Mesure

Réglages des analyseurs au maximum et demande d'analyse de l'intégralité des objets de la machine de tests. Le dépouillement des résultats fut un cauchemar tant les nommages des détections sont fantaisistes.

Il y a 13 parasites à découvrir. Voir le tableau récapitulatif ci-dessous.

### Notation : formule de calcul pour obtenir une notation /10

Cette mesure est prise en compte dans le comparatif final.
La note est attribuée au ratio entre parasites trouvés et parasites à trouver.
Parasites trouvés/Parasites à trouver*10
Celui qui ne trouve rien obtient 0, celui qui les trouve tous obtient 10.

### Notation : prise en compte dans la note finale

Le résultat du sondage de l'amplitude de la base de signatures des utilitaires de type scanners (antivirus [(52)] et anti-trojans [(51)]) est important mais moins, tout de même, que les modules « On access » et « On boot ». Le résultat de cette mesure influe de manière importante sur le résultat final et est affectée d'un coefficient 6.

## Les parasites signalés « On demand »

| | Déclaration de Kazaa | A² Free | Ad-aware se Personal | Intermute SpySubtract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner | Avg |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Kazaa | ✓ | | | | ✓ | ✓ | ✓ | | | | | | |
| Altnet TopSearch<br>Adware.Topsearch<br>icône Or – gestion DRM<br>http://www.altnet.com/faq/ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | |
| Altnet My Search Tool Bar<br>MyWay.MyBar<br>MyWay.SpeedBar<br>My-Way Speedbar<br>My Search Bar | ✓ | ✓ | | ✓ | ✓<br>☹ (7) | ✓ (8) | ✓ (8) | ✓ | ✓ | | ✓ | ✓ | |
| Altnet Joltid P2P Networking<br>Zombi Altnet caché dans FastTrack<br>Brillant Digital<br>Altnet Peer Points Components | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | |
| BullGuard P2P<br>BullGuard Popup Add | ✓ | | | ✓ | | | | ✓ | | | | | |
| Cydoor (1) | ✓ | | | | ✓ | | | ✓ | ✓ | | | | |
| GAIN Network (2)<br>Gain / Gator / Claria<br>Claria | ✓ | ✓ | ✓ | ✓ | ✓ (6)<br>☹(6) | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | |
| InstallFinder | ✓ | | | | ✓ | | | | | | | | |
| Grokster ??? | | | | ☹(1) | ☹(1) | | ☹(1) | | | | | | |
| Twain Tech | | | | | ✓ | ✓ | ✓ | | | | | | |
| DownloadWare ??? | | | | | ☹(2) | | | | | | | | |
| AdDestroyer<br>Adware.AdDestroyer [Norton]<br>VirtualBouncer<br>(Spyware Labs) | | | | | | ✓ | ✓ | | | | | | |
| FlashGet ??? | | | | | | ✓ (4) | | | | | | | |
| SearchCentrix | | | | | | ☹(5) | ☹(5) | | | | | | |
| CommonName | | | | | | | | ☹(3) | ☹(3) | | | | |
| Gain Gator PrecisionTime | | | | | | | ✓ | | | | | | |
| Gain Gator DateManager | | | | | | | ✓ | | | | | | |
| | | 2 | 2 | 6 | 9 | 9 | 9 | 6 | 6 | 0 | 5 | 2 | 0 |

*Figure 25 – Récapitulatif : Parasites signalés lors d'une analyse « A la demande »*

☹ Voir le chapitre « Analyses On demand - Erreurs et Faux positifs ».

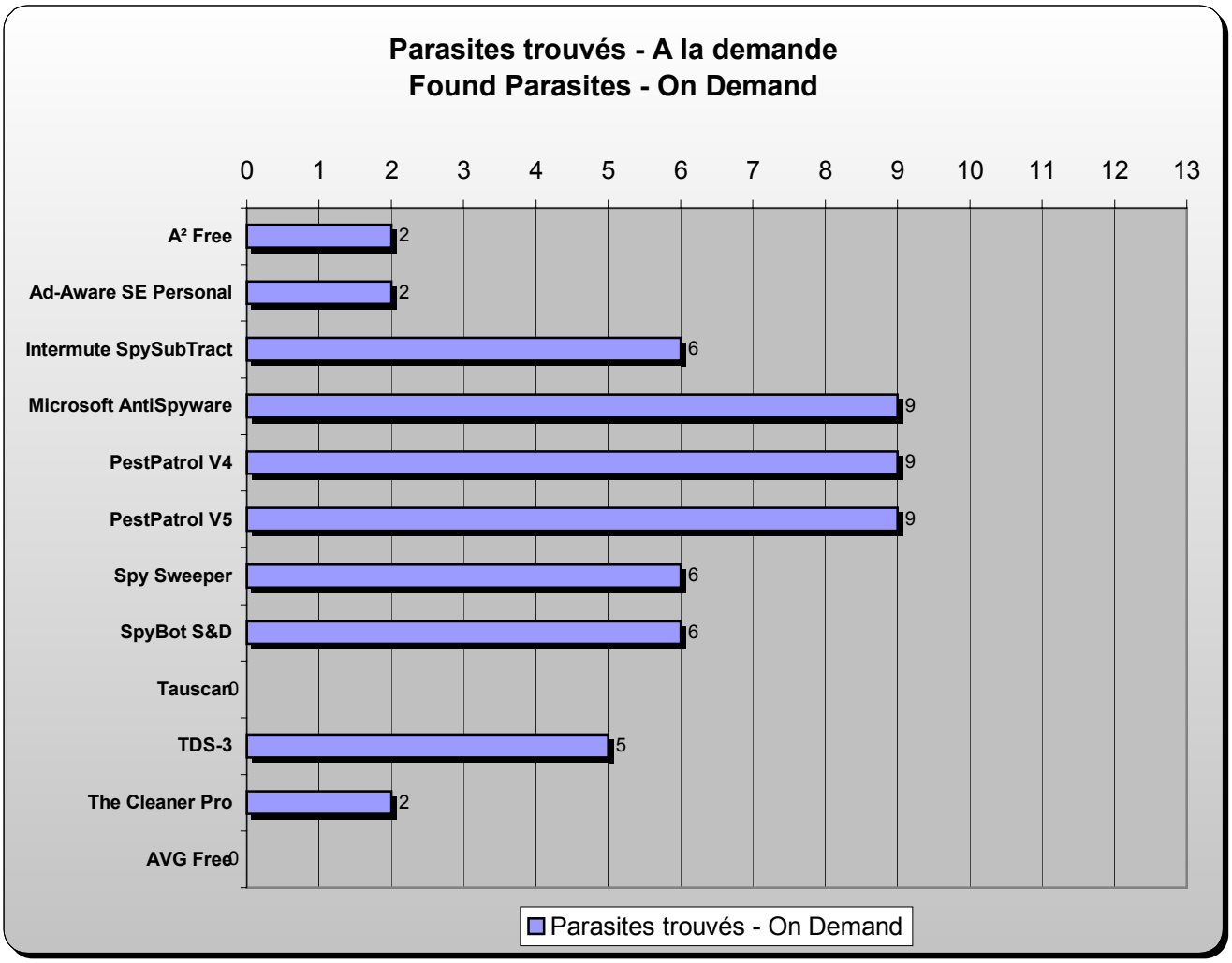


*Figure 26 – Comparatif : Parasites signalés lors d'une analyse « A la demande »*

## *Analyse « On demand » - Erreurs et faux positifs*

### But de la mesure

Vérifier que les utilitaires ne risquent pas de provoquer l'élimination d'objets légitimes. Commentaires, erreurs et faux positifs.

### Mesure

**☹(1) = Grokster**

Cette détection est un « faux positif » (une erreur). Grokster n'est absolument pas installé sur la machine de test. Le signalement de Grokster par plusieurs anti-trojans [(51)] provient du fait que TOPicks était, historiquement, livré en bundle avec Grockster et que la procédure d'installation de TOPicks contient quelques entrées qui portent encore le nom de Grokster ou qui font penser à Grokster, preuve que certains algorithmes travaillent au petit bonheur la chance, sans corréler les découvertes d'empreintes. Illustration ci-dessous.

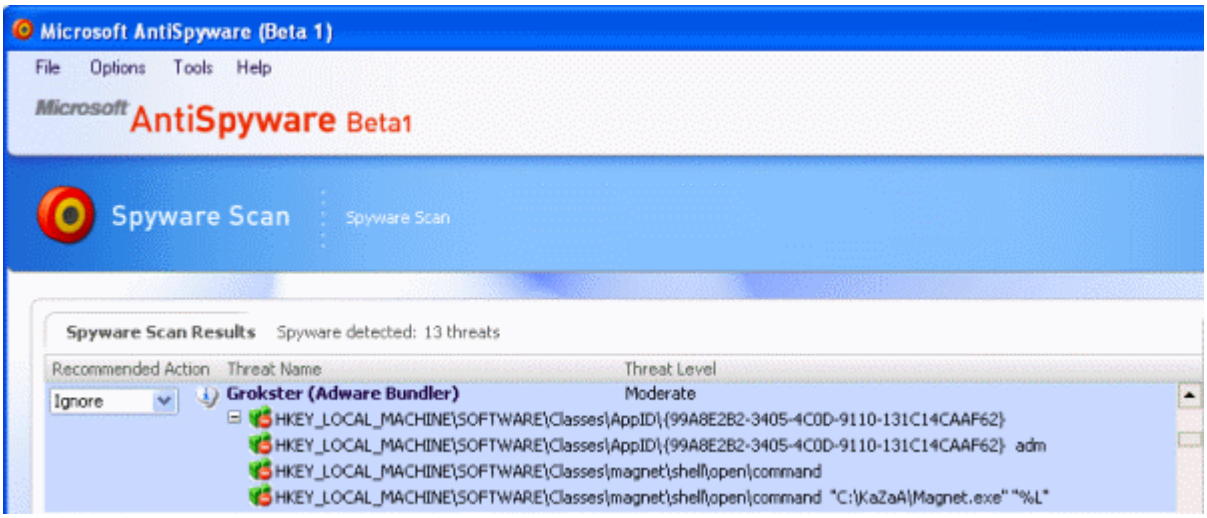


*Figure 27 – Microsoft AntiSpyware : Faux nommage d'un parasite*

**☹(2)=DownloadWare**

Cette détection est une faute de Microsoft AntiSpyware: Non seulement DownloadWare n'est absolument pas installé sur la machine de test mais, en plus, les 12 CLSID
0494d0da-f8e0-41ad-92a3-14154ece70ac
0494d0dc-f8e0-41ad-92a3-14154ece70ac
trouvées par Microsoft AntiSpyware (bêta 1) n'existent pas du tout dans la base de registre (recherches avec RegEdit).

- Ad-aware les classe à My Search ou à MyWay.SpeedBar ou à My-Way Speedbar, selon recherches Google.
- PestPatrol les classe à DownloadWare. Pourraient être retirées, depuis, de la base de signatures de PestPatrol ?
- SpyBot les classe à SideStep.MyWay.MyBar

Nous pouvons admettre, à la rigueur, une erreur de nommage lorsque des empreintes identiques apparaissent dans plusieurs parasites. Le cas de Grokster, vu ci-dessus, illustre la difficulté à corréler de nombreuses empreintes « floues » pour en sortir un nom de parasite certain. Nous ne pouvons admettre qu'un algorithme puisse prétendre trouver des données qui n'existent pas car cela témoigne d'un bug dans l'algorithme lui-même. Ce n'est plus une erreur, c'est une faute. Illustration ci-dessous.

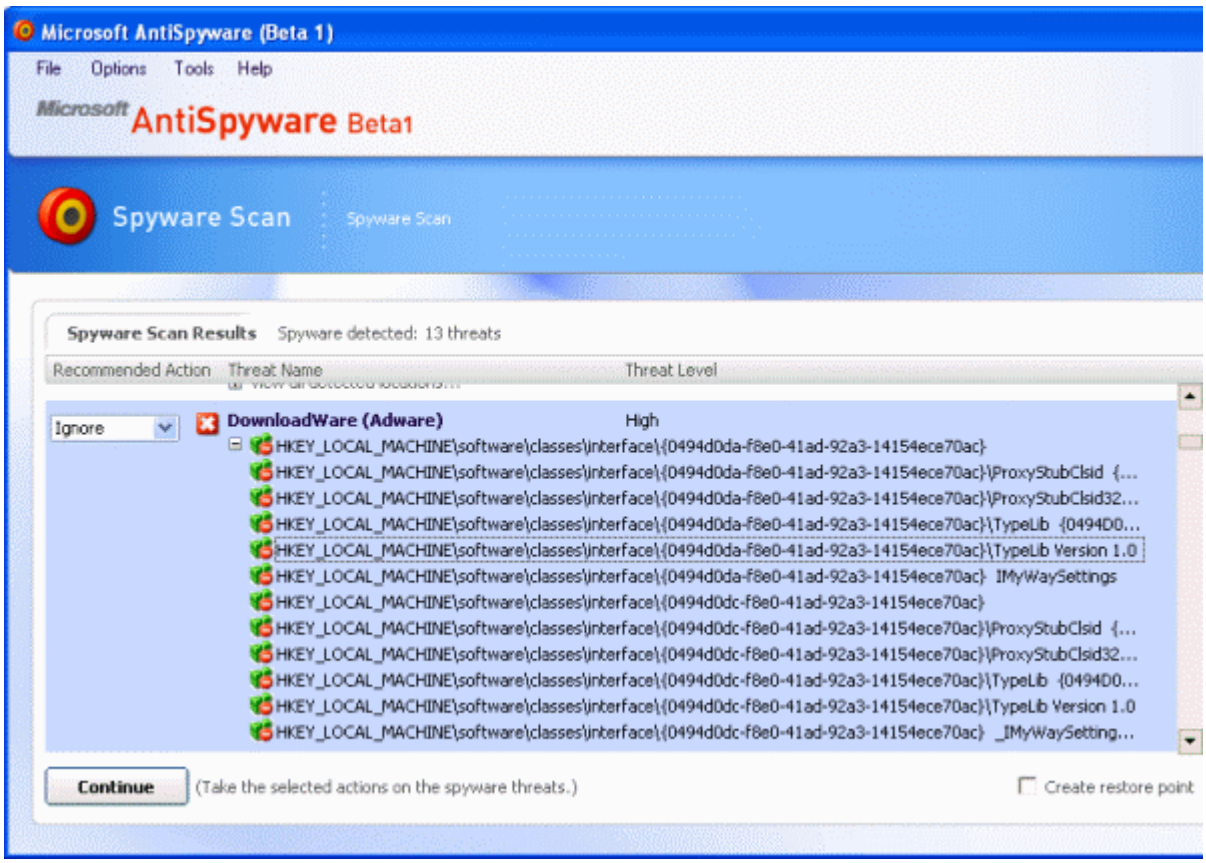


*Figure 28 – Microsoft AntiSpyware : Signale des clés et un parasite qui n'existent pas*

### ☹[3]= CommonName

SpyBot détecte CommonName.
Cette détection est un « faux positif » (une erreur).
SpyBot voit un répertoire dont le nom est c:\windows\Temp\Adware et, bien que ce répertoire soit complètement vide, il déclare la présence du parasite « CommonName » ce qui signifie qu'il s'intéresse à l'enveloppe des choses (aux apparences) et non à leur contenu. C'est l'une des caractéristiques de SpyBot qui n'analyse strictement aucun contenu, d'où sa vitesse « magique ». A ce petit jeu, il devrait effectuer plusieurs corrélations entre plusieurs empreintes pour arriver à déterminer la présence ou non d'un parasite. Ici, la présence d'un répertoire, en tout et pour tout, est complètement insignifiante et aucun objet ne permet de déclarer l'installation de ce parasite. Rappelons que SpyBot ne cherche pas et ne déclare pas la présence d'un parasite mais, simplement, son installation (son activation).

