LES DOSSIERS TECHNIQUES

PROGRAMMES POTENTIELLEMENT INDÉSIRABLES

-

SPYWARE

Espace Menaces - Groupe Spyware

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS

Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Table des Matières

REMERCIEMENTS ..... **I**

1 INTRODUCTION **2**

2 QU'EST QU'UN PROGRAMME INDESIRABLE ? **4**

2.1 DEFINITIONS 4

2.2 LANGAGE COURANT 6

2.3 ASPECT QUANTITATIF 6

2.4 TAUX DE PRESENCE AU NIVEAU MONDIAL 8

2.5 TAUX DE PRESENCE CHEZ LES PARTICULIERS 10

2.6 TAUX DE PRESENCE EN ENTREPRISE 11

3 ASPECTS TECHNIQUES ET FINANCIERS **13**

3.1 PROVENANCE DES PUPS LIES A L'ADMINISTRATION ET A LA SURVEILLANCE DES SYSTEMES INFORMATIQUES 13

3.2 PROVENANCE DES PUPS SE VOULANT HUMORISTIQUES 13

3.3 PROVENANCE DES PUPS LIES AU MONDE DE LA PUBLICITE, DU COMMERCE ET DU MARKETING 13

3.4 ASPECTS TECHNIQUES DES PUPS LIES AU MONDE DE LA PUBLICITE, DU COMMERCE ET DU MARKETING 15

3.4.1 Installation *15*

3.4.2 Chargement *16*

3.5 CIRCUITS FINANCIERS LEGAUX 17

3.6 CIRCUITS FINANCIERS MALVEILLANTS 21

3.7 QUELQUES SOCIETES SOUVENT MONTREES DU DOIGT 23

4 ORGANISATION DE LA LUTTE ANTI-SPYWARE **24**

4.1 DIMENSION HUMAINE – MESSAGE AUX UTILISATEURS 24

4.2 DEONTOLOGIE DES ANNONCEURS 24

4.3 LES ORGANISMES OFFICIELS OU INDEPENDANTS 25

4.4 ANTI-VIRUS & ANTI-SPYWARE 27

5 CONCLUSION **29**

© CLUSIF 2008

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Michel	**BERTIN**	
Olivier	**GUERIN**	*CLUSIF*
Rémy	**LE CHEVALIER**	*LCS Conseil*
François	**PAGET**	*McAfee*
Jean-Charles	**SIMON**	*Michelin*

1 INTRODUCTION

Les programmes potentiellement indésirables (en anglais – PUPs : Potentially Unwanted Programs) sont distribués par des sociétés commerciales ou des individus qui n'ont pas la volonté de nuire. Lorsqu'ils ne sont pas volontairement installés ou lorsqu'ils sont détournés de leur usage, ces programmes peuvent perturber l'utilisateur, secrètement modifier le niveau de sécurité de son système et porter atteinte à la confidentialité de ses activités et de ses données.

Sans pour autant en minimiser l'importance, les entreprises s'inquiètent moins que par le passé des nuisances apportées par les programmes potentiellement indésirables. La protection antivirale qui inclut souvent celle des PUPs et la surveillance globale de la navigation Internet protègent les entreprises. Les seuls éléments qu'elles craignent sont les adware (qui sont communément cités sous la dénomination de spyware).

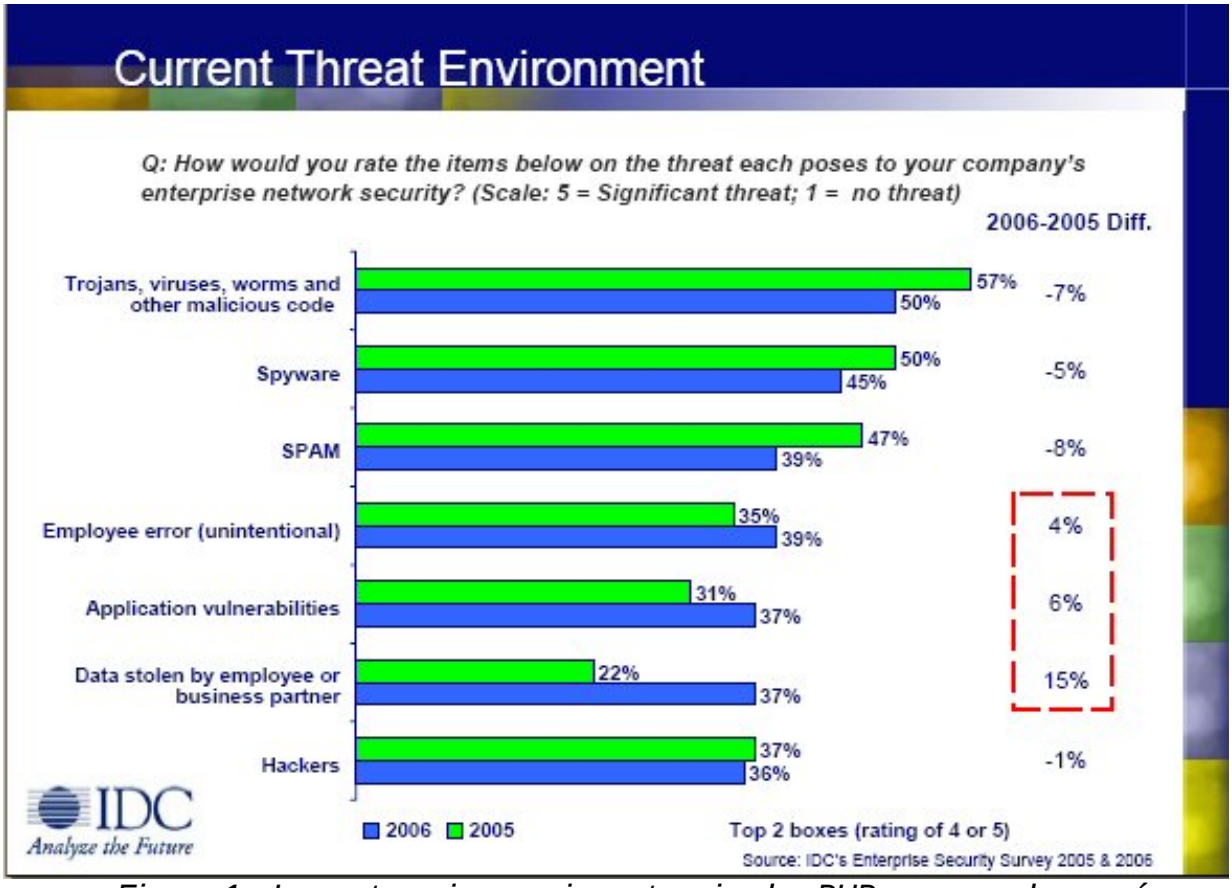

Figure 1 : Les entreprises craignent moins les PUPs que par le passé

Les particuliers sont, par contre, généralement inconscients du danger. Selon une étude IDC, les trois-quarts des machines connectées à Internet contiennent un tel programme [1].

Bien que la navigation sur Internet et toutes les activités menées en local sur ces machines soient perturbées, les propriétaires ne font souvent pas le lien entre ce type d'intrus et leurs problèmes. Ils s'imaginent attaqués par des virus inconnus ou sujets à des bogues à répétition.

Ce document se veut en tout premier lieu pédagogique. Alors que les caractéristiques et les modes de fonctionnement des divers programmes malveillants (vers, virus, chevaux de Troie) semblent maintenant relativement connus du public, il n'en est pas de même pour les programmes potentiellement indésirables. Les notions d'adware et de spyware sont souvent floues ou incorrectes et les deux prochains chapitres sont donc là pour en préciser les définitions et les modes de propagation. La seconde partie de ce document aborde les quelques spécificités liées à l'organisation de la lutte anti-spyware et signale quelques pièges à éviter.

[1] Worldwide Antispyware 2006-2010 Forecast and Analysis: Boom or Bust?, June 2006 : http://www.idc.com/getdoc.jsp?containerId=202020

2 QU'EST QU'UN PROGRAMME INDESIRABLE ?

2.1 Définitions

Même s'ils sont détectés par les logiciels dits « anti-virus », les PUPs ne doivent pas être confondus avec des programmes malveillants (malware). Ce sont des programmes distribués par des sociétés commerciales ou des individus qui n'ont pas la volonté de nuire. Ce sont des codes non autoreproducteurs.

Le caractère indésirable peut être mis en évidence :

- par la manière dont ces programmes sont implantés (volontairement ou à l'insu de l'utilisateur),
- par l'existence de fonctionnalités perturbatrices ou inconnues (dysfonctionnements des ordinateurs, utilisateurs inondés d'annonces publicitaires),
- par l'absence d'un processus de désinstallation,
- par une baisse non volontaire du niveau de sécurité du navigateur,
- par le fait d'un détournement de finalité et d'une utilisation malveillante,
- par une atteinte à la confidentialité des activités et des données (récupération d'infos personnelles).

Il existe 3 grands groupes de PUPs :

1. **PUPS liés au monde de la publicité, du commerce et du marketing**
    - Les logiciels d'affichage publicitaire (adware). Également dénommés pubiciel[2] en français, ces programmes dirigent des publicités ciblées vers les ordinateurs qui les contiennent. Ils observent les habitudes de navigation des internautes afin de leur fournir des offres adaptées à leur profil.
    - Les logiciels d'extension pour navigateur. Ils interagissent avec celui-ci afin d'offrir des fonctionnalités nouvelles (affichage de formats graphiques particuliers, lecteurs multimédia, etc.). Certains d'entre eux peuvent contenir des fonctionnalités dangereuses si elles ne sont pas désirées (surveillance de l'activité ou altération des données). On retrouve dans cette famille : des contrôles ActiveX, des outils d'aide à la navigation (Browser Helper Objects ou BHO) et des modules Mozilla Firefox.
    - Les fichiers de mémoire de visite et de surveillance (cookies et tracking cookies). Les cookies sont des groupes d'informations

[2] Le néologisme pubiciel se rapporte aux adware (logiciel publicitaire) alors que le néologisme publiciel concerne les logiciels publics (public domain software).

stockées dans de petits fichiers texte que certains serveurs web déposent sur l'ordinateur qui les visite. Ils permettent de garder une trace de chaque passage et de mémoriser quelques préférences de navigation.