### [4]=FlashGet

PestPatrol se base sur la présence d'un unique fichier certifié FlashGet par hashcode MD5 et par son système de chiffre clé (PVT). Le fichier incriminé est à
C:\windows\cdmxtras\uninst.exe
Une recherche Google sur cdmxtras ne donne rien. Le nom du fichier fait penser à un programme de désinstallation mais ce peut être un leurre. Il faudrait en lancer l'exécution ou le désassembler pour s'en assurer mais l'exécuter pourrait compromettre la machine de test et le désassemblage n'est pas prévu dans ce test déjà assez long à réaliser. Nous décidons de faire confiance au hashcode MD5 de PestPatrol qui dispose de la plus vaste bibliothèque au monde de hashcodes (plusieurs centaines de milliers de fichiers sont ainsi signés).
Rappel : La machine de test est une machine neuve (« propre »). Il ne s'agit pas d'une machine décontaminée sur laquelle il resterait des traces de désinstallations ou de décontaminations incomplètes.

### ☹[5]=SearchCentrix

PestPatrol v4 et v5 détectent SearchCentrix
Cette détection est un « faux positif » (une erreur).
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{3646C2BD-3554-49CA-8125-44DEEFB881DE}
Il s'agit d'une clé de MyWay.MyBar

**(6)=Gain/Claria**
Microsoft AntiSpyware classe une partie de ce parasite à GAIN et une autre partie à Claria. Il s'agit de la même chose.
Rappelons que GAIN est le nom du réseau de la société Claria (ex Société Gator (3)). Ses parasites sont
GAIN Network (2)
OfferCompagnion
eWallet
PrecisionTime
Date Manager
Voir http://assiste.free.fr/p/internet_attaquants/gator.php

**(7)=My Search Bar**
Microsoft AntiSpyware classe une partie de ce parasite à MyWay Search Bar et une autre à My Search Bar, ce qui est une erreur.

**(8)=MyWay\MyBar**
PestPatrol détecte et éradique ce parasite qu'il classe avec Kazaa ce qui pourrait être amélioré en terme de lisibilité des journaux d'analyse.

## Notation : formule de calcul pour les erreurs et faux positifs

Cette mesure est prise en compte dans le comparatif final.
Le nombre d'erreurs prises en compte est plafonné à 10.
La note obtenue est de 10 pour un utilitaire ne commettant aucune faute, 9 si une faute, 8 si 2 fautes etc. … 0 si 10 fautes ou plus.
Exception : si un utilitaire trouve 0 parasite lors des 3 tests « On Acces » + « On Boot » + « On demand »,il est considéré ne fonctionnant pas. Dans ces conditions, comme il ne trouve aucun faux positif, il pourrait obtenir la meilleure note de cette catégorie donc un test est fait : si nombre de parasites trouvés = 0, note de faux positif = 0 (c'est le cas pour Tauscan dans ce comparatif).

## Notation : prise en compte dans la note finale

Cette notation est importante et influe sur le résultat final. Elle est coefficientée 3. Autrement dit, chaque faute provoque une pénalité de 3 points et la pénalité maximum est de 30 points.

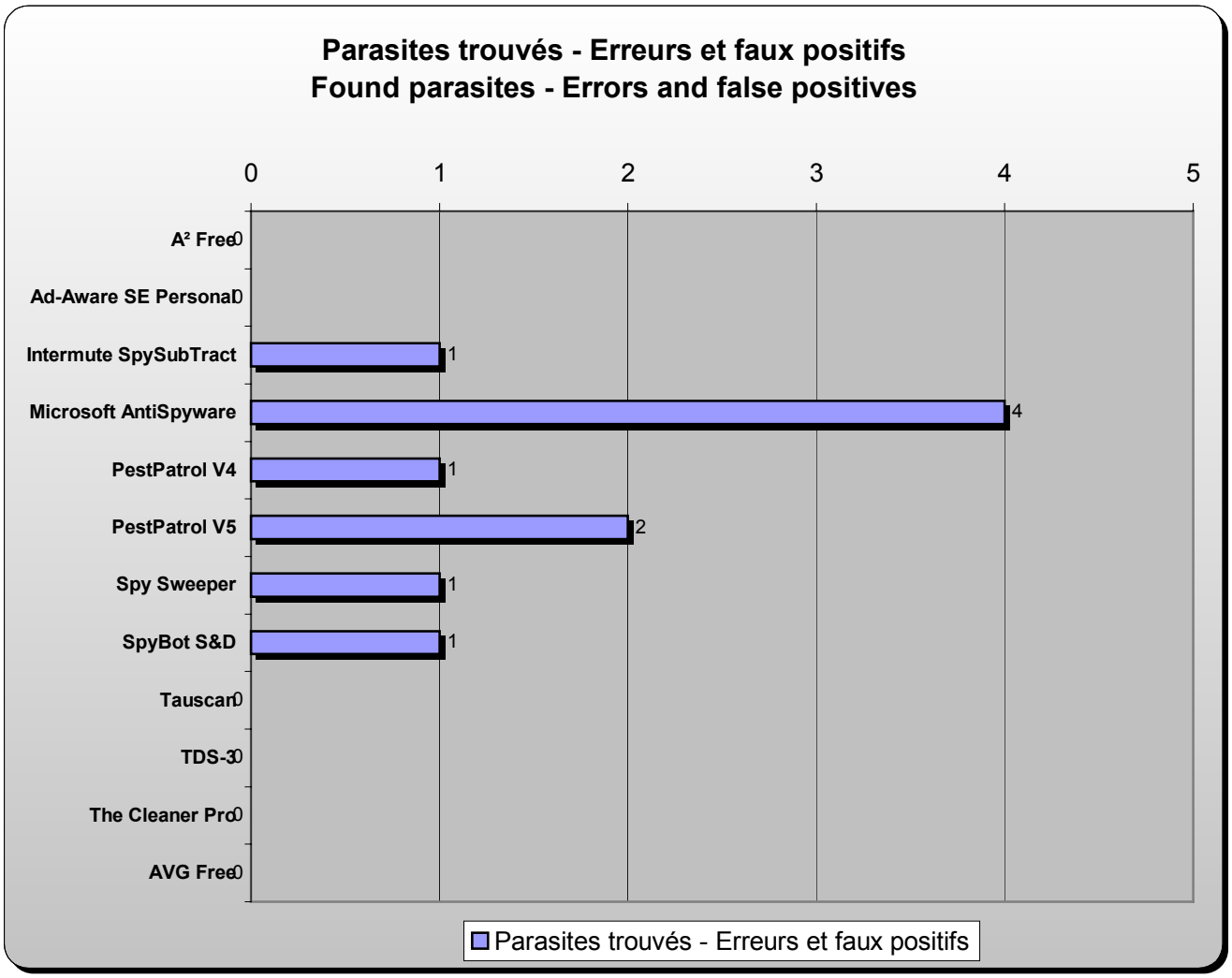


*Figure 29 – Comparatif : Erreurs et faux positifs  lors d'une analyse « A la demande »*

# *ADS [42] – Signalement et gestion*

## But de la mesure

Quels sont les utilitaires de sécurité qui traitent le cas des ADS [42] ?

## Mesure

Durant l'analyse à la demande, les utilitaires ayant développé une recherche des ADS [42] les signalent. Ils ne sont pas nombreux à le faire.

Seuls 2 utilitaires sur tous ceux testés ont signalé les ADS [42] présents. Notons qu'Ad-aware en a vu un de plus que TDS-3.
TDS-3 est le seul à permettre la lecture des contenus et la destruction des ADS [42].

Nota : SpyBot ne touche pas aux ADS [42] mais Patrick Kolla, son auteur, a développé « ADS Locator » qui ne fait que du signalement. Voir la page d'outils de SpyBot([45]).

## Notation : formule de calcul pour obtenir une notation /10

Cette mesure est prise en compte dans le comparatif final.
La note est attribuée, sur 10, de la manière suivante :

- L'utilitaire signale la présence d'ADS [42] : 2 points
- L'utilitaire permet de lire le contenu des ADS [42] : 3 points
- L'utilitaire permet de détruire les ADS [42] : 5 points

## Notation : prise en compte dans la note finale

La gestion des ADS [42] est un peu plus importante actuellement qu'elle ne le fût il y a peu. Des parasites sévères utilisent désormais cette technique qui semble se répandre. Le résultat de cette mesure influe donc légèrement sur le résultat final en étant affecté d'un coefficient 3.

| | A² Free | Ad-aware SE Personal | Intermute SpySubTract | Microsoft AntiSpywaye | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SbyBot S&D | Tauscan | TDS-3 | The Cleaner | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Signale la présence d'ADS | | ✓ | | | | | | | | ✓ | | |
| Lit le contenu des ADS | | | | | | | | | | ✓ | | |
| Détruit les ADS | | | | | | | | | | ✓ | | |

*Figure 30 – Récapitulatif : Gestion des ADS*

# 7. Fréquence des mises à jour

Information reprise des avis publiés librement sur Calendar of Updates [53], ***ASAP***, et sur Mises à jour [54] , ***ASAP***.

Précision toute relative et non officielle.

Certains utilitaires ne sont pas suivis. Mesure hors tableaux de notation.

| Fréquence des mises à jour | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Janvier 2004 | 15 | 9 | n/a | n/a | 7 | | 2 | 1 | 3 | 12 | 9 | 16 |
| Février 2004 | 4 | 12 | n/a | n/a | 4 | | 3 | 3 | 2 | 7 | 32 | 9 |
| Mars 2004 | 9 | 14 | n/a | n/a | 1 | | 7 | 2 | 4 | 5 | 27 | 29 |
| Avril 2004 | 1 | 22 | n/a | n/a | 0 | | 4 | 1 | 4 | 18 | 27 | 24 |
| Mai 2004 | 8 | 8 | n/a | n/a | 3 | | 1 | 4 | 2 | 21 | 25 | 26 |
| Juin 2004 | 8 | 14 | n/a | n/a | 2 | | 3 | 3 | 1 | 18 | 23 | 18 |
| Juillet 2004 | 7 | 10 | n/a | n/a | 3 | | 6 | 2 | 1 | 23 | 29 | 19 |
| Août 2004 | 7 | 4 | n/a | n/a | 4 | | 6 | 4 | 3 | 23 | 22 | 13 |
| Septembre 2004 | 5 | 6 | n/a | n/a | 4 | | 5 | 1 | 3 | 22 | 21 | 22 |
| Octobre 2004 | 4 | 4 | n/a | n/a | 3 | | 4 | 3 | 3 | 20 | 15 | 17 |
| Novembre 2004 | 6 | 1 | n/a | n/a | 5 | | 4 | 2 | 3 | 22 | 13 | 16 |
| Décembre 2004 | 17 | 2 | n/a | n/a | 7 | | 12 | 1 | 2 | 14 | 12 | 24 |
| Janvier 2005 | 9 | 1 | n/a | n/a | 6 | | 1 | 2 | 3 | 12 | 9 | 20 |
| Total | **100** | **107** | | | **49** | | **58** | **29** | **34** | **217** | **264** | **253** |

*Figure 31 – Tableau – Fréquence des mises à jour*

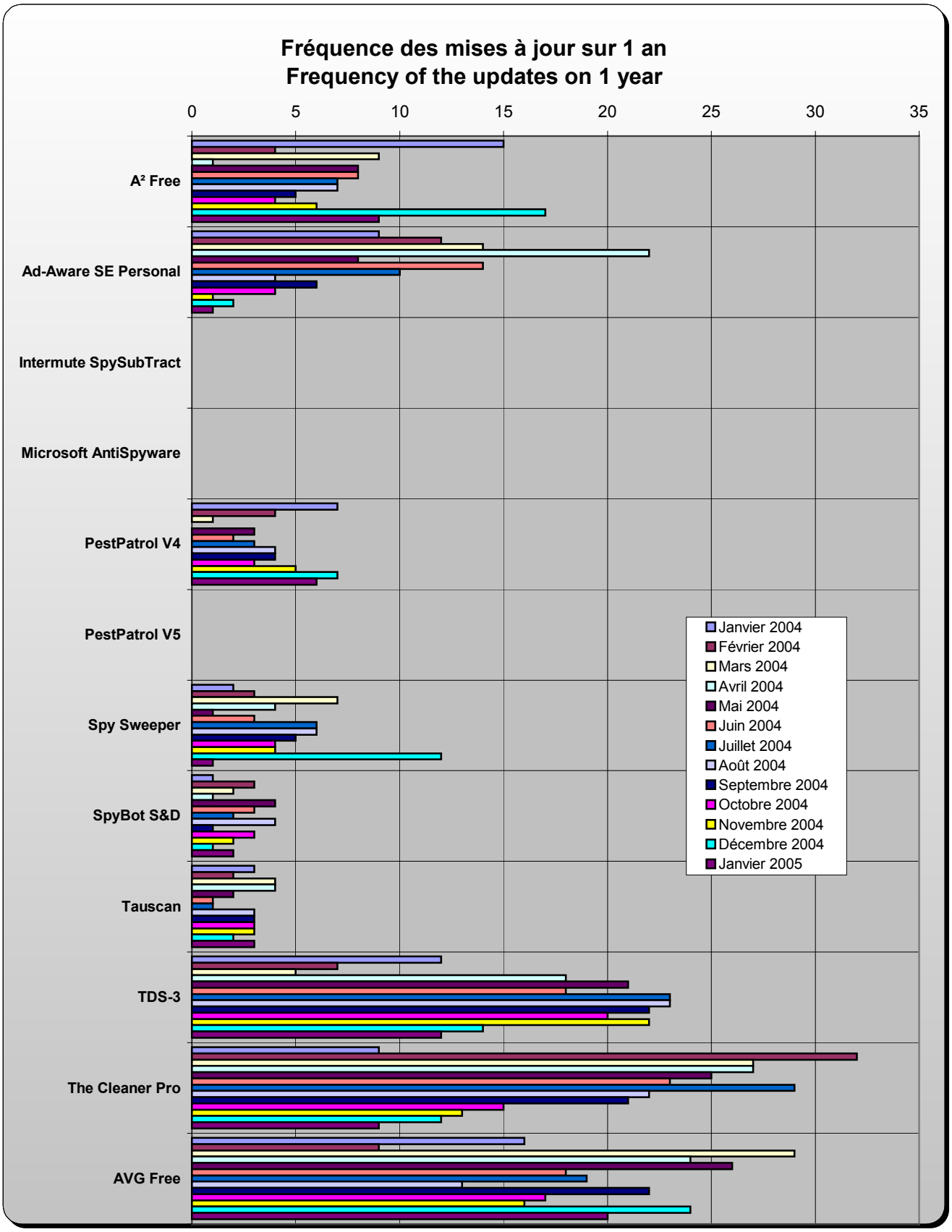


*Figure 32 – Graphique – Fréquence des mises à jour*

# 8. Fonctionnalités

## Qualité des analyses « On demand »

| Fonctionalités | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Qualité des analyses "on demand"** | **a2** | **aaw** | **isst** | **msas** | **pp4** | **pp5** | **ss** | **sb s&d** | **tau** | **tds** | **tc** | **avg** |
| Ads - Signalement d'ADS | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Ads - Lecture des ADS | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Ads - Effacement des ADS | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Analyse des processus actifs en mémoire | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| Analyse de la base de registre | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Analyse des URLs des raccourcis | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Analyse des emplacements privilégiés | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Analyse des fichiers | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗[1] | ✓ | ✓ | ✓ | ✓ |
| Signale les cookies à spywares | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Analyse d'objets choisis | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| Parfaire éradication au prochain redémarrage | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Détecte les extensions multiples | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Détecte un hijack de hosts | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓[2] | ✗ | ✗ | ✗ | ✗ |
| Détecte un hijack des favoris | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Détecte un hijack de la zone de confiance (IE) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Détecte un hijack de la zone bloquée (IE) | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Nettoyage des MRUs | ✗ | ✗ | ✗[1] | ✗[1] | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Mise en quarantaine | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |

*Figure 33 – Tableau des fonctionnalités – Qualité des analyses « On demand »*

MSAS[1]
Microsoft AntiSpyware permet le nettoyage des MRUs dans un module des « Advanced Tools » et non pas dans les résultats du scan anti-trojans.

## Qualité du module temps réel

| Fonctionalités | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Qualité du module "temps réel"** | **a2** | **aaw** | **isst** | **msas** | **pp4** | **pp5** | **ss** | **sb s&d** | **tau** | **tds** | **tc** | **avg** |
| Notification modif dans fichier Hosts | ✗ | ✗ | ✗ | ✗[1] | ✗ | ✗ | ✓ | ✓[3] | ✗ | ✗ | ✗ | ✗ |
| Modification des pages d'IE (Hijacker) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓[3] | ✗ | ✗ | ✗ | ✗ |
| Modification des réglages d'IE (personnes physique) | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Modification de zones privilégiées du registre | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Injection dans un processus monté en mémoire | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Accès aux objets (on access) | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| Anti-dialer par activité | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Anti-keylogger par activité | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Notification d'établissement de connexion WiFi | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification d'inscription dans sites de confiance (IE) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification d'addition/modification des Winsock LSPs | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification de changement d'état Net Send | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification robot de messagerie (spam zombie) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification d'addition/modification de serveur proxy | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification de changement de DNS | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification de modif paramètres TCP/IP | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification d'addition de services Windows | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif des menus contextuels | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif dans Shell Execute Hook | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif dans Shell Open Commands | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif dans system.ini | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification nom légitime dans répertoire inattendu | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif dans la liste des extensions | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif dans win.ini | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif panneau configuration (inetcpl.cpl) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif .ini file mapping | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif Shared TaskSheduller | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif Windows Shell Extensions | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif Shell Service Delay Load | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif User Shell Folders (répertoires) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif du Shell lancé au login utilisateur | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif paramètres de clé \Userinit | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif AppInit_DLLs | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification d'existence du trojan c:\explorer.exe | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification activation Win XP Pro Auto-Logon | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif paramétrage de Windows Update | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif des drivers de protocoles standards | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif restrictions d'utilisateurs anonymes | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif Windows logon policies (Log on/off) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |
| Notification modif de WOW\Boot\Shell | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ?[2] | ✗ | ✗ | ✗ | ✗ |

*Figure 34 – Tableau des fonctionnalités – Qualité des modules « Temps réel »*

SSD[2]
SpyBot Search & Destroy met en place, avec son TeaTimer en pseudo temps réel, comme Microsoft AntiSpyware avec son module en pseudo temps réel, de nombreuses notifications. En Février 2005 il en existe 35 (et 55 dans Microsoft AntiSpyware). Toutefois, Patrick Kolla n'ayant pas encore rédigé une communication étendue à propos du TeaTimer, on ne sait pas exactement quelles notifications sont en place et on ne peut qu'en deviner quelques-unes chaque fois que la fenêtre d'alerte nous saute aux yeux.

## Usage préventif et couteau Suisse

| Fonctionalités | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Usage préventif et couteau Suisse** | **a2** | **aaw** | **isst** | **msas** | **pp4** | **pp5** | **ss** | **sb s&d** | **tau** | **tds** | **tc** | **avg** |
| Fourni une liste cookies bloqués | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Fourni une liste domaines bloqués - Liste Hosts | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓1 | ✓1 | ✗ | ✗ | ✗ | ✗ |
| Fourni une liste domaines bloqués - Restriction IE | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Fourni une liste contrôles ActiveX bloqués - Kill Bit | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Permet de lire la liste des contrôles ActiveX installés | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Permet de gérer la liste des contrôles ActiveX installés | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Permet de lire la liste des BHOs installés | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Permet de gérer la liste des BHOs installés | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Fournit des informations sur les BHOs | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Permet de lire la liste des pages IE | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Permet de gérer la liste des pages IE | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Permet de lire la liste des tâches actives | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Permet de lire la liste des modules actifs dépendants | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Permet de gérer la liste des tâches actives (tuer) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Fournit des informations sur les tâches actives | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Recherche / Corrections des incohérences du registre | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓4 | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Permet de lire la liste de démarrage du système | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |
| Permet de gérer la liste de démarrage du système | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Fournit des informations sur les objets au démarrage | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓5 | ✗ | ✗ | ✗ | ✗ |
| Fournit des informations de désinstallations | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Permet de lire la liste des services (NT) | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓1 | ✗ | ✗ |
| Permet de gérer la liste des services (NT) | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓2 | ✗ | ✗ |
| | | | | | | | | | | | | |
| Permet de lire la liste des ajouts au Shell (Explorer.exe) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Permet de gérer la liste des ajouts au Shell | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Permet de lire la liste des Winsock LSPs | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Fournit des informations sur les Winsock LSPs | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Nettoyage des MRUs | ✗ | ✗ | ✓1 | ✓ | ✗ | ✗ | ✗ | ✗6 | ✗ | ✗ | ✗ | ✗ |
| | | | | | | | | | | | | |
| Fourni un mécanisme d'envoi de rapports et suspicions | ✗ | ✗ | ✓ | ✓1 | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Fourni un effaceur de sécurité | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |

*Figure 35 – Tableau des fonctionnalités – Usage préventif et « Couteau Suisse »*

ISST[1]
Intermute SpySubtract propose un nettoyage des MRUs dans un module en dehors de l'analyse générale anti-trojans.

MSAS[1]
SpyNet ; le mécanisme de rapport, si activé, est automatique. Nous conseillons de ne jamais activer ce genre de fonctions qui font sortir de l'information vers un serveur extérieur sans que nous puissions la contrôler.

MSAS[2]
Nous déconseillons les mises à jour automatiques en général sauf pour les antivirus. Le cas des anti-trojans peut ou peut ne pas être assimilé aux antivirus, c'est une affaire de prise de risque de chacun.

SS[1]

La liste hosts fournie par Spy Sweeper est très réduite (un peu moins de 700 entrées).

SB S&D[1]
La liste hosts fournie par SpyBot contient, à ce jour, 1021 entrées ce qui est surprenant car elle en comptait plus de 20.000 par le passé.

SB S&D[4]
Travaille sur une petite liste de clés généralement non traitées par les nettoyeurs de bases de registre habituels.

SB S&D[6]
Les informations, en français, proviennent de la PacMan Startup List. La traduction officielle de cette liste, pour SpyBot, est assurée par NickW (modératrice sur les forum http://assiste.free.fr et traductrice en français de SpyBot, du site de SpyBot…). La version française officielle de cette liste est déposée sur Assiste.com. Elle est consultable en ligne et téléchargeable depuis http://assiste.free.fr/p/pacman/liste_pacman_frameset.php ).

SB S&D[6]
SpyBot Search & Destroy permet le nettoyage des MRUs dans le module général d'analyse (dans les résultats du scan anti-trojans).

TDS3[1]
Voir la liste des services est un bien grand mot. On ne sait pas dans quel état ils sont et aucune information n'est donnée.

TDS3[2]
Gérer la liste est un bien grand mot !

## Profondeur du paramétrage / Configuration / Mise à jour

| Fonctionalités | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Profondeur du paramétrage / Configuration** | **a2** | **aaw** | **isst** | **msas** | **pp4** | **pp5** | **ss** | **sb s&d** | **tau** | **tds** | **tc** | **avg** |
| Liste d'exclusions - White List | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |
| Liste d'inclusions - Black List | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Cibles à analyser - Sélection de volumes | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | | ✓ |
| Cibles à analyser - Sélection de répertoires | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | | ✓ |
| Cibles à analyser - Sélection de fichiers | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | | ✗ |
| Cibles à analyser - Sélection par Drag and Drop | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Cibles à analyser - Sauvegardes des sélections | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | | ✗ |
| Cibles à analyser - 1 fichier (menu contextuel - Shell) | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | | ✗ |
| Cibles à analyser - 1 répertoire (menu contextuel) | ✗ | ✗[1] | ✓ | ✗ | ✓ | ✗ | ✗[1] | ✗ | ✓ | ✓ | | ✗ |
| Réglage de la priorité des scans "on demand" | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | | ✗ |
| Existence de Plugins | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | | ✗ |
| Sauvegarde des réglages | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | | ✗ |
| Sauvegarder / Défaire les corrections majeures (Trojans, Co | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | | ✗ |
| Sauvegarder / Défaire les corrections mineures (MRUs…) | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | | ✗ |
| Sauvegarder / Défaire les corrections système | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Age des sauvegardes (en jours ou paramétrable) | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | | ✓ |
| Automatismes programmables au démarrage Windows | ✗ | ✗ | ✓[1] | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | | ✗[1] |
| Automatismes programmables au lancement du logiciel | ✗ | ✗ | ✓[1] | ✗ | ✓ | ✗ | ✗[2] | ✓ | ✗ | ✗ | | ✗[1] |
| Automatismes programmables à intervalles | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | | ✗[1] |
| | | | | | | | | | | | | |
| **Mises à jour** | **a2** | **aaw** | **isst** | **msas** | **pp4** | **pp5** | **ss** | **sb s&d** | **tau** | **tds** | **tc** | **avg** |
| Mise à jour manuelle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Mise à jour automatique | ✗ | ✓ | ✓ | ✓[2] | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | | ✓ |
| Mise à jour programmée | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | | ✓ |
| Mise à jour par push | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

Figure 36 – Tableau des fonctionnalités – Qualité des paramétrages – configuration – mises à jour

AAW[1]
L'insertion de Ad-aware dans les menus contextuels de l'explorateur de Windows est possible dans les versions payantes de Ad-aware.

SS[1]
Détestable. Cela peut paraître fou mais l'insertion d'une entrée dans les menus contextuels de l'explorateur de Windows permet de lancer une analyse de… tout le système !!! Aucune possibilité d'analyser juste le répertoire en cours sur lequel on se trouve ou un fichier tout seul !
D'une manière général, Spy Sweeper ne permet jamais de sélectionner un fichier, ni même un répertoire à analyser. C'est un disque entier ou rien

SS[2]
Il y a bien un automatisme paramétrable, très mal placé et ambiguë, qui consiste en réalité à lancer le module temps réel de Spy Sweeper avec le démarrage de Windows.