- Les logiciels de connexions téléphoniques. Également connus sous la terminologie anglaise *dialers*, ils redirigent les connexions Internet vers des fournisseurs d'accès particuliers en utilisant le réseau téléphonique commuté. Ils deviennent dangereux, dès que cette redirection se fait sans le consentement de l'utilisateur (par exemple vers des numéros fortement surtaxés).

2. PUPS liés à l'administration et à la surveillance des systèmes informatiques

- Les logiciels de surveillance. Alors qu'ils sont toujours proposés pour des buts louables, tels que le contrôle parental, ils sont parfois détournés de leur but premier et utilisés à des fins d'espionnage. On retrouve dans cette catégorie les spyware. Les uns se rapprochent des adware, mais ne se contentent pas de rediriger des publicités ciblées. Ils transmettent des informations nominatives et personnelles pour poursuivre leur approche marketing par courrier électronique, postal ou par téléphone. Les sociétés collectrices peuvent ensuite monnayer les fichiers constitués. Les autres sont de véritables logiciels espions capables d'enregistrer secrètement et de retransmettre les opérations effectuées sur l'ordinateur sans que son utilisateur en ait connaissance.

- Les logiciels d'analyse de sécurité. Citons à titre d'exemple les logiciels de cassage de mot de passe ou les scanneurs de port. Utiles à l'administrateur système, ils sont une menace dès qu'ils sont employés de manière détournée.

- Les outils de contrôle et/ou d'administration à distance (Remote Access Tools - RAT). Utilisés à bon escient et par des administrateurs réseau compétents, ils permettent le contrôle à distance de machines éloignées. Entre les mains de pirates informatiques, ces outils deviennent éminemment dangereux.

- Les logiciels d'aide à la modification du système. La plupart d'entre eux sont clairement malveillants. Certains outils de redirection (*hijackers*) et de dissimulation (*rootkits*) sont cependant parfois utilisés de manière régulière.

3. PUPS se voulant humoristique

- Les plaisanteries (en anglais : *jokes*). Ces programmes totalement inoffensifs peuvent parfois troubler ou irriter l'utilisateur lorsque celui-ci les rencontre sans l'avoir souhaité.

2.2 Langage courant

L'industrie anti-virus et les associations professionnelles font circuler des définitions précises qui se rapprochent de celles données ci-dessus. La presse généraliste et le public ont tendance à n'utiliser que le terme spyware.

Parmi ces regroupements d'experts, citons l'Anti-Spyware Coalition (ASC). Sous l'égide de l'association américaine Center for Democracy and Technology (CDT), elle a pour objectif de définir clairement ce que sont ces programmes. Elle s'applique à mettre au point une terminologie commune en vue d'éclairer les usagers sur les pratiques à tenir pour s'en protéger.

L'association espère qu'une meilleure définition de ces termes permettra aux internautes de mieux savoir à quel type de menace ils s'exposent. Cette connaissance devrait leur permettre d'utiliser plus judicieusement les logiciels de sécurité informatique mis à leur disposition. L'ASC a ainsi son propre glossaire [3].

Conscients que le terme spyware est maintenant très largement détourné de son sens exact, les membres de l'association ont décidé, pour les documents techniques, d'utiliser la mention [spyware(narrow)] lorsqu'il fallait l'employer dans son sens strict (en anglais « *narrow* »). Sachant aussi qu'il est impossible d'éviter des connotations plus larges dans des utilisations généralistes ou populaires, elle a pris acte de l'existence d'une interprétation plus générale qui regroupe alors l'ensemble des programmes potentiellement indésirables. Le nom de l'association utilise ainsi le terme spyware, tout comme il est repris dans bon nombre de logiciels anti-spyware qui ne s'attachent pas uniquement à détecter et éliminer les [spyware(stricts)]. Dans ce document, le terme spyware n'est jamais utilisé dans un sens large (sauf au niveau du titre du document), mais toujours dans son sens strict.

2.3 Aspect quantitatif

La comptabilisation des PUPs est très difficile à obtenir car les critères qui les amènent à être – ou non - détectés par un anti-virus sont parfois subjectifs. Une société peut très bien considérer un programme comme un PUP alors qu'une autre n'en verra pas l'utilité.

A la fin 2007, l'ensemble des programmes indésirables est environ 16 fois moins nombreux que les malware soit 360 000 programmes malveillants pour 21 600 PUPS. Aujourd'hui inefficaces du fait des nouvelles technologies d'accès sur le réseau Internet (ADSL, câble, etc.), les logiciels de connexion téléphonique malveillants (dialers) ont été minimisés dans cette statistique. Leur nombre dépasse cependant les 300 000 bien qu'une majorité d'entre eux provienne de sources communes, conditionnée par divers compacteurs qui en augmentent artificiellement le nombre. Seules les têtes de variantes sont ici comptabilisées.

---

[3] Anti-Spyware Coalition – Glossaire : http://www.antispywarecoalition.org/documents/glossary.htm

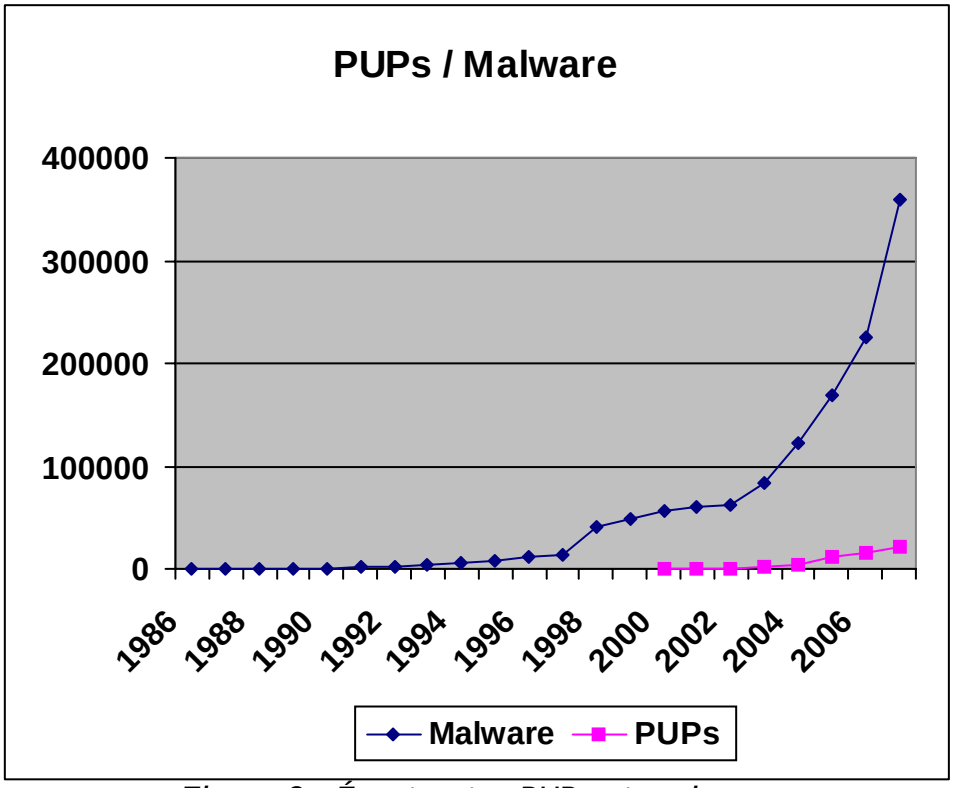

Figure 2 : Écart entre PUPs et malware

A la différence des virus et des chevaux de Troie, l'adware ou le spyware est un ensemble logiciel qui comporte plusieurs fichiers et nécessite un processus d'installation à part entière. Ces deux sous-familles représentent environ la moitié des PUPs.

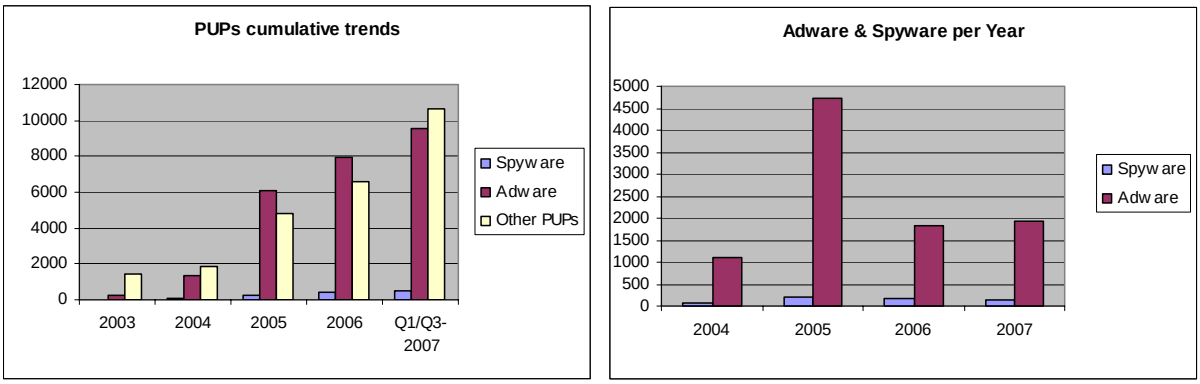

Figure 3 : Écart entre adware, spyware et dialers

2.4 Taux de présence au niveau mondial

La figure ci-dessous est une capture d'écran de la carte mondiale des infections accessible depuis le site McAfee [4].