AVG[1]
Disponible dans la version commerciale

# 9. Résultats des courses

## Récapitulatif – Mesures brutes effectuées

| Récapitulation des résultats bruts obtenus | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Fiche (17) | Fiche (18) | Fiche (19) | Fiche (20) | Fiche (21) | Fiche (22) | Fiche (49) | Fiche (23) | Fiche (24) | Fiche (25) | Fiche (26) | Fiche |
| Durée du scan | 776 | 270 | 511 | 390 | 400 | 77 | 254 | 103 | 640 | 830 | 994 | 568 |
| Pic de taille du processus | 20724 | 25332 | 47308 | 42468 | 38392 | 38840 | 37380 | 33856 | 12528 | 35888 | 23072 | 28908 |
| Charge moyenne du processeur | 70 | 50 | 50 | 30 | 45 | 2 | 55 | 100 | 40 | 75 | 80 | 50 |
| Total parasites annoncé (résultat inexploitable) | 5 | 163 | 1166 | 13 | 509 | 11 | | 6 | 0 | 6 | 9 | 0 |
| Parasites trouvés - On Access | 0 | 0 | 6 | 5 | 4 | 0 | 3 | 8 | 0 | 0 | 6 | 0 |
| Parasites trouvés - On Boot | 0 | 0 | 1 | 0 | 3 | 0 | 1 | 0 | 0 | 0 | 2 | 0 |
| Parasites trouvés - On Demand | 2 | 2 | 6 | 9 | 9 | 9 | 6 | 6 | 0 | 5 | 2 | 0 |
| Parasites trouvés - Erreurs et faux positifs | 0 | 0 | 1 | 4 | 1 | 2 | 1 | 1 | 0 | 0 | 0 | 0 |
| Nombre d'objets analysés (résultat inexploitable) | 25800 | 85605 | 49435 | 23177 | 50723 | ? | | 25607 | 32207 | 24099 | 31703 | 33211 |

*Figure 37 – Tableau récapitulatif : Mesures brutes effectuées*

## Récapitulatif – Notes calculées ou attribuées, /10.

| Notation des résultats (sur 10) | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Durée du scan | 2,38 | 7,90 | 5,27 | 6,59 | 6,48 | 10,00 | 8,07 | 9,72 | 3,86 | 1,79 | 0,00 | 4,65 |
| Pic de taille du processus | 7,64 | 6,32 | 0,00 | 1,39 | 2,56 | 2,43 | 2,85 | 3,87 | 10,00 | 3,28 | 6,97 | 5,29 |
| Charge moyenne du processeur | 3,06 | 5,10 | 5,10 | 7,14 | 5,61 | 10,00 | 4,59 | 0,00 | 6,12 | 2,55 | 2,04 | 5,10 |
| Total parasites annoncé (résultat inexploitable) | | | | | | | | | | | | |
| Parasites trouvés - On Access | 0,00 | 0,00 | 5,45 | 4,55 | 3,64 | 0,00 | 2,73 | 7,27 | 0,00 | 0,00 | 5,45 | 0,00 |
| Parasites trouvés - On Boot | 0,00 | 0,00 | 0,91 | 0,00 | 2,73 | 0,00 | 0,91 | 0,00 | 0,00 | 0,00 | 1,82 | 0,00 |
| Parasites trouvés - On Demand | 1,54 | 1,54 | 4,62 | 6,92 | 6,92 | 6,92 | 4,62 | 4,62 | 0,00 | 3,85 | 1,54 | 0,00 |
| Parasites trouvés - Erreurs et faux positifs | 10,00 | 10,00 | 9,00 | 6,00 | 9,00 | 8,00 | 9,00 | 9,00 | 0,00 | 10,00 | 10,00 | 0,00 |
| Nombre d'objets analysés (résultat inexploitable) | | | | | | | | | | | | |
| ADS (Voit+Lit+Efface) | 0,00 | 2,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 10,00 | 0,00 | 0,00 |
| Ergonomie générale | 4,00 | 4,00 | 5,00 | 9,00 | 6,00 | 6,00 | 7,00 | 7,00 | 5,00 | 0,00 | 4,00 | 4,00 |
| Ergonomie de lecture des résultats à l'écran | 0,00 | 5,00 | 6,00 | 8,00 | 3,00 | 0,00 | 8,00 | 8,00 | 0,00 | 0,00 | 4,00 | 0,00 |
| Ergonomie de lecture des logs | 0,00 | 0,00 | 0,00 | 8,00 | 2,00 | 0,00 | 0,00 | 5,00 | 0,00 | 0,00 | 2,00 | 0,00 |
| Logiciel et documentation en français | 10,00 | 10,00 | 0,00 | 0,00 | 10,00 | 0,00 | 0,00 | 10,00 | 0,00 | 0,00 | 0,00 | 0,00 |

*Figure 38 – Tableau récapitulatif : Notes calculées (ou attribuées) sur 10*

## Récapitulatif – Les coefficients de pondération utilisés.

Les coefficients de pondération permettent de donner plus ou moins d'importance aux notes ci-dessus. Pour un anti-trojans [(51)] comme pour un antivirus [(52)], découvrir des parasites est plus significatif que la vitesse à laquelle cela est fait. Le faire en temps réel l'est encore plus.

| Coefficients de pondération | Coef | Note maxi |
|---|---|---|
| Durée du scan | 1,00 | 10 |
| Pic de taille du processus | 1,00 | 10 |
| Charge moyenne du processeur | 1,00 | 10 |
| Total parasites annoncé (résultat inexploitable) | | |
| Parasites trouvés - On Access | 13,45 | 134,5 |
| Parasites trouvés - On Boot | 13,45 | 134,5 |
| Parasites trouvés - On Demand | 8,07 | 80,69 |
| Parasites trouvés - Erreurs et faux positifs | 4,03 | 40,34 |
| Nombre d'objets analysés (résultat inexploitable) | | |
| ADS (Voit+Lit+Efface) | 3,00 | 30 |
| Ergonomie générale | 2,00 | 20 |
| Ergonomie de lecture des résultats à l'écran | 3,00 | 30 |
| Ergonomie de lecture des logs | 1,00 | 10 |
| Logiciel et documentation en français | 1,00 | 10 |
| **Note totale maximum** | | **520** |
| Total des coefficients non "Parasites" | 13,00 | |
| Total des coefficients "Parasites" | 39,00 | |
| Total des coefficients | 52,00 | |

*Figure 39 – Tableau récapitulatif : Les coefficients de pondération utilisés*

## Nota Important

Le système de notation pourra varier dans l'avenir, en particulier par l'adjonction de nouvelles notes (ce qui est sans incidence dans le résultat final des prochains comparatifs puisque c'est la totalité des tests qui est reprise chaque fois). Par contre, la somme des 4 coefficients de pondération :

- Parasites trouvés - On Access
- Parasites trouvés - On Boot
- Parasites trouvés - On Demand
- Parasites trouvés - Erreurs et faux positifs

Représentera toujours les ¾ (75%) de la pondération totale car :

- C'est tout de même le plus important et de loin
- Ceci marginalise le risque de notation subjective d'éléments comme le « confort d'usage »… la notation « Parasites » étant automatique sans risque d'interférence avec la subjectivité humaine.

Le calcul des coefficients est :
Total des coefficients « Non parasites » = une certaine somme.
Total des coefficients « Parasites » = Total des coefficients « Non parasites » * 3

La proportion entre les 4 coefficients « Parasites » est et sera toujours respectée. Elle représente :

- Parasites trouvés - On Access34,48% du total des coefficients « Parasites »
- Parasites trouvés - On Boot34,48% du total des coefficients « Parasites »
- Parasites trouvés - On Demand20,69% du total des coefficients « Parasites »
- Parasites trouvés - Erreurs et faux positifs10,34% du total des coefficients « Parasites »

# 10.Résultat final du comparatif

## Les notes finales obtenues

| Notation pondérée des résultats | A² Free | Ad-Aware SE Personal | Intermute SpySubTract | Microsoft AntiSpyware | PestPatrol V4 | PestPatrol V5 | Spy Sweeper | SpyBot S&D | Tauscan | TDS-3 | The Cleaner Pro | AVG Free |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Durée du scan | 2,38 | 7,90 | 5,27 | 6,59 | 6,48 | 10,00 | 8,07 | 9,72 | 3,86 | 1,79 | 0,00 | 4,65 |
| Pic de taille du processus | 7,64 | 6,32 | 0,00 | 1,39 | 2,56 | 2,43 | 2,85 | 3,87 | 10,00 | 3,28 | 6,97 | 5,29 |
| Charge moyenne du processeur | 3,06 | 5,10 | 5,10 | 7,14 | 5,61 | 10,00 | 4,59 | 0,00 | 6,12 | 2,55 | 2,04 | 5,10 |
| Total parasites annoncé (résultat inexploitable) | | | | | | | | | | | | |
| Parasites trouvés - On Access | 0,00 | 0,00 | 73,35 | 61,13 | 48,90 | 0,00 | 36,68 | 97,81 | 0,00 | 0,00 | 73,35 | 0,00 |
| Parasites trouvés - On Boot | 0,00 | 0,00 | 12,23 | 0,00 | 36,68 | 0,00 | 12,23 | 0,00 | 0,00 | 0,00 | 24,45 | 0,00 |
| Parasites trouvés - On Demand | 12,41 | 12,41 | 37,24 | 55,86 | 55,86 | 55,86 | 37,24 | 37,24 | 0,00 | 31,03 | 12,41 | 0,00 |
| Parasites trouvés - Erreurs et faux positifs | 40,34 | 40,34 | 36,31 | 24,21 | 36,31 | 32,28 | 36,31 | 36,31 | 0,00 | 40,34 | 40,34 | 0,00 |
| Nombre d'objets analysés (résultat inexploitable) | | | | | | | | | | | | |
| ADS (Voit+Lit+Efface) | 0,00 | 6,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 30,00 | 0,00 | 0,00 |
| Ergonomie générale | 8,00 | 8,00 | 10,00 | 18,00 | 12,00 | 12,00 | 14,00 | 14,00 | 10,00 | 0,00 | 8,00 | 8,00 |
| Ergonomie de lecture des résultats à l'écran | 0,00 | 15,00 | 18,00 | 24,00 | 9,00 | 0,00 | 24,00 | 24,00 | 0,00 | 0,00 | 12,00 | 0,00 |
| Ergonomie de lecture des logs | 0,00 | 0,00 | 0,00 | 8,00 | 2,00 | 0,00 | 0,00 | 5,00 | 0,00 | 0,00 | 2,00 | 0,00 |
| Logiciel et documentation en français | 10,00 | 10,00 | 0,00 | 0,00 | 10,00 | 0,00 | 0,00 | 10,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| | | | | | | | | | | | | |
| **Note totale** | **83,84** | **111,07** | **197,50** | **206,32** | **225,41** | **122,57** | **175,97** | **237,94** | **29,98** | **109,00** | **181,57** | **23,04** |

Figure 40 – Tableau récapitulatif : Les notes finales obtenues

## Le graphique comparatif final

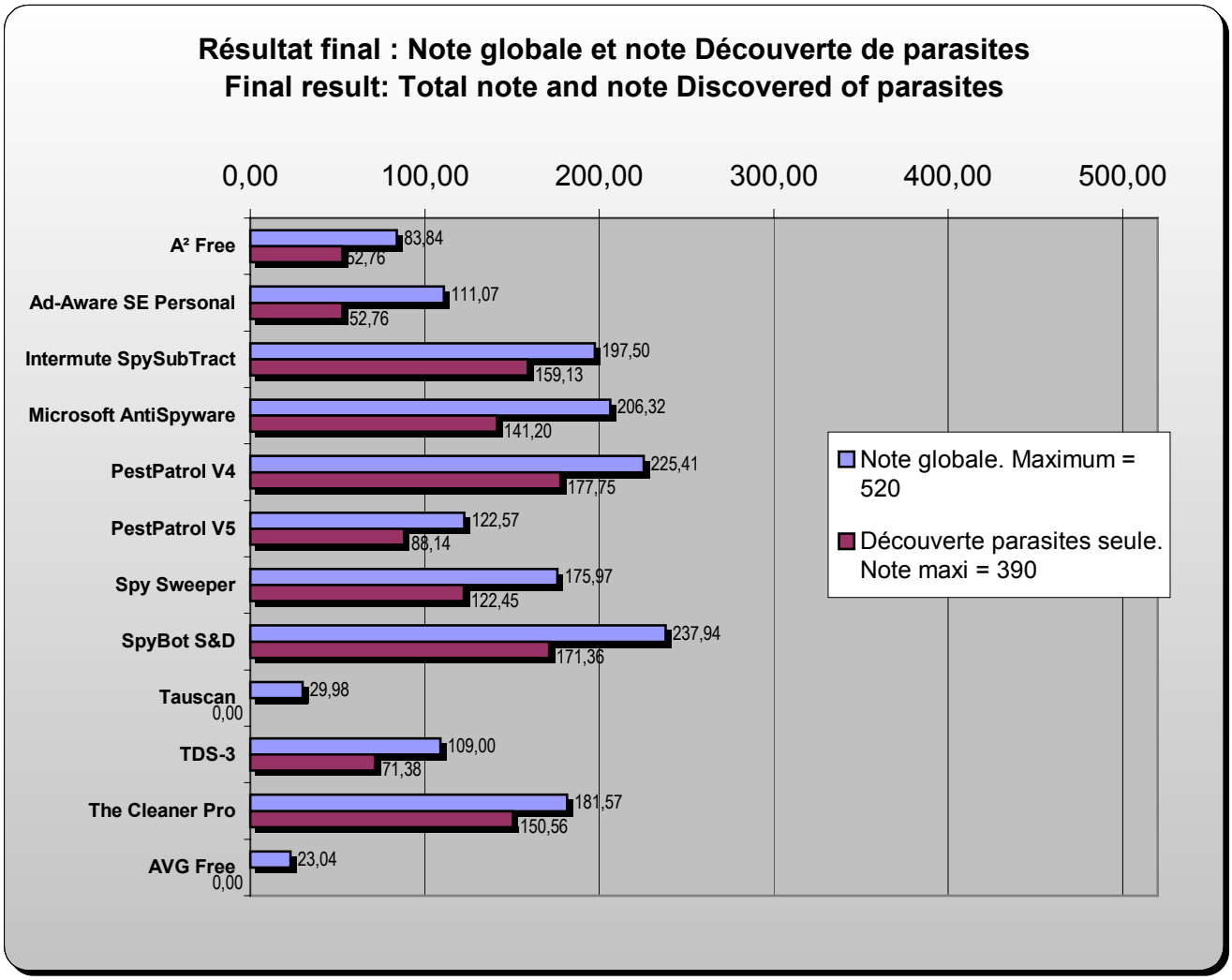


*Figure 41 – Comparatif : Résultat final des tests*

# 11.Conclusions

## *Conclusions du test portant sur une installation de Kazaa V 3.0 US*

Les analyses ont été exécutées complètement, 3 fois, afin de s'assurer qu'aucun parasite n'a été ajouté ou détruit durant les tests.

Qu'ont trouvé les utilitaires de sécurité, sachant que Kazaa déclare lui-même contenir :

- Bullguard antivirus
- Altnet Topsearch
- Cydoor (1)
- GAIN Network (2)
- Altnet peerpoints Manager Package incluant
  - My Search Toolbar
  - P2P Networking Application

Nous devrions donc trouver, au moins, ce qui précède.

Les utilitaires qui n'ont pas tout trouvé sont complètement impardonnables. On ne peut admettre que l'on puisse passer à côté de l'une des charges actives conduites par le cheval de Troie le plus diffusé au monde depuis des années.

- Remarque sur Bullguard.
  Cette suite intégrée, constituée d'un antivirus, d'un pare-feu et d'un outil de sauvegarde, peut être considérée comme un antivirus (52) « normal » par les outils testés mais sa distribution repose essentiellement sur son déploiement avec Kazaa. Il est donc légitime de penser que le produit, qui est une version spéciale P2P, est suspect de ne jamais découvrir les parasites inclus dans Kazaa, son principal distributeur. De ce fait, la présence de Bullguard dans les résultats d'analyses des anti-trojans (51) est considérée comme tout à fait légitime : il ne s'agit pas d'un faux positif. D'autre part, ce produit contient un adware : une fenêtre publicitaire, en pop-up.

### A² Free

**http://assiste.free.fr/p/internet_utilitaires/a2.php**

Sur le test « On Access », A² Free ne bronche pas. Il ne voit strictement rien.
Sur le test « On Boot », c'est la même chose. Il est totalement inexistant.
Sur le test « On Demand » A² free ne voit vraiment pas grand-chose :

1. Spyware.Win32.Gator – il s'agit de GAIN Network (2) / Gator (3) / Claria
2. Spyware.Win32.Toolbar.MyWay.b – il s'agit de MyWay Search Bar

a² Free n'arrive pas à décoller malgré l'énorme capital sympathie et confiance dont il bénéficiait lorsqu'il n'existait que sur le papier. Ce produit est extrêmement décevant. Voir ce fil de discussion (50). Il est insignifiant (sur ce test) et n'est pas recommandé du tout. C'est la version gratuite de A², illimitée dans le temps. Une version appelée A² Personal, commerciale, est plus complète.

### Ad-Aware SE Personal

**http://assiste.free.fr/p/internet_utilitaires/ad_aware.php**

Sur le test « On Access », Ad-Aware SE Personal Free ne bronche pas. Il ne voit strictement rien
Sur le test « On Boot », c'est la même chose. Il est totalement inexistant.
Sur le test « On Demand » Ad-aware SE Personal ne voit pas grand-chose

1. AltNetBDE (113 items) (également cité pour 6 items sous le nom de BrillantDigital)
2. Claria (Gator (3)) (32 items)

Ce produit est extrêmement décevant. Il est insignifiant, complètement laminé (sur ce test) et n'est pas recommandé du tout. Il s'agit de la version gratuite, illimitée dans le temps, de Ad-Aware. Le module temps-réel n'est disponible que dans les versions commerciales Ad-Aware Plus et Ad-Aware Professional qui sont plus complètes.

## Intermute SpySubTract

**http://assiste.free.fr/p/internet_utilitaires/spysubtract.php**

Sur le test « On Access », Intermute SpySubtract tire son épingle du jeu et voit 6 parasites sur 9, dont Kazaa lui-même.
Sur le test « On Boot », son comportement est passif (une analyse appelée « Vénus », boucle indéfiniment en arrière plan., Elle met plusieurs minutes avant de signaler très peu de choses et recommence ce qui la rend agaçante. Nous finissons par la désactiver. Le produit se retrouve sans module « boucle infinie appelée « temps réel » » ). (voir notre commentaire dans le § « On Boot »)
Sur le test « On Demand » Intermute voit

1. Sharman NetWorks (649 items) – Il s'agit d'une partie d'Altnet - le zombie Altnet
   Altnet, Inc (210 items) – Il s'agit d'une autre partie d'Altnet. Pourquoi sous 2 noms ?
   Joltid Ltd. (64 items) – Il s'agit d'une troisième partie d'Altnet. « P2P Networking », un trojan (downloader)
2. GAIN Network [2] Gain Publishing, Inc (235 items) – il s'agit de Gator [3] / Claria
3. BullGuard (1 Item)

Intermute Spy Subtract fait également une erreur avec Grokster (4 items).
C'est un produit qui, sur ce test, est moyen d'autant qu'il s'agit d'une version commerciale complète.

## Microsoft AntiSpyware (ex Giant) Antispyware

**http://assiste.free.fr/p/internet_utilitaires/microsoft_antispyware.php**

Sur le test « On Access », Microsoft AntiSpyware voit 5 parasites sur 9.
Sur le test « On Boot », il est totalement inexistant.
Sur le test « On Demand » il voit

1. Kazaa
2. Altnet TopSearch
3. MyWay Search Bar
   My Search Bar (Adware) ??? Pourquoi 2 fois sous 2 noms différents?
4. Altnet Joltid P2P Networking (signalé sous plusieurs noms)
5. Altnet Peer Points Companents
6. Cydoor [1] (Adware)
7. GAIN Network [2] (Adware)
   Claria (Adware)
   ClariaDashbar (Gator Toolbar) – Pourquoi 3 fois GAIN Network [2] / Claria / Gator [3]?
8. InstallFinder
9. Twain Tech (Adware)

Mais il signale simultanément Claria alors qu'il s'agit de Gator déjà signalé (Microsoft AntiSpyware semble beaucoup aimer déclarer un parasite sous plusieurs noms et ainsi en trouver 2 ou 3 là où il n'y en a qu'un), Grokster qui n'a rien à voir là-dedans (erreur) et DownloadWare (Faux positif).

Microsoft AntiSpyware est remarquable en fonctionnalités. Le travail de l'équipe de développement (la société Giant, Microsoft n'a rien à voir avec le développement de ce logiciel, pour l'instant) sur son interface graphique est également remarquable, exemplaire (malgré quelques problèmes comme la non utilisation de la molette des souris, des problèmes d'affichage lorsque de nombreux résultats sont déployés, une lenteur certaine même sur une machine très puissante et dotée d'une très grosse carte graphique…et, plus généralement, il semble que le produit ne respecte pas les standards Windows). L'essentiel étant dans la découverte des parasites, il est pénalisé par des erreurs et faux positifs. Son module temps réel, efficace, est également pris en défaut (hijack de hosts, par exemple). Il lui reste à corriger ses défauts de jeunesse.

Détestable : n'utilise pas le navigateur par défaut mais, systématiquement, Internet Explorer, donc toutes les urls contenues sortent en erreur. Pour des raisons de sécurité ou de goût personnel, tout navigateur alternatif doit être reconnu. Nous agissons dans le monde de la sécurité ce qui sous-entend, immédiatement, actuellement, que Internet Explorer est totalement bloqué (par le pare-feu, par exemple) et qu'un navigateur alternatif est utilisé.

Contrairement à toutes les réserves que l'on peut entendre au sujet de ce logiciel parce que ce serait une version « Bêta », ceci est absolument faux ! Il s'agit strictement de la version commerciale de Giant AntiSpyware avec, pour seul changement, le nom et le logo de Microsoft (mal) accolés dessus, le mot de « Bêta » ajouté, la gratuité jusqu'au 31 juillet 2005 (date après laquelle cette version cessera de fonctionner).

## PestPatrol V4

**http://assiste.free.fr/p/internet_utilitaires/pestpatrol.php**

Sur le test « On Access », PestPatrol V4 ne réagit qu'à 4 reprises. Il pourrait faire beaucoup mieux.
Sur le test « On Boot », PestPatrol donne le meilleur résultat mais il est loin d'être parfait.
Sur le test « On Demand »

1. Kazaa
2. Altnet TopSearch
3. Altnet My Search ToolBar
4. Altnet Joltid P2P Networking
5. Altnet PeerPoints Components
6. (GAIN Network [2] / Gator [3] / Claria)
7. Twain Tech (Adware)
8. AdDestroyer (VirtualBouncer)
9. FlashGet

En terme de découverte des parasites, ce qui est tout de même le plus important, nous recommandons, et de loin, PestPatrol car son spectre est le plus fin et ses bases de signatures les plus vastes. Cet utilitaire gagnerait énormément en refondant complètement son interface graphique, en soignant sa présentation et ses listes de résultats et en proposant l'exportation des journaux (sans verbiage). L'un des usages fondamentaux de tous ces utilitaires est la possibilité donnée à l'utilisateur de copier tout ou partie du journal produit afin de le soumettre à des experts, sur des listes de discussion ou des forums. Avec PestPatrol, cela est complètement impossible ! Il doit également, impérativement, se doter d'une vaste boite à outils s'il veut rester en tête des comparatifs.

## PestPatrol V5 Corporate

**http://assiste.free.fr/p/internet_utilitaires/pestpatrol.php**

Sur le test « On Access », PestPatrol V5 Corporate ne bronche pas et pour cause : il n'est pas fait pour cela.
Sur le test « On Boot », c'est la même chose. Il n'est pas fait pour cela.
Sur le test « On Demand »

1. Kazaa
2. Altnet TopSearch
3. Altnet My Search ToolBar
4. Altnet Joltid P2P Networking
5. (GAIN Network [2] / Gator [3] / Claria)
6. Twain Tech (Adware)
7. AdDestroyer (VirtualBouncer)
8. Gain Gator Precision Time
9. Gain Gator DashBar

Nota :
Cet anti-trojans [51] est le seul à avoir vu le système pyramidal de Claria qui, dans un fichier caché, donne l'ordre de télécharger et installer silencieusement deux autres produits de Claria, DateManager et PrecisionTime

***InstallDateManager.exe=/silent***
***InstallPrecisionTime.exe=/silent /aic=$aic$***

PestPatrol 5 Corporate est un cas à part. C'est un produit purement temps différé dédié réseaux. Sa base de signatures semble être la même que celle de PestPatrol 4 mais ses algorithmes semblent plus fins. Si on le compare aux autres uniquement sur ce qui est comparable pour lui, « Analyse On demand », c'est le meilleur de tous.

## Spy Sweeper

**http://assiste.free.fr/p/internet_utilitaires/spy_sweeper.php**
Sur le test « On Access », Spy Sweeper ne voit que 3 parasites sur 9
Sur le test « On Boot » son comportement n'est pas clair (voir notre commentaire dans le § « On Boot »).
Sur le test « On Demand » Spy Sweeper tire son épingle du jeu. Il voit :

1. Altnet TopSearch
2. Altnet My Search Bar
3. Altnet Joltid P2P Networking
4. Altnet Peer Points Components

5. Cydoor [1]
6. GAIN.Dashbar
   GAIN Network [2].( Gator [3] )

Sur le test Kazaa, Spy Sweeper a un comportement moyen.
Détestable : les liens dans Spy Sweeper, par exemple le lien « Acheter Spy Sweeper », cherchent à utiliser Internet Explorer au lieu du navigateur par défaut.

## Spybot Search & Destroy

**http://assiste.free.fr/p/internet_utilitaires/spybot_search_destroy.php**

Sur le test « On Access », SpyBot Search and Destroy, grâce à son module pseudo temps réel efficace, concentré sur les emplacements privilégiés, réagit bien mieux que tous les autres.
Sur le test « On Boot » il est totalement inexistant.
Sur le test « On Demand »

1. Altnet TopSearch
2. Altnet My Search Bar
3. Altnet Joltid P2P Networking
4. Altnet Peer Points Components
5. Cydoor [1]
6. GAIN.Dashbar
   GAIN Network [2].( Gator [3] )

Il commet également un faux positif.

Nous recommandons SpyBot Search & Destroy, gratuit, qui obtient une très bonne note, juste derrière PestPatrol en terme de découverte de parasites. Son ergonomie est perfectible mais déjà bonne. Une mesure n'a pas été conduite et le pénaliserait considérablement : les restes après décontamination : SpyBot est difficilement comparable car ce n'est pas un scanner de fichiers mais uniquement d'emplacements privilégiés. Après décontamination, 100% des fichiers de parasites sont laissés intacts. SpyBot ne recherche pas les fichiers contaminés mais uniquement les parasites installés, actifs. Il devrait proposer une exportation de ses journaux. Sa boite à outils est remarquable. Le TeaTimer, le module pseudo temps réel, gagnerait probablement si son auteur, Patrik Kolla, communiquait sur ce qu'il fait (chaque emplacement surveillé). Ses pop-ups d'alerte sont perfectibles :

- on devrait pouvoir y copier l'information pour l'exploiter ailleurs (dans la rédaction d'un rapport, dans une soumission à un moteur de recherche ou un outil d'analyse, dans une demande d'aide sur un forum…) – il suffit d'utiliser des zones éditables ou lieu de zones de labels.
- elles devraient être redimensionnables (ou plus grandes) car une partie de l'information est masquée
- pour des raisons de compatibilité avec les Windows 9x, des informations essentielles sont absentes dont le nom du processus qui tente d'ajouter / modifier / supprimer une clé. Une détection du système hôte devrait permettre d'utiliser des fonctions spécifiques NT.