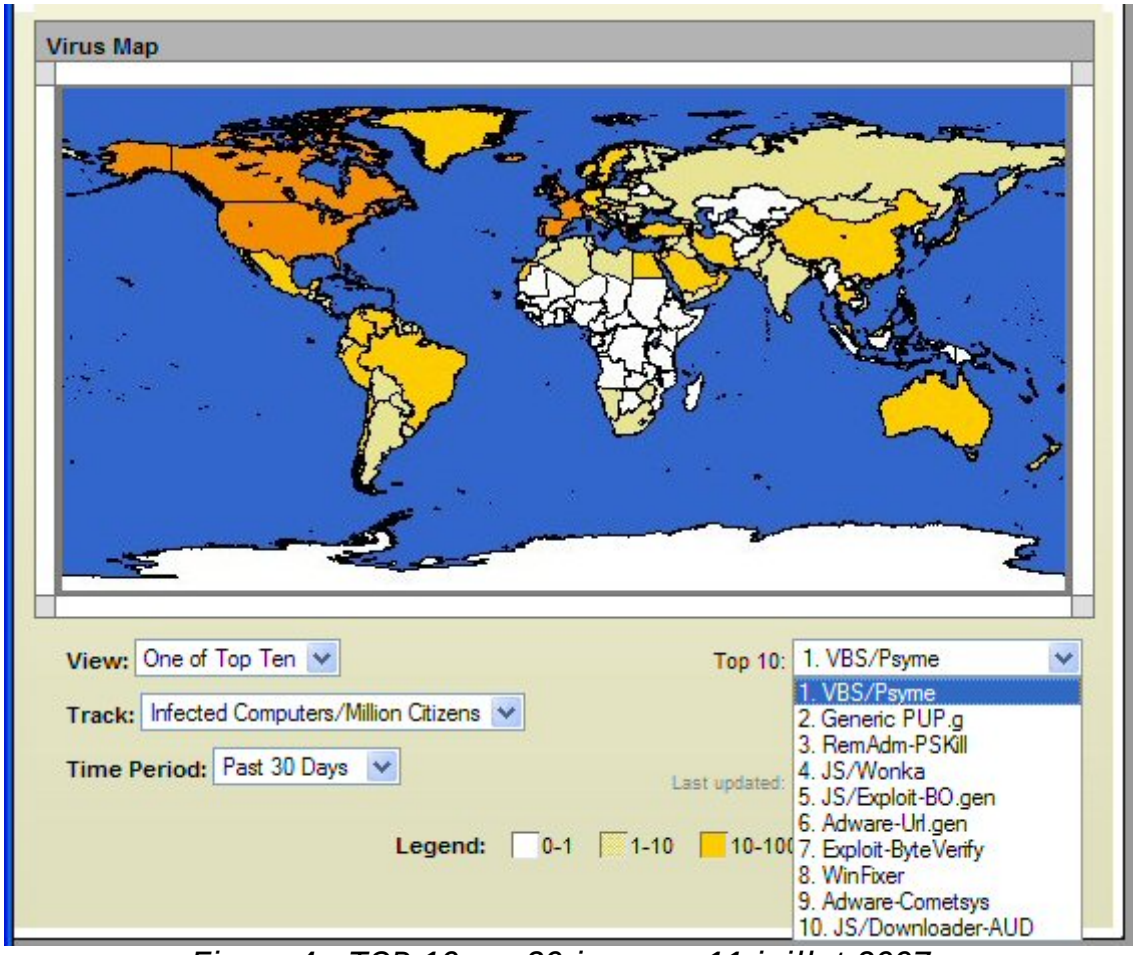

Figure 4 : TOP-10 sur 30 jours au 11 juillet 2007

Elle date du 11 juillet 2007 et présente, à un instant donné, le « TOP-10 temps réel » des 30 derniers jours. Outre les 3 PUPS (rangs 2, 6 & 9), tous les exploits et le downloader sont connus pour leur utilisation dans l'installation d'adware (et non pas simplement de programmes malveillants). Même si parfois quelques virus et chevaux de Troie entrent temporairement dans ce TOP-10, cet état de fait dure maintenant depuis de nombreux mois.

[4] McAfee Virus Map : http://mastdb2.mcafee.com/VirusMap3.asp?Cmd=Map&b=IE&ft=JPEG&lang=en

Rang	Désignation	Type
1	VBS/Psyme	Exploit
2	JS/Exploit-BO.gen	Exploit
3	Exploit-ANIfile.c	Exploit
4	Exploit-MS06-014	Exploit
5	RemAdm-PSKill	PUP
6	Adware-Url.gen	PUP
7	JS/Wonka	Exploit
8	Winfixer	PUP
9	JS/Downloader-AUD	Downloader
10	Exploit-Byte Verify	Exploit

Tableau 1 : TOP-10 sur 30 jours au 16 avril 2007

De son côté, Panda Software (qui n'a pas d'exploit dans son TOP-10) annonçait que les adware représentaient 31% des infections en indiquant que :

> « *[s'ils] sont à l'origine d'autant d'infections, c'est principalement en raison de leurs méthodes de propagation. Dernièrement, nous avons constaté une augmentation sensible du nombre de pages web malveillantes qui installent des adware sur les ordinateurs en exploitant des failles de sécurité. Ces codes malicieux s'installent automatiquement lorsque les utilisateurs visitent ces pages, sans même qu'ils aient à accepter les conditions générales. Comme les utilisateurs n'étaient même pas informés de leur installation, ces malware sont plus difficiles à détecter et ils peuvent rester plus longtemps sur les ordinateurs.* »

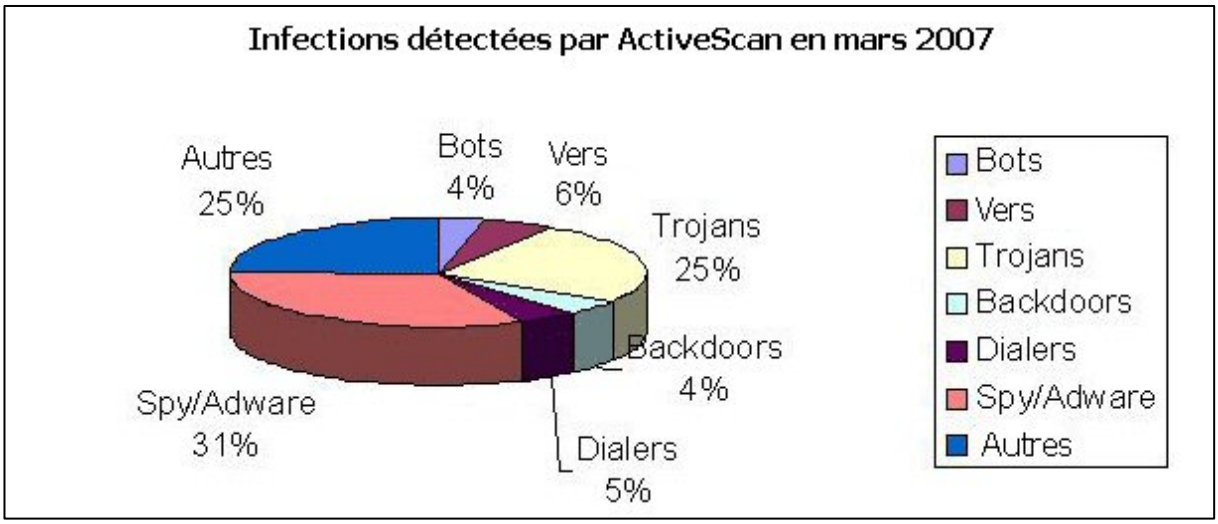

Figure 5 : Statistiques Panda pour Mars 2007

2.5 Taux de présence chez les particuliers

En 2004, une étude menée au Pays-Bas et en Belgique a montré le fort degré de présence de programmes indésirables dans les ordinateurs familiaux [5]. L'enquête a été réalisée auprès de 200 personnes suite à un appel lancé à travers les journaux.

Le rapport révèle que 76% des ordinateurs analysés contenaient un programme malveillant ou indésirable avec une forte prédominance de ces derniers (adware/spyware et dialers).

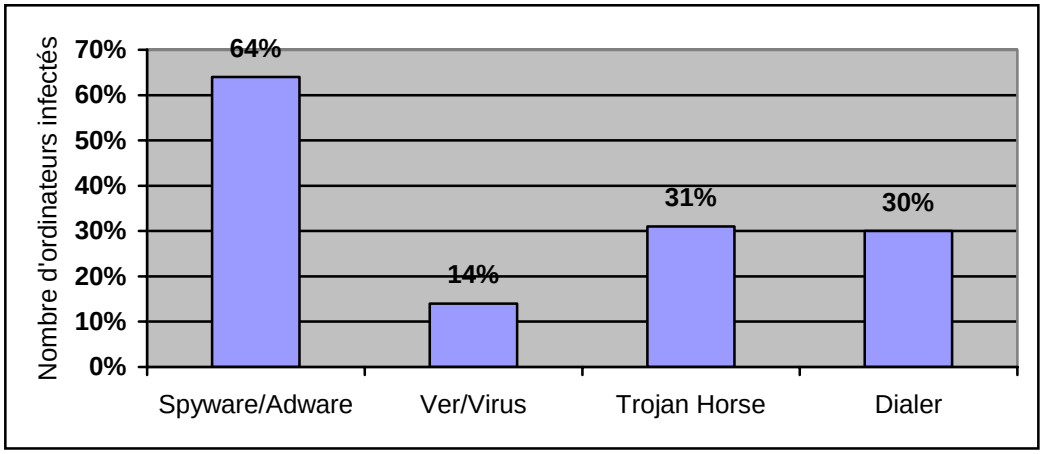

Figure 6 : Degré d'infection

Sur les dix éléments affectant le plus grand nombre d'ordinateurs, neuf sont des adware, avec en tête la variante Adware.Binet (23%). Le seul élément qui n'est pas un adware est un dialer. Il n'y a aucun malware dans ce Top-10.