## Tauscan

**http://assiste.free.fr/p/internet_utilitaires/tauscan.php**

Sur le test « On Access », Tauscan ne bronche pas. Il ne voit strictement rien.
Sur le test « On Boot », c'est la même chose. Il est totalement inexistant
Sur le test « On Demand » il ne voit encore rien.
Nous avons pensé, longtemps, à une erreur de manipulation ou une incompatibilité avec autre chose mais d'autres essais ont été conduits sur d'autres machines pour s'assurer que nous ne faisions pas de fausse manip. Nous l'avons même confronté aux prémices des collections de parasites en cours de constitution pour le prochain test comparatif. Force est de constater que Tauscan ne voit absolument rien. Nous avons tenté d'obtenir un résultat en le relançant plusieurs fois, avec divers réglages (par défaut, minimum, maximum, avec l'assistant (Wizard), en mode contextuel (clic droit sur un objet (Disque, Répertoire, fichier)). Nous l'avons même lancé dans son mode avancé (l'analyse à duré 8h53 !!!). Nous avons procédé à une mise à jour en dehors du créneau de temps alloué à cette manœuvre qui veut que tous les outils testés soient à égalité (mise à jour au même moment). Nous sommes même allés au-delà dans le viol de notre protocole. Nous l'avons re-téléchargé, ré-installé dans son répertoire par défaut (normalement, toutes les applications que nous installons le sont dans un répertoire spécifique, hors des bibliothèques de Windows), remis à jour plusieurs jours après la mise à jour

des autres produits. Rien n'y fait ! Nous entrerons en communication avec Agnitum pour trouver une solution car Tauscan est, normalement, un très bon produit. Peut-être ne gère t'il que certaines familles de parasites. En tout état de cause nous avons même du modifier notre équation de calcul automatique de points car Tauscan recevait le maximum de points sur la note « Ne génère pas de faux positif ». Désormais, si un produit ne trouve rien à l'analyse normale, il est déduit qu'il ne fonctionne pas du tout. Cette note est alors fixée à zéro.

## The Cleaner

**http://assiste.free.fr/p/internet_utilitaires/the_cleaner.php**

Sur le test « On Access », The Cleaner voit 6 parasites sur 9.
Sur le test « On Boot », il n'en voit que 2 mais, au royaume des aveugles, les borgnes sont rois car la majorité des utilitaires ne voit strictement rien « On Boot ».
Sur le test « On Demand »The Cleaner ne voit pas grand-chose :

1. Gator (3)
2. Altnet MySearchBar

C'est un produit qui, très curieusement, est meilleur en temps réel, domaine réputé difficile, qu'en temps différé (scan à la demande), domaine réputé facile. C'est le coefficient de pondération appliqué à sa note temps réel qui le sauve.

## TDS-3

**http://assiste.free.fr/p/internet_utilitaires/tds.php**

Sur le test « On Access », TDS-3 ne bronche pas. Il ne voit strictement rien.
Sur le test « On Boot », c'est la même chose. Il est totalement inexistant.
Sur le test « On Demand »

1. Adware.AltNet
2. Adware.Gator.4126
3. Adware.Gator.5017.a
4. Adware.Toolbar.MyWay.f
5. Adware.Altnet.a
6. Adware.Altnet.b1

TDS-3 a vraiment besoin d'une cure de jouvence sévère, une ré-écriture complète, bien que ses algorithmes soient solides (il fut, par exemple, l'un des premiers, si ce n'est le premier, à empêcher l'injection dans des processus actifs). C'est un produit pour techniciens avec des allures de « mode console » incroyablement désuets, des pointes de courtoise et d'humour (si... si…) !

Détestable : Le bouton « Stop Scan » est énervant. Vous avez beau appuyer dessus, TDS-3 continue de scanner : il passe au volume suivant !

Détestable : La fenêtre TDS Scan Control non redimensionnable ! Impossible de lire la « Curent Scan List ». D'autre part, nous avons introduit 36 fois la même ligne sans que cela ne le fasse broncher.

# 12.L'avenir de ce comparatif

Ce comparatif sera maintenu à jour régulièrement.

- Il sera augmenté horizontalement de nouveaux produits comparés.
- Il sera augmenté verticalement de nouveaux tests. En particulier :
    - Tests de comportement sur des configurations de Windows durcies (nombreux services désactivés, ports fermés etc. …).
    - Tests classiques de confrontation à des bibliothèques de parasites.
    - Tests de restes après décontamination (T'as d'beaux restes tu sais !).
    - Tests des algorithmes.
    - Notation des fonctionnalités. L'inventaire des fonctionnalités n'est pas terminé actuellement, compte tenu du manque de communication des éditeurs et du manque de temps. Lorsqu'il sera stabilisé, un système de notation sera alors développé.

Les éditeurs qui souhaitent voir leur produit testé peuvent nous en faire parvenir une version complète et illimitée ainsi qu'une documentation étendue.

Merci de bien vouloir signaler les erreurs, omissions, suggestions à assiste.comparatif@free.fr

Le protocole de test a été décrit dans le texte afin qu'il soit reproductible par chacun.

# 13.Analyse de Kazaa

Qui a si gentiment, et contre son gré, servi de cobaye pour ce premier comparatif anti-trojans.

## *Première partie – Avant l'installation*

Cette première partie de l'analyse consiste à aller sur le site de Kazaa et sur les sites de ses partenaires (à partir du moment où un lien existe sur le site de Kazaa) afin de faire l'inventaire des déclarations de Kazaa (lire les présentations des produits, les contrats et licences etc. …) qui seront ensuite comparées aux réalités.

Suppression du mode « Apprentissage » de ProcessGuard
Réglages de Internet Explorer
Tous réglages de sécurité sur « Moyen »

- Sécurité > Internet > Niveau par défaut > Moyen
- Avancé > Paramètres par défaut
- La JVM de SUN n'est pas installée et Microsoft ne livre plus sa JVM, donc JAVA n'est pas du tout installé [29].

Page de démarrage de IE réglée sur http://www.kazaa.com
TeaTimer de Spybot réagit à la modification de la clé du registre – J'accepte définitivement
Microsoft AntiSpyware réagit également – J'accepte définitivement (Amusant : il me rappelle que la valeur par défaut devrait être la sienne soit http://www.msn.com !!!)

### Analyse des documents de Sharman Networks

Nous allons en apprendre presque autant, avec une lecture attentive de plusieurs documents, lecture à laquelle plus personne ne s'astreint, qu'avec tous les utilitaires du monde.

Lancement de Internet Explorer > Connexion directe sur kazaa.com
**Instantanément 135.919 caractères sont reçus et 12.987 sont envoyés !?!**

**Nota :**
Rappelons nous que Kazaa a déclaré une liste de « fonctionnalités » installées avec Kazaa. Revoir notre traduction en première page de ce document.

Clic sur « Français »
Nous tentons de lire la page « Pourquoi Kazaa est gratuit » mais il s'agit d'une traduction automatique de l'anglais vers le français ce qui donne un texte incompréhensible. Retour vers l'anglais qui sera plus fluide.

Sharman Networks nous dit, page http://www.kazaa.com/us/help/faq/howis_kazaa_free.htm, que Kazaa est gratuit car il est supporté par de la publicité (entendez par-là que la société Sharman Networks est payée pour la publicité qu'elle vous délivre via le logiciel Kazaa. Les moyens logiciels mis en œuvre pour gérer cette publicité sur le poste client (sur votre ordinateur) sont Cydoor [1] et GAIN Network [2] (de la société Gator [3]). Donc, en voilà déjà deux ! En lisant le contrat « Utilisateur final », que personne ne lit, un peu plus loin, Sharman Networks citera 4 logiciels et non plus 2. Le test en dénombrera un peu plus. Ce que Sharman Networks ne dit pas c'est qu'elle est payée pour chaque implantation de chaque parasite : c'est là son cœur de métier – déployer des parasites. Pour Sharman Networks, Kazaa n'est qu'un moyen, le véhicule, le Cheval de Troie. Il faut qu'il soit le meilleur possible pour conduire au plus grand déploiement possible des parasites contenus.

**Nota :**
Nous emploierons, dans ce qui suit, « Kazaa » par simplification de langage mais il faut, chaque fois, entendre « Sharman Networks », propriétaire de Kazaa.

### Déclaration « Vie Privée »

La déclaration « Vie privée » de Kazaa [5] [6] est à nouveau une insulte à notre intelligence. Cette page déclare simplement que, dans le logiciel Kazaa, la fonction « En savoir plus sur cet utilisateur » est décochée par défaut et donc que les autres utilisateurs de Kazaa n'ont pas accès à votre répertoire partagé ! Ceci n'a aucun rapport

avec l'usage fait par la société Kazaa des informations collectées sur nous ! C'est sur ces points que nous attendons des commentaires.

## Licence Utilisateur Final

Les articles 1 à 8.1 dégagent Kazaa de tout problème qui pourrait advenir à votre ordinateur, vos fichiers et à vous même etc…
L'article 9 concerne les logiciels Tierce partie qui viennent en « cadeau » avec Kazaa. On peut y lire que :

- Vous « devez » installer des logiciels de tierces parties
- Vous êtes liés aux fournisseurs de ces logiciels tiers selon des contrats spécifiques autres que celui de Kazaa et vous devez lire tous ces contrats attentivement.
- Le simple fait d'utiliser ces logiciels de tierces parties (pourtant vous n'avez rien demandé !) implique l'acceptation de toutes les clauses de leurs licences etc. …
- Kazaa ne vend ni ne revend ni ne licencie ces logiciels tiers et s'en lave les mains aussi loin que le permettent les lois applicables (rappel – Kazaa est installé sur une petite île au large de l'Australie)
- Kazaa ne donne strictement aucune garantie quant à la qualité ou l'innocuité de ces logiciels tiers et ne saurait être recherché en aucun cas, même s'ils enfreignent des lois, causent des dommages directs ou indirects etc. … où qu'ils arrivent et même si Kazaa a été prévenu préalablement de la survenance possible de tels dommages.
- Ces logiciels sont listés au paragraphe 9.4 mais sans limitation. On sait donc que l'on reçoit, au moins, Cydoor [(1)], Altnet Topsearch, Bullguard P2P et GAIN Network [(2)].
- Il y a des risques inhérents à l'installation de tout logiciel depuis l'Internet. Kazaa vous met en garde contre ces logiciels tiers, vous êtes seul responsable etc. …

L'article 9.4.6 est savoureux : en échange du fait que vous avez eu le privilège de télécharger gratuitement ces parasites, vous acceptez expressément ces parasites et vous vous engagez à ne jamais rien faire pour tenter de les retirer, les bloquer, les désactiver, interférer avec eux, etc. … tant que vous n'avez pas totalement désinstallé Kazaa ! Cet article met donc la totalité des internautes du monde ayant Kazaa et un antivirus [(52)], un anti-trojans [(51)], un anti-spywares, un firewall etc. … dans l'illégalité, le contrat n'étant pas respecté ! L'article 12, que vous avez accepté, bien sûr, vous rend passible d'indemnisations lourdes à verser à Kazaa pour violation de cette licence et, excusez du peu, pour la violation des droits d'un tiers (alors qu'ils viennent de dire un peu plus haut qu'ils s'en lavent les mains et n'interviennent pas là-dedans).

Déconnexion du site de Kazaa

# *Installation de Kazaa 3.0 US Free*

## Installation du downloader de Sharman Networks

L'installation de Kazaa passe obligatoirement par l'installation d'un téléchargeur et installeur. Si vous téléchargez Kazaa depuis un site de téléchargement (télécharger.com, c|net etc. …) vous ne téléchargez que le téléchargeur. L'installation de Kazaa se fera toujours et obligatoirement sous le contrôle de ce téléchargeur et uniquement depuis les serveurs de Sharman Networks. Kazaa en lui-même n'est pas disponible en libre téléchargement direct.

Etablissement d'une connexion, directement sur le site de Kazaa.
8.617 caractères reçus et 12.386 envoyés. On est loin des chiffres de la première connexion au même site (voir § précédent).
Clic sur « Français »
Clic sur « Télécharger maintenant »

Le downloader kazaa_setup, 575 Ko, est proposé en exécution. Je choisis de le télécharger et non pas de l'exécuter directement. Il est téléchargé en moins de 4 secondes à 143 Ko / seconde : leur serveur est rapide !

## Sharman NetWorks – Licence et Vie privée

Navigation, sur la machine de tests, jusqu'à kazaa_setup.exe et double clic pour lancer son exécution qui nous dirige immédiatement sur une page d'accueil de Sharman Networks. Celle-ci ne nous apprend rien sinon qu'il faut suivre 4 étapes pour installer Kazaa. Nous passons à la page suivante qui s'avère plus loquace :

- Qu'est-ce que vous acceptez d'installer ?
  - Kazaa
  - Bullguard antivirus
  - Altnet Topsearch
  - Cydoor [1]
  - GAIN Network [2]
  - Altnet peerpoints Manager Package incluant
    - My Search Toolbar
    - P2P Networking Application

Ceci à au moins le bénéfice d'une « certaine » honnêteté mais, en réalité, quel utilisateur se pose la question de savoir ce que sont ces « choses ».