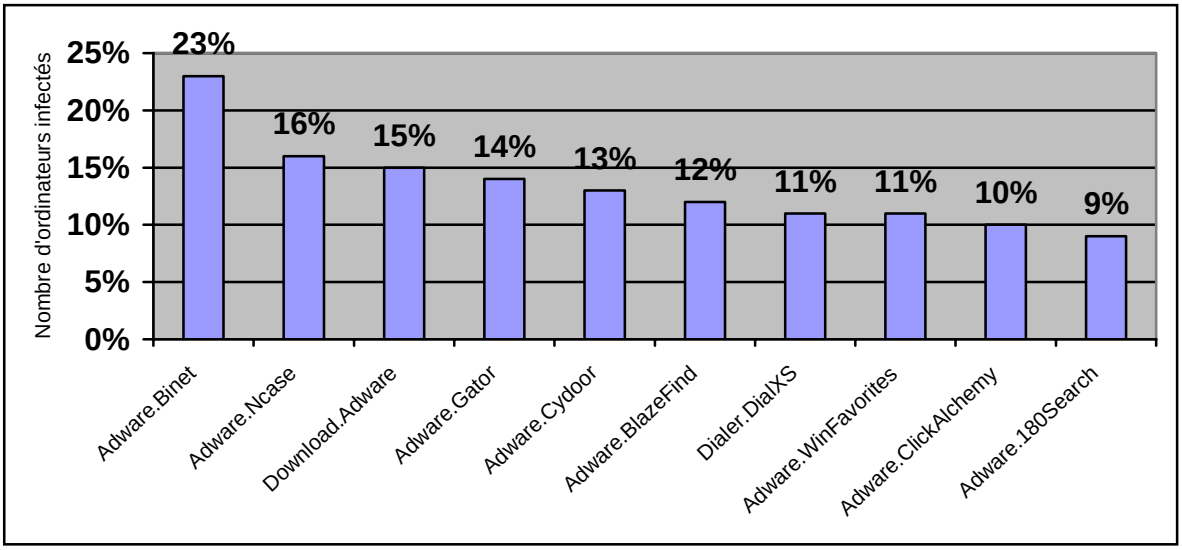

Figure 7 : Prévalence PUPs

[5] Spyware et autres malware dans le Benelux : http://www.expatica.com/be/spyware-survey.pdf

On retrouve ce fort pourcentage de programmes indésirables dans l'étude menée par la société Webroot [6]. Malgré un léger mieux en 2005, les six premiers mois de 2006 se sont avérés tout aussi catastrophiques. Même si les virus ne sont pas pris en compte dans cette étude, la prédominance des programmes indésirables face aux programmes malveillants est ici aussi observable.

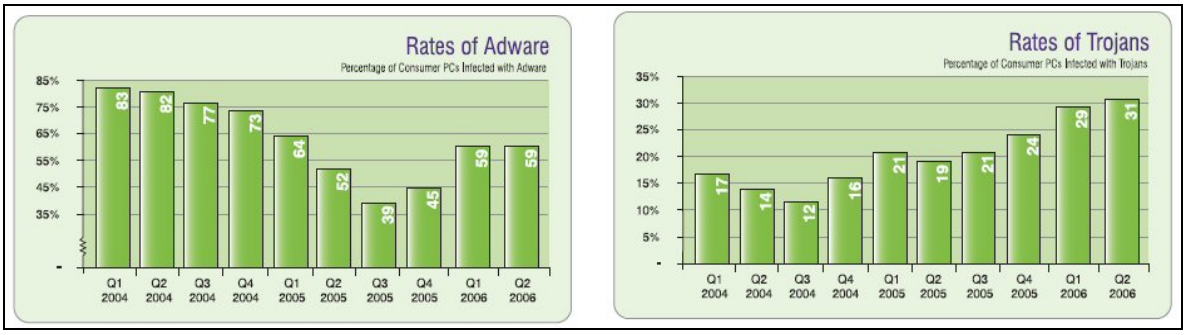

Figure 8 : Niveau d'infection chez les particuliers pour 100 PC (Webroot)

2.6 Taux de présence en entreprise

Alors que le particulier est souvent mal protégé des PUPs, en entreprise, la sécurisation des postes de travail se fait à un niveau global : malware et programmes indésirables confondus. La présence de ces derniers s'en trouve limitée. Ils sont, eux aussi, stoppés aux portes de l'entreprise et leur taux de pénétration se confond souvent avec celui des programmes malveillants. L'étude Webroot citée ci dessus montre cependant, que tout comme pour les particuliers, les PUPs sont plus fréquemment rencontrés que les chevaux de Troie.

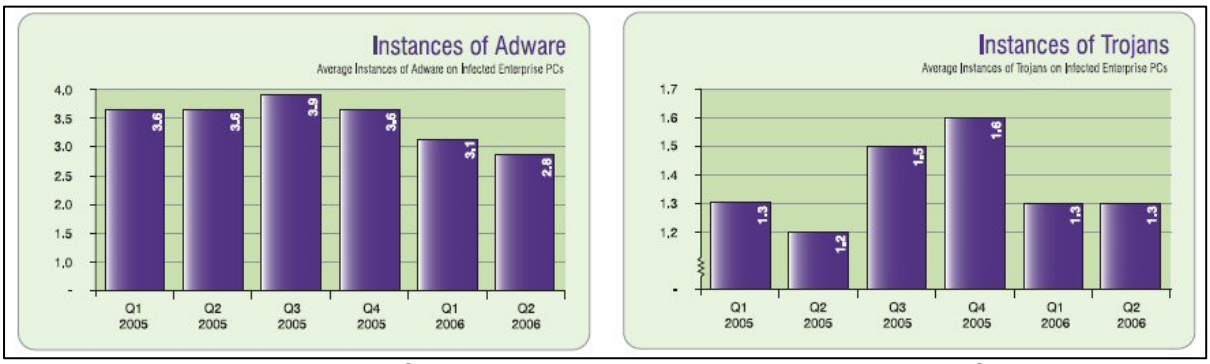

Figure 9 : Taux de présence pour un PC d'entreprise infecté (Webroot)

[6] State of Spyware – Q2-2006 : http://h30307.www3.hp.com/pdf/SOS_Q206_USA.pdf

Une seconde statistique du même éditeur place les adware avant les virus [7].

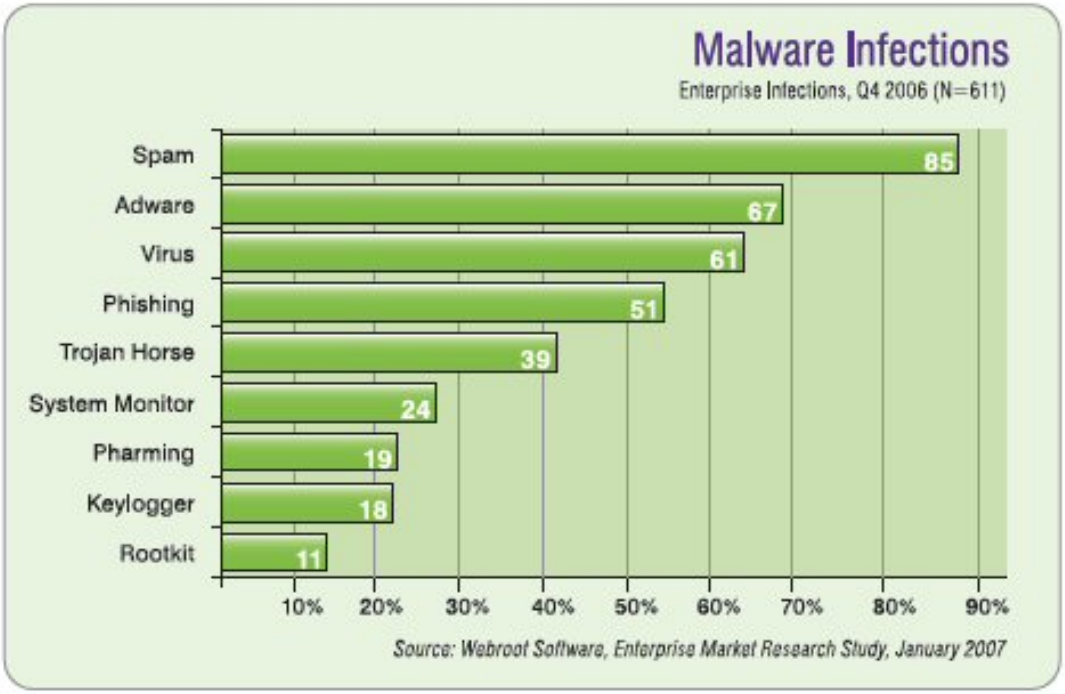

Figure 10 : Statistiques d'infections (Webroot)

[7] State of Internet Security Q107 : http://www.avsec.hu/downloads/webroot/Webroot-State-of-Inetrent-Security-Report-Q107.pdf

3 ASPECTS TECHNIQUES ET FINANCIERS

3.1 Provenance des PUPS liés à l'administration et à la surveillance des systèmes informatiques

Il s'agit le plus souvent de copies pirates de logiciels commerciaux de sécurité trouvées sur des sites spécialisés. Ceux qui les téléchargent les utilisent ensuite de façon détournée.