Autre déclaration de Sharman Networks :
« Sharman Networks respecte votre vie privée et vous demande de lire sa déclaration « Vie privée » [6] ». Bien entendu, la liste des informations collectées n'est jamais exhaustive et on vous dit toujours que Sharman Networks collecte des informations telles que etc. … On ne vous donne que des exemples, jamais l'intégrale. Les exemples :
- Nom
- Adresse (une adresse réelle pour expédition d'un achat)
- Informations démographiques (âge… mais aussi sexe, pays etc. …)
- Adresse e-mail
- Etc. …

Tout est dans les etc. … et les points de suspension.

Ces données sont remises à des sponsors ( ? Qui ? Où ? Quoi ? Quand ? Comment ? Pourquoi ?…) et des tiers sous-traitants (Qui ?… Et qui sont censés ne rien en faire ?).

L'adresse e-mail sert à vous faire parvenir de la publicité à partir de « partenaires » (on ne sait pas ce que cela veut dire) de Sharman Networks implantés dans le pays de l'utilisateur de Kazaa.

Sharman Networks insiste beaucoup sur la propreté de leur cookie mais s'empresse d'ajouter que leurs partenaires utilisent aussi des cookies qui leur échappent complètement.

Les publicités sur le site de Kazaa et dans le logiciel Kazaa sont gérées par Cydoor [1].

## Altnet – Licence et Vie Privée

Lire http://www.altnet.com/privacy
Les informations collectées sont, au moins

- Nom
- Adresse e-mail
- Age
- Sexe
- Mot de passe
- Références de carte bancaire et autres informations de facturation (adresse géographique…)
- Adresse IP (adresse de votre machine sur Internet) et autres informations d'identification certaine de votre machine (adresse MAC, GUID, systèmes d'espionnage sophistiqués sous couvert de gestion des droits numériques… dont, en toutes lettres dans le texte : « pour traquer les téléchargements et télé-déchargements de fichiers »… « pour forcer à respecter notre licence »… « pour protéger nos intérêts » « pour compter les points que vous avez échangés ou gagnés… »).

Ce dernier point, « compter les points », est très important car il est la « justification » ou « l'amende honorable et misérable » fournie par Altnet au scandale de son sous-réseau de P2P planqué dans le réseau utilisé par Kazaa, constitué des puissances volées de nos ordinateurs et ré-utilisées à son seul profit. Relire notre article Altnet – Brillant Digital – Kazaa [9].

Toutes les machines des internautes utilisateurs de Kazaa, ayant conservé l' « Opt In » d'Altnet, sont transformées en « zombies serveurs » du réseau Altnet de vente de musiques enregistrées. Altnet n'a besoin d'aucun serveur et d'aucune bande passante. Son réseau ne lui coûte rien. La puissance distribuée ainsi détournée dans un but mercantile est fantastiquement supérieure à celle, misérable, qu'arrivent à obtenir gracieusement, de la part d'internautes qui se sentent impliqués, de grands projets humanitaires comme le pliage des protéines [11], Seti@home [12] ou Décrypthon [13].

Cette déclaration « Vie privée » dit, en toutes lettres, que vous êtes profilé (votre profil est établi donc vous êtes espionné et on calcule vos centres d'intérêts et vos préférences) afin que leurs partenaires puissent vous abreuver de « la bonne pub au bon moment ».

Ces informations sont partagées avec d'autres si vous restez sur l'Opt In.

## Poursuite de l'installation de Kazaa

- Nous acceptons les deux licences et poursuivons l'installation (il n'y a pas le choix).
  - Kazaa Media Desktop End User License Agreement
  - Altnet PeerPoints Manager Package End User License Agreements.

- Nous acceptons d'installer le parasite « GAIN Network [2] » de Gator [3]

- Nous acceptons d'installer leur antivirus, BullGuard. En réalité il s'agit du téléchargement de BullGuard qui n'est pas installé à ce stade.

- Nous acceptons d'installer Skype (la téléphonie « gratuite »)

- Installation de Kazaa

- Lancement de Kazaa et exécution durant quelques minutes

- Fermeture de Kazaa

- Redémarrage

- Mise à jour de BullGuard (l'antivirus en version démo livré avec Kazaa qui cherche à le vendre avec son firewall et son outil de backup). Nous choisissons toutefois de ne pas installer BullGuard.

Durant l'installation, un certain nombre d'alertes sont émises par les outils installés. Elles sont présentées dans le tableau comparatif « On access », plus loin.

## *Conclusions sur Kazaa*


*Figure 42 – Kazaa affirme "No Spywares" sur son site*

Kazaa 3.0 est livré avec, le 23 janvier 2005 :

### Le cheval de Troie Kazaa

- Kazaa est l'archétype du Cheval de Troie. C'est une application ayant une activité apparente (utile ou futile) cachant en son sein des parasites. Le déploiement du Cheval de Troie sert au déploiement de la charge active embarquée. Il est catastrophique, en terme d'outils anti-trojans [(51)], de voir que seuls 3 d'entre eux signalent le parasite Kazaa, es qualité Cheval de Troie.
- Kazaa est un outil de P2P dont l'usage est en contradiction formelle avec les contrats de travail de l'universalité du monde du travail. Comment des outils commerciaux destinés à sécuriser les environnements professionnels peuvent-ils ne pas signaler sa présence ?
- Les objets introduits dans les ordinateurs avec Kazaa relèvent de la piraterie ou des parasites (virus. …). La présence de Kazaa sur une machine est une faille de sécurité majeure et relègue tous les outils anti-trojans [(51)] ne signalant pas sa présence au rang de gadgets à usage domestique. La présence de contenus piratés met le propriétaire (l'employeur…) hors la loi et l'expose aux poursuites prévues.
- Kazaa écrit, en toutes lettres, sur son site à http://www.kazaa.com/us/privacy/spyware.htm « Kazaa Media Desktop contains banner advertising **and the option to install other third party applications** in order to remain free to the user. »
  Kazaa dispose de la capacité de télécharger (downloader) et installer des applications sans notre consentement, sans que nous sachions de quoi il retourne et sans que nous puissions nous y opposer. Kazaa est donc un downloader (pas au sens du P2P) et doit être éradiqué.

### L'adware [(37)] et spyware [(38)] Gain [(2)] de Claria (ex Gator [(3)])

Il s'agit du plus important adware et spyware au monde. Moultes fois dénoncée sous son nom d'origine, Gator [(3)], la société a été obligée de changer de nom (Claria) pour tenter de se refaire une virginité avec les mêmes logiciels et le même réseau.
La déclaration de Kazaa, « NO SPYWARE », est mensongère.

## L'adware [37] et spyware [38] MyWay SearchBar

Alias MyWay Toolbar, My SpeedBar, MyWay Search Bar, MyWay myBar, MyWay toolbar.
C'est une barre de recherches qui s'installe en tant que BHO [32] dans Internet Explorer et, analysant vos mots clés, établit votre profil et vous inonde de bannières[33], pop-up[34], liens contextuels[35] et pratique la publicité intrusive[36].
Ils déclarent ne collecter aucune information lorsque nous n'utilisons pas leur service mais ne disent pas un mot de ce qu'ils collectent et de ce qu'ils en font lorsque nous utilisons leur service.
La déclaration de Kazaa, « NO SPYWARE », est mensongère.

## Altnet - L'adware[37] et spyware[38] TOPicks

Alias Spyware/Altnet
Cet adware est implanté par Altnet, en même temps que son zombie. S'implante sous forme de BHO dans Internet Explorer. Analyse en temps réel [27] les contenus vus durant votre navigation sur le Net pour vous profiler et orienter vos recherches vers des sites particulièrement ciblés (pas au sens de vos intérêts mais au sens de leurs intérêts, en fonction des relations commerciales qu'ils ont signées avec ces sites).
La déclaration de Kazaa, « NO SPYWARE », est mensongère.

## Altnet - Le zombie Altnet NetWork [31]

Un réseau de P2P privé et sécurisé, caché dans le réseau FastTrack, utilise les ressources (disques, mémoire ram, bande passante, puissance de calcul etc. …) des utilisateurs de Kazaa pour le profit commercial de Brillant Digital. La manière dont l'existence de cette zombiification de nos machines est portée à notre connaissance est particulièrement floue. Le fait que nos machines ne soient plus qu'un pion d'un immense réseau commercial privé, mondial, est complètement occulté.
Nota : le composant Altnet n'est plus caché à l'intérieur de la visionneuse de Brillant Digital mais est désormais incorporé dans Kazaa.

## Altnet – P2P Networking

C'est la gestion des droits DRM. Tout l'espionnage au profit des majors peut être attendu de cet outil d'une part pour assurer la rémunération d'Altnet dans sa démarche commerciale de vente de contenus téléchargeables payants (musiques, films, etc. …) mais aussi pour calmer ces mêmes majors outragées par l'usage du réseau FastTrack et intentant procès sur procès à Altnet et toute sa mouvance.

## L'adware[37], Spyware[38], KeyLogger[39] et Trojan[40] Twain-Tech

Alias Adware/MultiMPP [Panda], Adware/Twain-Tech [Panda], Trojan.Win32.Keyhost.e, Twain-Tech adware, Win32/Spy.BiSpy.C trojan [Eset]
S'installe en BHO dans Internet Explorer. S'exécute en mode furtif. Affiche des publicités, parfois de manière intrusive[36].
PestPatrol le classe également à KeyLogger et à Cheval de Troie
La déclaration de Kazaa, « NO SPYWARE », est mensongère.

## L'adware[37] et spyware[38] Cydoor[1]

Cydoor [1] revendique 55 millions d'ordinateurs pollués par sa technologie et 300.000 nouveaux ordinateurs par jour sont infestés par ses outils grâce auxquels il annonce fièrement diffuser plusieurs billions de publicités par mois dans le monde.
Collecte des données de tracking et des données démographiques (Genre, âge, centres d'intérêt, statut marital, salaire, code postal, pays, niveau d'éducation...)
La déclaration de Kazaa, « NO SPYWARE », est mensongère.

## L'adware AdDestroyer

Alias : Adware.AdDestroyer [Symantec], VirtualBouncer
Se connecte silencieusement à l'Internet après chaque redémarrage de votre ordinateur, sans votre consentement et sans que vous en ayez connaissance. Reste résident en tâche de fond sans votre permission lorsque vous quittez votre navigateur. Affiche des publicités en pop-up ou pop-under même hors connexion. Ne dispose d'aucune procédure de désinstallation dans Ajout/Suppression de programmes » ou ailleurs.

## ADS – Alternate Data Stream [42]

Sur les machines dont le système de fichiers est NTFS, Kazaa cache une petite chaîne de caractères de 26 octets, probablement un identificateur unique de type GUID [43] ou une clé de licence de sa version payante (sans publicité) dans un emplacement particulièrement discret (l'existence des ADS est quasiment inconnue). On la trouve attachée à kazaa_setup.exe (kazaa_setup.exe :zone.identifier).

## Hosts Hijack

A la fin du test Kazaa nous avons procédé à une installation d'une petite liste hosts [48] (celle de Spy Sweeper - il en existe d'autres, livrées avec SpyBot ou avec Spy Sweeper ou en libre service sur le site Assiste.com [48]). Nous avons ensuite procédé à une re-installation de Kazaa avec kazaa_setup.exe. Nous avons eu une alerte incontournable de l'installateur : « réparation » du « problème » ou abandon de l'installation. Nous avons donc autorisé la « réparation » et avons alors observé la liste hosts [48]. Toutes les lignes BrillantDigital, DoubleClick, Kazaa et b3d ont été taguées (inhibées, mises en commentaire).

Nous avons alors, à la main, redressé la liste hosts (ôté le signe « # » devant les lignes hijackées) avec Notepad (le bloc-notes de Windows) et re-démarré la machine avec lancement de Kazaa.exe. Même alerte : « réparation » du « problème » ou abandon de Kazaa.

Les hijackers sont donc kazaa.exe et kazaa_setup.exe et, encore une fois, la communication de Kazaa sur son site, « No Spyware », est mensongère. Kazaa protège ces spywares directement dans ses binaires.

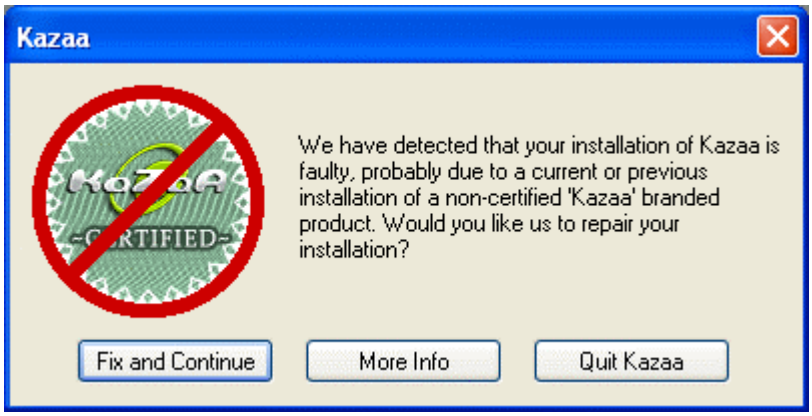


*Figure 43 – Kazaa propose (impose) le Hijack de hosts ou la sortie*

Remarque : lors de notre modification « à la main » de hosts avec le bloc-notes de Windows – (nous pensons que c'est un produit Microsoft ;o)) – Microsoft AntiSpyware nous a signalé cette tentative de modification (il a été le seul à le faire) et nous a demandé de confirmer cette action. D'autres utilitaires, comme SpyBot, permettent de protéger la liste hosts mais il faut le demander explicitement tandis que Microsoft AntiSpyware le fait par défaut et c'est la désactivation de cette surveillance qui peut être demandée. Malheureusement pour Microsoft AntiSpyware, lors du hijack par kazaa.exe et du hijack par kazaa_setup.exe, il n'a rien vu du tout. Ceci est extrêmement curieux.

Remarque : il est probable que sur des listes hosts beaucoup plus ambitieuses que celle de Spy Sweeper, qui est une toute petite liste hosts, d'autres blocages de domaines soient hijackés.