3.2 Provenance des PUPS se voulant humoristiques

On les trouve sur des sites dédiés et les internautes les diffusent fréquemment via le courrier électronique.

3.3 Provenance des PUPS liés au monde de la publicité, du commerce et du marketing

Les PUPS liés au monde de la publicité, du commerce et du marketing sont souvent présentés comme des utilitaires destinés à faciliter la navigation sur Internet ou à en agrémenter certaines activités. Ils peuvent aussi être jumelés à des programmes gratuits qui ne s'installeront qu'après acceptation d'une implantation combinée aboutissant à une mise en place :

- intégrée, avec des routines incorporées à l'application principale,
- externalisée, avec une installation menée parallèlement à celle de l'application principale.

L'accès à certains sites Internet spécifiques peut être également assujetti à l'installation d'un de ces logiciels. Comme préalable à la connexion, on impose la mise en place du produit. L'existence et la finalité de ces PUPs sont généralement mentionnées, mais souvent dans des termes ambigus et toujours en langue anglaise (ce qui perturbe énormément les utilisateurs non anglophones). L'installation peut aussi se faire de manière plus ou moins silencieuse sans véritable accord préalable dès que l'on visite des sites à la déontologie douteuse. Ce mode d'installation plus ou moins furtif sert parfois de critère de détection aux éditeurs de produit de sécurité.

En résumé, les principaux vecteurs d'introduction sont :

- les logiciels gratuits ou en démonstration téléchargés sur Internet ou diffusés sur des supports joints à certaines revues. On se méfiera plus particulièrement :
    - o des outils d'aide à la navigation,
    - o des logiciels de téléchargement et de partage de ressources (poste à poste / peer to peer),
    - o des économiseurs d'écran, des packs gratuits d'émoticons (*smileys*),

    - de certains jeux gratuits,
    - de logiciels de contournement de sécurité (hack, crack).
- les sites à risque :
    - stars et célébrités,
    - charme et sites pour adulte,
    - logiciels gratuits,
    - jeux d'argent (casinos),
    - monde underground.
- Les pièces jointes à du courrier électronique indésirable (spam) ou provenant des messageries instantanées,
- les procédures d'enregistrement en ligne des licences de logiciels ou celles permettant l'accès à des zones de navigation privées,
- les réseaux poste à poste,
- les virus et les chevaux de Troie qui peuvent être chargés de les déposer sur la machine.

La rumeur veut que les sites pour adultes et à caractère pornographique soient les plus prolifiques en matière de diffusion d'adware. L'étude de l'Université de Washington contredit cette affirmation [8]. L'analyse des résultats démontre qu'un site de jeu sur cinq est dangereux (20%). Viennent ensuite les sites de musique, de fond d'écran, de célébrité. Les sites pour adultes n'arrivent qu'en cinquième position.

	adult	celebrity	games	kids	music	news	pirate	wallpaper	c|net	random
URLs crawled	3,465,024	3,131,497	872,686	733,648	3,421,796	458,079	3,042,390	678,506	193,118	5,858,619
domains crawled	157	144	125	183	220	20	311	125	1	1,356
executables found	158	153	4,872	112	4,218	19	3,422	6,860	1,944	2,000
domains with executables	26 (16.6%)	28 (19.4%)	76 (60.8%)	24 (13.1%)	72 (33.2%)	7 (35.0%)	111 (36.0%)	51 (40.8%)	1 (100%)	102 (7.5%)
infected executables	18 (11.4%)	25 (16.3%)	272 (5.6%)	3 (2.7%)	149 (3.5%)	0 (0%)	74 (2.2%)	789 (11.5%)	6 (0.3%)	6 (0.3%)
infected domains	12 (7.5%)	11 (7.6%)	25 (20.0%)	3 (1.6%)	24 (11.4%)	0 (0%)	21 (7.1%)	12 (9.6%)	1 (100%)	5 (0.4%)
unique spyware programs	12	10	32	5	55	0	43	34	5	2

Figure 11 : Executable infections across Web categories (UofW)

[8] A Crawler-based Study of Spyware on the Web : http://www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf

A coté des sites généralistes, de nombreux sites ne sont en fait que des sous-marins travaillant directement pour des sociétés publicitaires. Certaines changent régulièrement de nom ou sont liées entre elles par des accords plus ou moins secrets. Il est possible de se faire une idée de ces ramifications en interrogeant le site d'analyse McAfee SiteAdvisor [9]. Outre l'outil d'aide à la navigation qu'il propose, il offre un aperçu des liens commerciaux qui ont été repérés au moment de l'analyse.

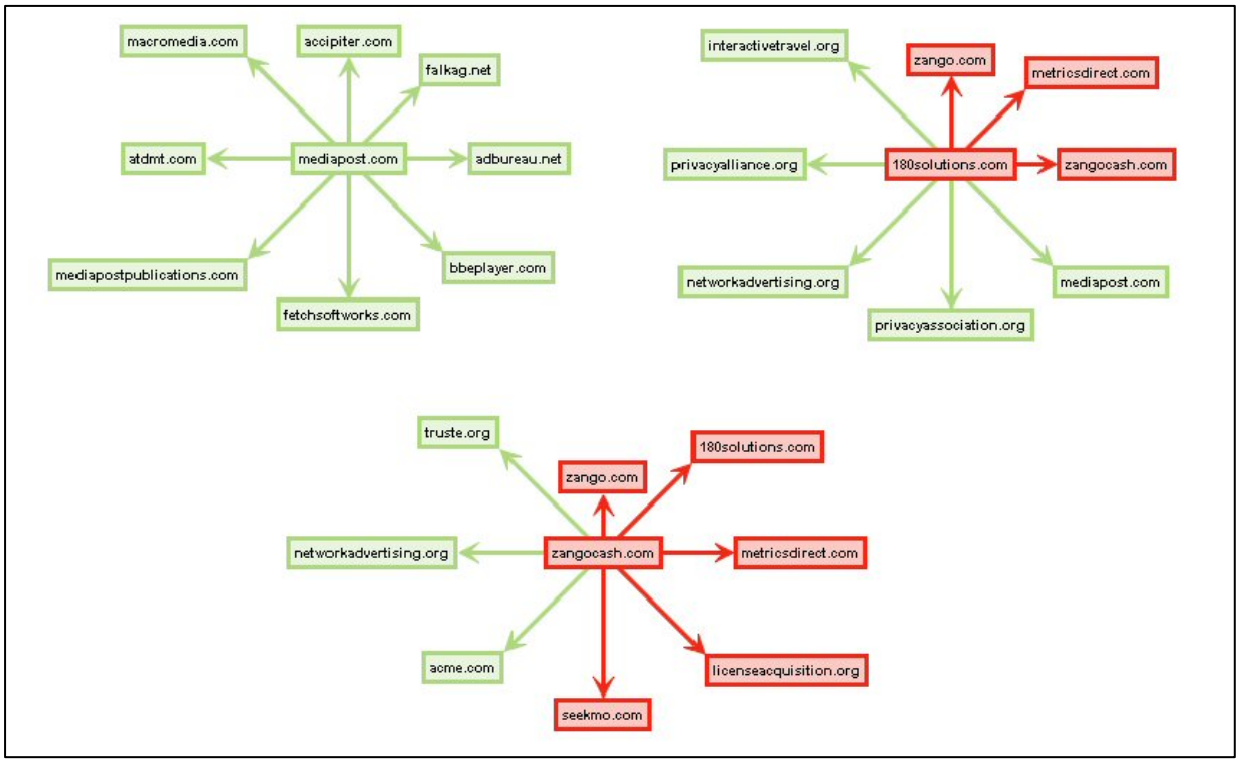

Figure 12 : Exemples de liens commerciaux entre sociétés publicitaires.

3.4 Aspects techniques des PUPS liés au monde de la publicité, du commerce et du marketing

Les codes malicieux traditionnels ont longtemps été développés par des amateurs, un peu comme une sorte de hobby. Dès leur origine, les adware ont été conçus par de véritables professionnels pour le compte de sociétés commerciales ayant des moyens financiers adaptés à leurs besoins. Les techniques d'installation sont sophistiquées et l'élimination est rendue volontairement difficile.

3.4.1 Installation

Elle devrait systématiquement faire l'objet d'un accord préalable. Beaucoup d'adware s'installent cependant de manière discrète, voire invisible lorsque l'utilisateur visite un site web où charge un logiciel gratuit ou à l'essai (freeware, shareware). Les méthodes employées sont variées :

[9] McAfee SiteAdvisor : http://www.siteadvisor.com

- Alerte de sécurité : une fenêtre d'avertissement signale un problème sur le poste de travail. Un message invite l'utilisateur à installer un programme d'analyse qui est en fait lui-même un adware. Le site Spyware Warrior [10] en recense près de 350.
- Fenêtres superposées : une fenêtre imitant un message système courant apparaît à l'écran ; elle se superpose au message de sécurité qui invite à la prudence. S'il n'y prend garde, l'utilisateur qui ne lit pas le message qu'il croit connaître, risque d'être induit en erreur et d'accepter une installation qu'il s'imagine refuser.
- Contrôles ActiveX : sous couvert d'une proposition d'installation d'un contrôle Active-X pour le traitement d'un fichier audio ou vidéo, on oblige à l'installation simultanée d'un adware [11].
- Sollicitations continuelles : un message proposant une installation apparaît à l'écran. Il boucle sur lui-même en cas de réponse négative. L'utilisateur ne peut reprendre la main qu'en acquiesçant et en déclenchant ainsi l'installation.
- Installation groupée : l'installation d'un logiciel (souvent gratuit) est soumise à l'accord d'installation d'un adware.
- Exploits : certains sites utilisent les failles de sécurité des navigateurs pour installer furtivement des adware.

3.4.2 Chargement

Avertissement : *les informations de ce paragraphe concernent différentes techniques d'installation également utilisées par de nombreux programmes légitimes. En conséquence, nous vous recommandons de ne modifier aucun de ces paramètres si vous n'êtes pas certain de ce que vous faites.*

Une fois installé, l'adware est activé à chaque démarrage ou redémarrage du poste de travail :

- Via certaines clés de registre :
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run

[10] Spyware Warrior list : http://www.spywarewarrior.com/rogue_anti-spyware.htm

[11] Spyware ravageur via le peer-to-peer : http://www.presence-pc.com/actualite/Peer-To-Peer-spyware-13480/

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

- Via certains sous répertoires de *Documents and Settings* :
  - *Nom d'utilisateur\Start Menu\Programs\Startup* (Sur une version de Windows anglophone)
  - *Nom d'utilisateur\Menu Démarrer\Programmes\Démarrage* (Sur une version de Windows française)
- Via des plug-ins, des extensions ou de faux sites de confiance insérés dans Internet Explorer ou Winsock. Pour Internet Explorer, ils sont visibles en utilisant la procédure suivante :
  - Démarrer Internet Explorer,
  - Aller dans le menu Outils/Options Internet,
  - Aller ensuite sous l'onglet Général,
  - Aller dans la rubrique Historique de navigation/Paramètres,
  - Cliquer alors sur le bouton Afficher les objets.

  D'autres intrusions sont visibles au travers des clés :
  - HKLM\Software\Microsoft\Internet Explorer\Extensions
  - HKLM\Software\Microsoft\Internet Explorer\Styles
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains

Pour Winsock, certains outils tels que LSPFIX ou Sporder peuvent être utiles pour découvrir les intrus. Mais ils doivent être utilisés, ici encore, avec beaucoup de précautions.

3.5 Circuits financiers légaux

Si le phénomène des PUPS liés au monde de la publicité, du commerce et du marketing est prédominant, c'est qu'il touche à de nombreux intérêts financiers. En mars 2006, le « Center for Democracy and Technology » (CDT) a publié un rapport démontrant que les intérêts financiers liés à la publicité encouragent la malveillance et la production d'adware. Ce document propose également quelques pistes pour renverser cette tendance [12].

La suite de ce paragraphe est une libre traduction d'une partie de ce rapport.

En théorie, le modèle commercial de la diffusion d'adware est simple : les annonceurs ne devraient avoir aucune difficulté à surveiller et à contrôler le

[12] Following the money : http://www.cdt.org/privacy/20060320adware.pdf

placement de leurs annonces publicitaires. Le diagramme suivant schématise ce modèle commercial théorique.

Figure 13 : Modèle commercial théorique lié à la distribution d'adware

Dans la pratique, le modèle commercial du marché de l'adware est souvent beaucoup plus complexe. Bien que le scénario simple montré ci-dessus existe parfois, il y a souvent une multitude d'autres intervenants dans la chaîne de publicité. Ainsi, le chemin suivi par une publicité depuis sa source jusqu'à l'ordinateur d'un utilisateur est difficile à suivre. Le diagramme suivant illustre les complexités du vrai marché de l'adware.

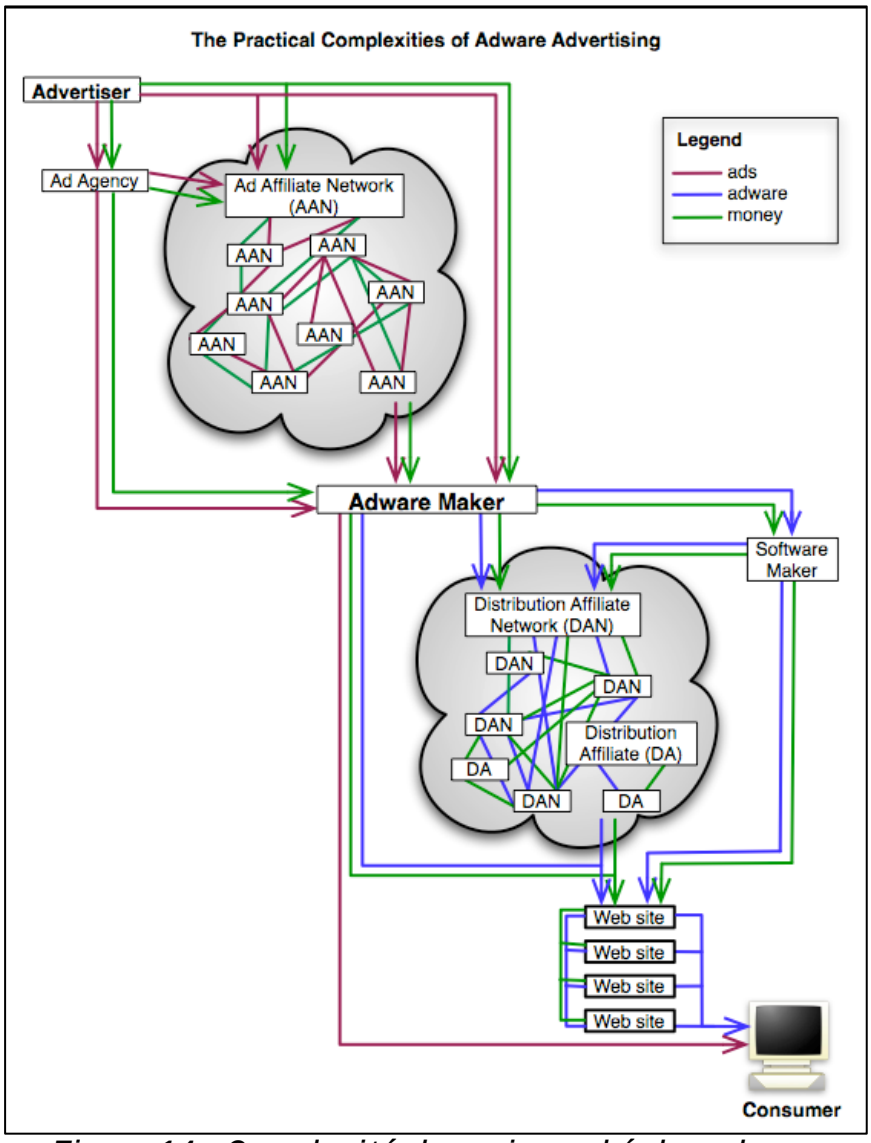

Figure 14 : Complexité du vrai marché des adware

De nombreux intervenants peuvent être impliqués pour diffuser la publicité d'un annonceur à un consommateur. Parmi eux :

- Annonceurs (Advertisers) : ce sont les entreprises qui payent les annonces. Les annonceurs s'adressent le plus souvent à des agences de publicité (Ad Agency) ou à des réseaux d'annonceurs (AAN) pour faire réaliser leurs campagnes publicitaires. Plus rarement, certains annonceurs traitent directement avec les éditeurs d'adware (Adware Maker).

- Agences de publicité (Ad Agencies) : elles sont rémunérées par les annonceurs pour réaliser leurs campagnes de promotion et pour faire diffuser les annonces auprès de multiples médias. Les agences de publicité fonctionnent habituellement avec des réseaux d'annonceurs (AAN) pour faire diffuser les messages publicitaires en ligne, mais elles peuvent également s'adresser directement aux éditeurs d'adware.

- Réseaux d'annonceurs (Advertising Affiliate Networks - AAN) : ces réseaux servent d'intermédiaire entre une agence de publicité et les éditeurs d'adware. Le plus souvent cependant, un réseau d'annonceurs utilisera un

autre réseau d'annonceurs sous-traitant, qui pourra lui aussi procéder de la même manière et ainsi de suite (voir exemple en fin de paragraphe). Dans ce cas, les différents accords créent une longue chaîne par laquelle les publicités transitent. De plus, certains réseaux fonctionnent en mode « invisible », afin que le client initial (l'annonceur) ne puisse pas savoir où et comment sa publicité est placée.

- Editeurs d'Adware (Adware Makers) : ils conçoivent, développent et distribuent les adware. Tous les autres intervenants du marché de l'adware cités précédemment (c'est-à-dire annonceurs, agences de publicité, ou réseaux d'annonceurs) peuvent commander à ces éditeurs des programmes servant à diffuser leurs publicités : ces programmes sont les adware.

- Editeurs de logiciels (Software Makers) : ces éditeurs développent de petites applications (utilitaires, jeux, goodies divers, etc.) qui sont distribuées gratuitement sur Internet. Cette gratuité est possible car les éditeurs d'adware payent pour y inclure leurs programmes en tant qu'élément du logiciel gratuit. De plus, les éditeurs de ces applications profitent des réseaux de distribution des éditeurs d'adware : réseaux de distribution, filiales de distribution, et/ou sites Web.

- Filiales de distribution (Distribution Affiliates - DA) : ils aident à distribuer les adware et tout autre logiciel en utilisant des sites Web. Par exemple, un hébergeur pourrait offrir une prestation d'hébergement Internet gratuit aux sociétés qui acceptent de distribuer des adware sur leur site web. Ici encore, il peut exister de la sous-traitance en chaîne entre filiales de distribution.