## SearchCentrix, CommonName, Grokster

Ces autres parasites sont détectés par l'un ou l'autre des anti-trojans [51]. Une analyse plus approfondie a permis de déterminer qu'il s'agit de faux positifs.

## Remarques sur Kazaa

1. La politique de communication de Kazaa s'est améliorée. Les documents disponibles (contrat de licence, Déclaration « Vie privée » etc. …) sont beaucoup plus proches de la réalité aujourd'hui qu'ils ne l'étaient lors de notre précédente analyse approfondie, il y a 2 ans (30).

2. La lecture de ces documents est préférable en anglais. Les versions françaises, lorsqu'elles existent, proviennent de traductions automatiques et sont incompréhensibles.

3. La lecture « entre les lignes » est un art. Parmi les lecteurs des imbuvables et innombrables contrats de licence de Kazaa et de tous ses produits tiers, lecteurs ô combien peu nombreux, quelle infime partie d'entre eux a compris l'ingénieux fonctionnement du réseau Altnet (détournement de la puissance de calcul de leurs ordinateurs) en apprenant qu'ils « gagnent des points » [(31)] ?

   La constitution du réseau de peer to peer Altnet, caché dans le réseau FastTrack, sur le dos des utilisateurs de Kazaa, s'institutionnalise par l'entrée d'AltNet sur le marché du contenu en téléchargement payant. AltNet, avec la puissance fabuleuse d'un tel réseau, qui ne lui coûte rien puisque ce sont nos ordinateurs qui sont zombiifiés, veut être un acteur majeur du téléchargement payant et donc, faisant d'une pierre deux coups, justifier (dirions-nous « légaliser » ?), aux yeux des majors, son réseau FastTrack de P2P sauvage. Le réseau AltNet pourrait être le plus puissant du monde et ne pas coûter un centime à Brillant Digital. C'est brillant !

4. Les parasites implantés dans Kazaa sont beaucoup moins nombreux que lors de notre analyse précédente mais sont de plus en plus subtils. Il faut rester méfiant : Plusieurs parasites sont de type « downloader » (téléchargeurs). Ils ont la capacité d'aller chercher, télécharger et installer d'autres programmes, plus tard, sans que l'analyse immédiate de l'implantation de Kazaa ne le laisse deviner.

5. Plusieurs parasites s'implantent sous forme de BHO qui est une technologie spécifique à Internet Explorer. L'usage d'un navigateur alternatif est recommandé (Mozilla Suite ou Firefox, par exemple)

# 14.Ressources

(1) Cydoor
http://assiste.free.fr/p/internet_attaquants/cydoor.php

(2) Gain (Gain Network)
http://assiste.free.fr/p/internet_attaquants/gator.php

(3) Gator
http://assiste.free.fr/p/internet_attaquants/gator.php

(4) Kazaa - Licence "Utilisateur final"
http://www.kazaa.com/us/terms2.htm

(5) Kazaa - Vie privée
http://www.kazaa.com/us/privacy/index2.htm

(6) Kazaa - vie privée (lien depuis l'installateur de Kazaa)
http://www.kazaa.com/us/privacy/privacy.htm

(7) Kazaa 3.0 US
http://www.kazaa.com/us/products/downloadKMD.htm

(8) Altnet "Vie privée" et Altnet "Termes et conditions d'utilisation".
http://www.altnet.com/privacy
http://www.altnet.com/support/terms

(9) Altnet - Brilliant Digital - Kazaa
http://assiste.free.fr/p/internet_attaquants/brillantdigital_altnet.php

(10) Projets de calcul distribué :
Cette page, qui traite d'un parasite s'attaquant à un projet de calcul distribué, explique ce qu'est le calcul distribué.
http://assiste.free.fr/p/internet_attaquants/iosdt_exe.php

(11) Calcul distribué : Comprendre le pliage des protéines, leur assemblage et les maladies qui y sont liées
http://www.alliancefrancophone.org/stanford/foldingathome/

(12) Calcul distribué : Seti@home - La vie intelligente extraterrestre
Le radio télescope d'Arecibo à Puerto Rico balaye le ciel. Chaque jour, 35 giga octets d'ondes radio électriques sont captées. Cela est tronçonné en petits bouts de 0.35 méga-octets soumis aux machines des internautes partageant leur puissance de calcul inutilisée. Cela s'appelle une « unité de travail ».
http://www.setifrance.org/index.php

(13) Calcul distribué : Décrypthon
http://www.infobiogen.fr/services/decrypthon/
Initié par l'AFM (Association Française contre les Myopathies) dans le cadre du Téléthon 2001, Décrypthon a été rendu possible par la contribution de plus de 75 000 volontaires qui ont prêté bénévolement la puissance de calcul de leurs PC. Grâce à cette mobilisation sans précédent en France, les calculs (comparaison de 559275 séquences protéiques, au moyen de l'algorithme d'alignement local de Smith-Waterman) ont pu être effectués en moins de deux mois.

(14) Mises à jour automatiques et contre-mesures
http://assiste.free.fr/p/internet_attaques/mises_a_jour_automatiques.php
http://assiste.free.fr/p/internet_contre_mesures/anti_mises_a_jour_auto.php

(15) Total Uninstall
http://assiste.free.fr/p/internet_utilitaires/total_uninstall.php

(16) ProcessGuard
http://assiste.free.fr/p/internet_utilitaires/processguard.php

(17) A² Free (gratuit)
http://assiste.free.fr/p/internet_utilitaires/a2.php

(18) Ad-aware se Personal (gratuit)
http://assiste.free.fr/p/internet_utilitaires/ad-aware_6_01.php

(19) Intermute SpySubTract
http://assiste.free.fr/p/internet_utilitaires/spysubtract.php

(20) Microsoft Antispyware (anciennement Giant Antispware)
http://assiste.free.fr/p/internet_utilitaires/microsoft_antispyware.php

(21) PestPatrol version 4
http://assiste.free.fr/p/internet_utilitaires/pest_patrol.php

(22) PestPatrol version 5 corporate
http://assiste.free.fr/p/internet_utilitaires/pest_patrol.php

(23) Spybot Search & Destroy (gratuit)
http://assiste.free.fr/p/internet_utilitaires/spybot_search_destroy.php

(24) Tauscan
http://assiste.free.fr/p/internet_utilitaires/tauscan.php

(25) TDS-3
http://assiste.free.fr/p/internet_utilitaires/tds.php

(26) The Cleaner
http://assiste.free.fr/p/internet_utilitaires/the_cleaner.php

(27) Temps-réel et Pseudo Temps-réel

- Temps réel pur
  Les modules « temps réel pur » (« On access ») réagissent à un événement du système d'exploitation (une demande d' « interruption système » telle une demande faite à Windows d'ouverture de fichier…). Ils suspendent l'exécution de cet événement pour effectuer une analyse de l'objet sollicité. Si celui-ci est, à leurs yeux, propre, le contrôle de l'objet est rendu au système et la tâche peut s'activer, sinon, l'utilisateur est informé afin qu'il décide quel sort réserver au parasite trouvé.
- Pseudo temps réel
  Les modules en « pseudo temps réel » n'ont pas la capacité de s'immiscer dans la gestion des interruptions système. Ce sont, en réalité, de petits scanners en temps différé, type « On demand », allégés en terme de capacités d'analyse comme en terme de base de signatures utilisée, bouclant en permanence (s'exécutant en continu) pour surveiller les processus qui se sont déjà lancés et quelques autres objets du système comme certaines clés de la base de registre. S'ils trouvent un objet hostile, ils vont alors proposer de tuer le processus (qui est déjà actif) ou de revenir à une situation préalable. Le TeaTimer de Spybot S&D est un module typiquement en pseudo temps réel. Lorsqu'il rencontre une modification de la base de registre sur une des clés qu'il surveille, il ne vous dit pas qu'une tentative de modification a lieu mais vous dit qu'une modification a eu lieu et vous demande si vous souhaitez la conserver ou restaurer les valeurs précédentes dont il a fait une copie au démarrage du système.

(28) MRUs (derniers utilisés - Most Recently Used)
http://assiste.free.fr/p/internet_utilitaires/mru_blaster.php

(29) Java, JVM de Microsoft, JVM de SUN, installation, désinstallation…
http://assiste.free.fr/p/internet_attaques/java.php
http://assiste.free.fr/p/internet_contre_mesures/anti_java.php

(30) Kazaa – Analyse des 17, 18 et 19 septembre 2002
http://assiste.free.fr/p/internet_attaquants/kazaa_spyware.php

(31) AltNet de Brillant Digital
http://assiste.free.fr/p/internet_attaquants/brilliant_digital.php

(32) BHO
http://assiste.free.fr/p/internet_attaques/bho.php
http://assiste.free.fr/p/internet_contre_mesures/anti_bho.php

(33) Bannières
http://assiste.free.fr/p/internet_attaques/bannieres.php
http://assiste.free.fr/p/internet_contre_mesures/anti_bannieres.php

(34) Pop-up
http://assiste.free.fr/p/internet_attaques/pop-up.php
http://assiste.free.fr/p/internet_contre_mesures/anti_pop-up.php

(35) Liens contextuels
http://assiste.free.fr/p/internet_attaques/smart_links.php
http://assiste.free.fr/p/internet_contre_mesures/anti_smart-links.php
http://assiste.free.fr/p/internet_attaques/smart_tags.php
http://assiste.free.fr/p/internet_contre_mesures/anti_smart-tag.php

(36) Publicité intrusive
http://assiste.free.fr/p/internet_attaques/publicite_intrusive.php
http://assiste.free.fr/p/internet_contre_mesures/anti_publicite_intrusive.php

(37) Adware
http://assiste.free.fr/p/internet_attaques/adware.php

(38) Spyware
http://assiste.free.fr/p/internet_attaques/spyware.php

(39) KeyLogger
http://assiste.free.fr/p/internet_attaques/keylogger.php

(40) Trojans
http://assiste.free.fr/p/internet_attaques/trojan.php

(41) Points de restauration du système (Windows ME et Windows XP)
http://assiste.free.fr/p/comment/activer_desactiver_points_restauration.php

(42) ADS – Alternate Data Stream
http://assiste.free.fr/p/internet_attaques/ads_alternate_data_stream.php

(43) GUID
http://assiste.free.fr/p/internet_attaques/guid_identificateur.php

(44) HashCode MD5 des fichiers
http://assiste.free.fr/p/internet_utilitaires/summerproperties.php

(45) Outils offerts par l'auteur de SpyBot
http://newpages.safer-networking.org/index.php?page=tools

(46) Anti-Logithèque - Les faux utilitaires de sécurité et les sites et utilitaires crapuleux
http://www.spywarewarrior.com/rogue_anti-spyware.htm
http://assiste.free.fr/p/faux_utilitaires/faux_utilitaires_frameset.php

http://www.pcworld.com/news/article/0,aid,118362,00.asp

(47) Téléchargeur (downloader)
http://assiste.free.fr/p/internet_attaques/downloader.php

(48) Liste hosts
http://assiste.free.fr/p/internet_contre_mesures/hosts.php

(49) Spy Sweeper
http://assiste.free.fr/p/internet_utilitaires/spy_sweeper.php

(50) A² - Est-ce bien raisonnable ?
http://assiste.forum.free.fr/viewtopic.php?t=3506

(51) Les anti-trojans
http://assiste.free.fr/p/familles/anti_trojans.php
http://assiste.free.fr/p/familles/anti_trojans_gratuits.php
http://assiste.free.fr/p/frameset/anti_trojans_en_ligne.php

(52) Les antivirus
http://assiste.free.fr/p/familles/antivirus.php
http://assiste.free.fr/p/familles/antivirus_gratuits.php
http://assiste.free.fr/p/antivirus_gratuits_en_ligne/antivirus_en_ligne.php

(53) Calendar of Updates
http://www.dozleng.com/updates/index.php?act=calendar

(54) Liste de chevaux de Troie
http://assiste.free.fr/p/internet_les_listes/vecteurs_spyware_longue.php

(55) Adware
http://assiste.free.fr/p/internet_attaques/adware.php

(56) Backdoor
http://assiste.free.fr/p/internet_attaques/backdoor.php

(57) Binder
http://assiste.free.fr/p/internet_attaques/binder.php

(58) Dialer
http://assiste.free.fr/p/internet_attaques/dialer.php

(59) Hijacker
http://assiste.free.fr/p/internet_attaques/hijack_hijacker_hijacking.php

(60) Keylogger
http://assiste.free.fr/p/internet_attaques/keylogger.php

(61) Killer
http://assiste.free.fr/p/internet_attaques/killer.php

(62) Packer
http://assiste.free.fr/p/internet_les_listes/liste_packer.php

(63) Password Stealer
http://assiste.free.fr/p/internet_attaques/mots_de_passe.php

(64) Password Attacker
http://assiste.free.fr/p/internet_attaques/mots_de_passe.php

(65) Password Cracker
http://assiste.free.fr/p/internet_attaques/mots_de_passe.php

(66) Leak Tests
http://assiste.free.fr/p/internet_essentiel/on_line_evasion.php

(67) Probe tools
http://assiste.free.fr/p/internet_les_listes/liste_probe_tool.php

(68) RAT – Remote Administration Tool
http://assiste.free.fr/p/internet_attaques/rat_remote_admin_tool.php

(69) Spyware
http://assiste.free.fr/p/internet_attaques/spyware.php

# 15.Révisions de ce document

| Version | Date | Commentaire |
|---|---|---|
| 01 | 10 février 2005 | Première publication du document initial – Quelques infos à ajouter (dont pour The Cleaner) |
| 01.01 | 12 février 2005 | Corrections mineures - Fautes de frappes, échelle d'un graphique ajustée, liens cliquables. |
| 01.02 | 27 février 2005 | Correction d'une erreur de mise en page et de l'exemple de PhotoFiltre qui n'est pas un cheval de Troie mais pâtit d'un faux positif de PestPatrol. |