- Réseaux de filiales de distribution (Distribution Affiliate Networks - DAN) : ils sont payés par les éditeurs d'adware et les éditeurs de logiciel pour multiplier les processus de diffusion des adware et des logiciels les incluant. Ces réseaux peuvent fonctionner directement avec des sites Web ou des filiales de distribution, mais ils peuvent également travailler les uns avec les autres pour former des chaînes de réseaux de distribution.

- Sites Web (Web Sites) : ils diffusent les adware et les logiciels les contenant. Les « consommateurs » qui visitent ces sites peuvent télécharger les programmes directement sur leur ordinateur. Un site Web peut avoir des accords avec d'autres sites Web pour fournir le logiciel, et, de ce fait, former une chaîne de sites par laquelle le logiciel est distribué.

- Consommateurs (Consumers) : ils visitent les sites Web distribuant l'adware ou le logiciel conditionné avec l'adware.

Ce réseau complexe de relations rend difficile, pour l'annonceur, la compréhension du circuit de diffusion de sa campagne publicitaire.

Un scénario typique ressemble à ceci : un annonceur loue les services d'une agence de publicité pour exécuter sa campagne publicitaire. Cette agence charge un réseau d'annonceurs de la diffusion de la publicité pour une rémunération de $5 les 1000 affichages (l'affichage d'une annonce publicitaire est connu sous le terme d'« impression »). Ce premier réseau d'annonceurs a déjà un accord avec un autre

réseau pour $4.50 les 1000 impressions. Celui-ci a, lui aussi, un accord avec un troisième réseau pour $4 les 1000 impressions. C'est ce dernier réseau de la chaîne qui passe un accord avec un éditeur d'adware pour $3.50 les 1000 impressions. D'autres intermédiaires prendront ensuite leurs marges dans ce processus de distribution qui mène à l'internaute.

3.6 Circuits financiers malveillants

La diffusion frauduleuse d'adware par le biais de programmes robots est une activité qui s'avère très lucrative. Avec l'aide à la diffusion de spam et les possibilités de chantage au DDOS (déni de service distribué), cette capacité explique l'intérêt constant pour ces programmes et leur présence sur de nombreuses machines de particuliers. A l'aide de ceux-ci, un affilié malhonnête peut envisager une diffusion furtive d'adware et considérablement influencer en sa faveur les mesures de performances sur la base desquelles sa rémunération est calculée.

Le cas de Jeanson James Ancheta est particulièrement instructif à cet égard. Ce pirate informatique a utilisé ce mode de diffusion entre novembre 2004 et avril 2005 et ses rentrées financières furent aussi régulières que confortables. Ayant été arrêté en novembre 2005 l'acte d'accusation réalisé pour cette affaire [13] montre que si l'on moyenne les sommes et les ordinateurs touchés, il est possible d'estimer à 0,15 dollar la rémunération par machine « infectée » [14].

COUNT	APPROXIMATE DATES	APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION	APPROXIMATE PAYMENT
SEVEN	November 1, 2004 through November 19, 2004	26,975	$4,044.26 from Gammacash
EIGHT	November 16,2004 through December 7,2004	8,744	$1,306.52 from LOUDcash
NINE	January 15, 2005 through February 7, 2005	19,934	$2,988.11 from Gammacash
TEN	March 1, 2005 through March 22, 2005	53,321	$7,996.10 from Gammacash
ELEVEN	April 1, 2005 through April 22, 2005	28,066	$4,010.81 from Gammacash

Figure 15 : Payments for Botnet Services

[13] United States District Court for the Central District of California – Indictment : http://www.usdoj.gov/usao/cac/news/pr2005/Botnet_Indictment.pdf

[14] Adware and Spyware: Unraveling the Financial Web : http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_adware.pdf

Un autre pirate, connu sous le pseudonyme de « 0x80 » (prononcé « X-eighty »), a, lui aussi, levé un coin du voile sur ses activités illégales impliquant des réseaux de robots. Dans une interview accordée au Washington Post [15], il affirme que, comme beaucoup de « maîtres de robots » (botmaster), il gagne de l'argent en distribuant clandestinement des logiciels publicitaires. Il affirme avoir contrôlé plus de 13 000 ordinateurs dans plus de 20 pays, ce qui lui a rapporté, en moyenne, quelque 6 800 dollars par mois, avec un revenu mensuel total pouvant atteindre les 10 000 dollars. Majy, un ami de 0x80, a lui aussi raconté ses exploits et prétend recevoir, pour chaque installation, 0,20 dollar pour un ordinateur situé aux Etats-Unis et 0,05 dollar dans 16 autres pays, dont la France, l'Allemagne et le Royaume-Uni. Majy indique percevoir des recettes d'une myriade de sociétés affilieuses, dont TopConverting, Gammacash et LOUDCash.

Toutes ces affirmations semblent plausibles si l'on se fie aux offres proposées sur le NET.

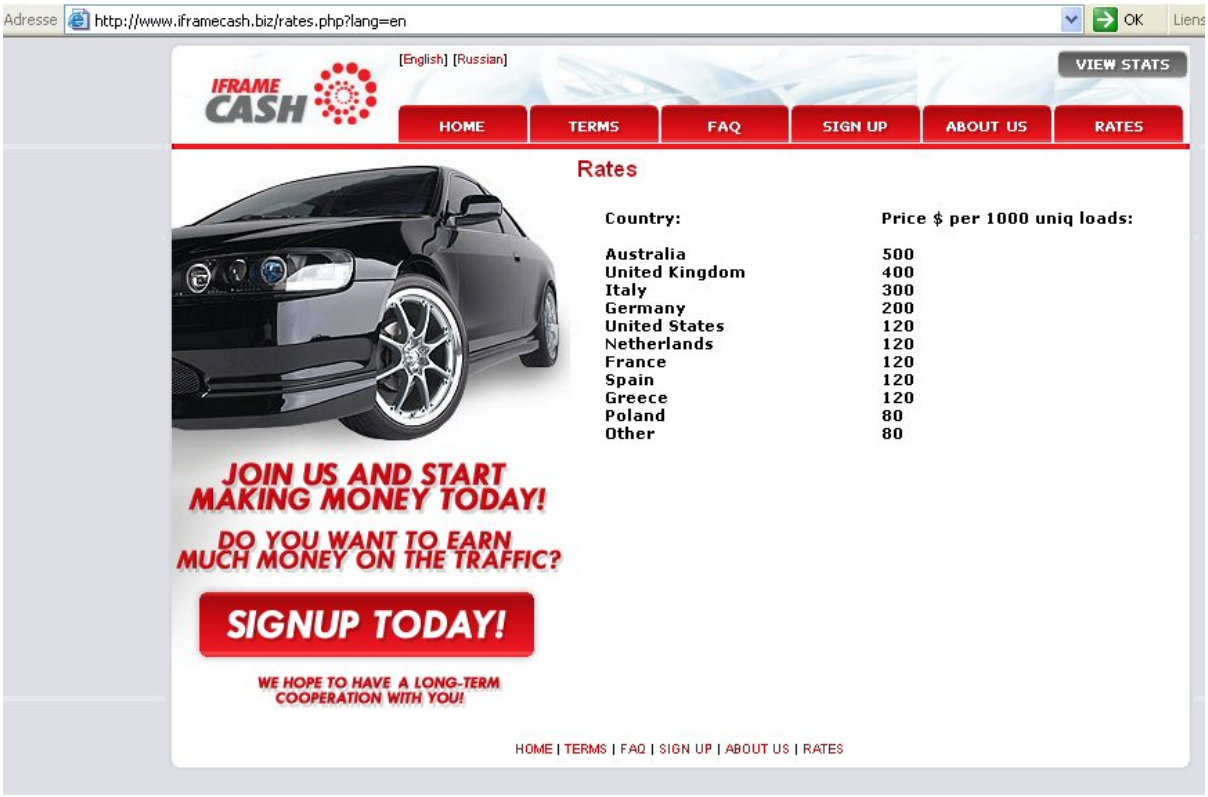

Figure 16 : Offre IFrameCash

[15] Invasion of the Computer Snatchers : http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html

Figure 17 : Offre ZangoCash

3.7 Quelques sociétés souvent montrées du doigt

Le site de Benjamin Edelman [16] (voir paragraphe 4.3) liste les principales sociétés américaines qui travaillent dans le domaine des adware tel que lui-même les définit (*tracking and/or collecting sensitive information, either without notice and consent or without meaningful notice and informed consent*) et celles qui les soutiennent par des investissements :

- 180Solutions (Zango, nCase),
- Claria / Gator (GAIN),
- Direct Revenue (BetterInternet, OfferOptimizer, et autres alias),
- eXact Advertising (BargainBuddy, BullsEye),
- Vendare Group,
- Hotbar,
- Webhancer.

[16] Investors Supporting Spyware : http://www.benedelman.org/spyware/investors/

4 ORGANISATION DE LA LUTTE ANTI-SPYWARE

La lutte anti-spyware rejoint la lutte anti-virus. Dans de nombreux cas, l'anti-virus inclut la détection des adware et spyware[stricts]. Nous invitons donc le lecteur à se référer au document « virus informatique » qui traite du sujet [17].

4.1 Dimension humaine – Message aux utilisateurs

Vérifiez que votre anti-virus est aussi adapté à la détection des programmes indésirables, sinon utilisez un produit complémentaire. Rationalisez votre politique d'installation de programmes utilitaires.

Ne pensez pas être mieux protégé en utilisant un navigateur « alternatif ». Vérifiez que le niveau de sécurité d'Internet Explorer est en position « moyen-haut ». Effectuez régulièrement les mises à jour de sécurité.

La sécurité informatique repose aussi sur le bon sens : méfiez-vous des offres promotionnelles ou gratuites. Lisez attentivement les avertissements qui s'affichent, même s'ils ressemblent à des messages connus.

Éduquez les jeunes internautes ou les débutants. Sensibilisez-les aux bonnes pratiques de navigation sur Internet.

4.2 Déontologie des annonceurs

En janvier 2006, le « Center for Democracy and Technology » (CDT) a déposé deux plaintes auprès de la « Federal Trade Commission » contre la société 180solutions, un des plus grands développeurs de publicité du monde de l'Internet, pour « pratiques commerciales déloyales et trompeuses ».

Par la suite, le CDT a identifié 18 annonceurs, clients de la société 180solutions, afin de les interroger sur leur politique en matière de publicité par adware. Cette enquête a démontré, malgré les affirmations de certains d'entre eux, qu'aucun n'avait de réel code de déontologie.

Ce manque de déontologie de la part des annonceurs conduit le CLUSIF à formuler quelques recommandations :

- Sensibiliser le public à l'existence des adware ;
- Se donner les moyens de connaître les acteurs du marché français utilisant des adware pour diffuser leurs annonces ;
- Faire en sorte que ces acteurs mettent en place un code de déontologie et refusent de travailler avec des sociétés n'ayant pas fait de même.

[17] Les Virus Informatique : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/VirusInformatiques.pdf

4.3 Les organismes officiels ou indépendants

- ASC (Anti-Spyware Coallition) : l'ASC est une association qui regroupe les grands noms qui font l'informatique, Internet et la sécurité informatique, avec entre autres AOL, Computer Associates, HP, Lavasoft (éditeur du logiciel anti-spyware Ad-Aware), McAfee, Microsoft, Symantec ou Yahoo!. Cette association est destinée à établir un consensus relatif aux définitions et aux bonnes pratiques en matière de lutte contre les logiciels espions et les autres technologies potentiellement indésirables. L'ASC se charge de communiquer sur le risque et de proposer des perspectives aux problèmes de contrôle et d'éradication des spyware.

  Site Internet : http://www.antispywarecoalition.org/

- Les pages de Benjamin Edelman : le site de Benjamin Edelman est une mine d'information au sujet des adware. En anglais, il explique leurs méthodes d'installation, documente nombre d'informations sur les entreprises qui les utilisent et compile une liste de sociétés ayant des intérêts financiers avec de nombreux éditeurs de spyware ou d'adware.

  Site Internet : http://www.benedelman.org/

- Federal Trade Commission (FTC) : agence fédérale américaine de régulation en charge de la protection des consommateurs et de la concurrence. Créé par le Congrès des États-Unis en 1913, sa mission est de veiller à ce que s'exerce sur le marché US une concurrence sans entrave et loyale et d'assurer la protection des consommateurs contre les pratiques commerciales frauduleuses et déloyales. Pour l'organisme, « *une concurrence sans entrave et loyale donne aux consommateurs accès au plus large éventail de biens et services possible, aux prix les plus bas, et une protection efficace des consommateurs renforce la confiance de ces derniers dans le marché* ». Les deux missions de la FTC – protection des consommateurs et surveillance de la concurrence – concourent à la réalisation d'objectifs plus vastes qui consistent à faciliter des choix de consommation éclairés sur le marché US et à éviter les préjudices aux consommateurs [18].

  Site Internet : http://www.ftc.gov/

- Center for Democracy and Technology (CDT) : organisme US de défense des intérêts du public qui agit en faveur des libertés publiques et des valeurs démocratiques dans le domaine des nouvelles technologies de l'informatique et des communications. Il coordonne les travaux de l'ASC.

  Site Internet : http://www.cdt.org/

---

[18] Pour plus de détails sur la FTC, voir le document de l'OCDE : Coopération Bilatérale pour Combattre la Fraude Transfrontalière : L'Expérience des États-unis et du Canada : http://www.olis.oecd.org/olis/2000doc.nsf/3dce6d82b533cf6ec125685d005300b4/c125692700623b74c12569eb0059aec6/$FILE/JT00103626.PDF

- Spyware Warrior : site recensant les produits suspects qui se prétendent être des anti-spyware.

  Site Internet : http://spywarewarrior.com/

4.4 Anti-virus & Anti-spyware

De nombreux produits affirment détecter et éliminer les programmes indésirables. Suivant la terminologie courante, ils prennent le nom d'anti-spyware. Les sociétés qui les diffusent annoncent qu'elles détectent un nombre impressionnant de programmes suspects. La plupart d'entre elles ne sont que des entités suspectes que beaucoup considèrent comme dangereuses. Le site Spyware Warrior [19] en recense, en avril 2007, près de 350.

Il existe néanmoins des produits de qualité. Là aussi le nombre de détections annoncées peut varier dans un rapport de 1 à 10. Cet écart s'explique du fait que ces produits détectent également certains programmes malveillants – souvent des chevaux de Troie - en plus des programmes commerciaux indésirables contre lesquels ils sont censés agir. Citons ici quelques produits strictement dédiés à la détection et l'élimination des adware et des spyware:

- Ashampoo AntiSpyWare
- AVG Anti-Spyware
- Lavasoft Ad-aware
- McAfee AntiSpyware
- Microsoft Windows Defender
- PestPatrol
- Spybot Search & Destroy
- Spyware Doctor
- Spyware Fighter
- Spyware Terminator
- Sunbelt CounterSpy
- SUPERAntiSpyware
- Tenebril SpyCatcher
- TrendMicro Anti-Spyware
- Webroot Spy Sweeper
- X-Cleaner
- ZeroSpyware

[19] Spyware Warrior list : http://www.spywarewarrior.com/rogue_anti-spyware.htm

Des liens vers les sites de ces produits sont disponibles depuis la page : http://www.spywarewarrior.com/uiuc/soft6.htm

La plupart des sociétés anti-virus ont intégré dans leurs produits un module anti-spyware. Pour les entreprises, c'est l'utilisation de cette solution que nous privilégions.

5 CONCLUSION

Jusqu'en 2005, le nombre de programmes indésirables découverts annuellement a suivi approximativement la progression des virus (programmes autoreproducteurs). Liés au monde de la publicité, les adware restent, dans cette famille, les principaux éléments perturbateurs. Les statistiques nous montrent cependant une réelle tendance à la baisse [20].

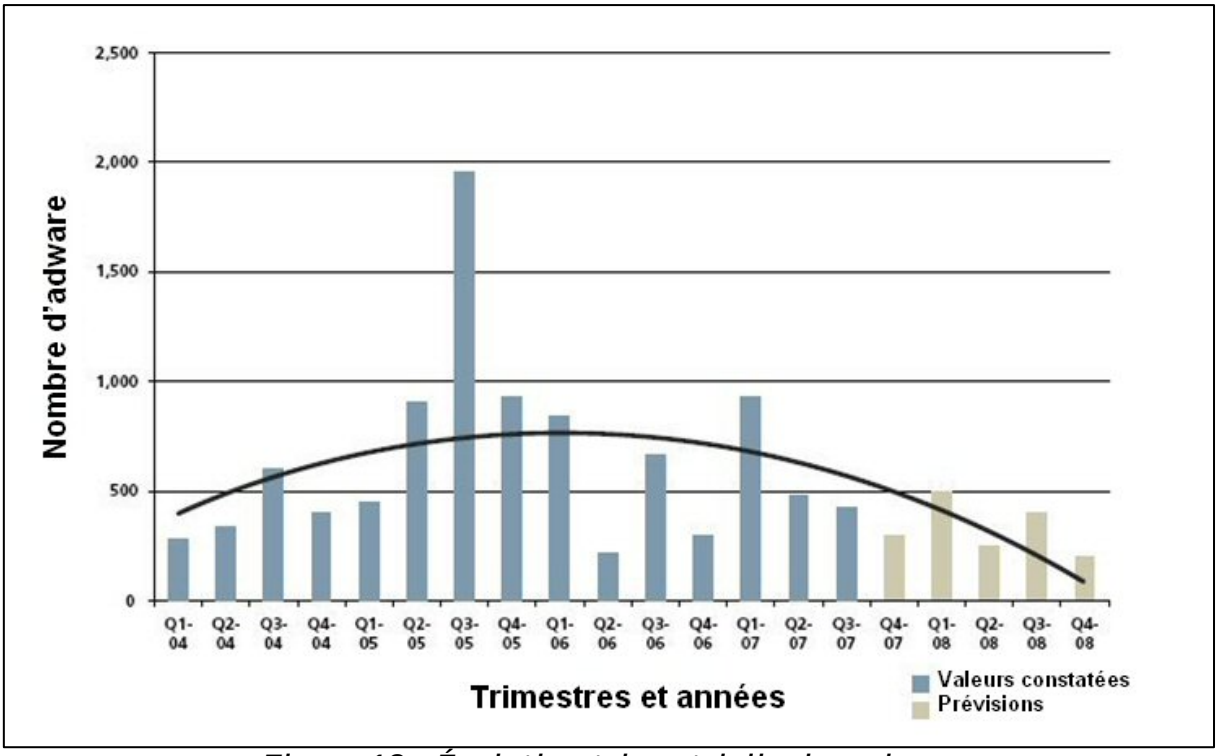

Figure 18 : Évolution trimestrielle des adware

Des actions en justice associées à de meilleures défenses et à une connotation négative pour ce mode de publicité, ont participé dès 2006 au déclin de la menace. La FTC (Federal Trade Commission), agence fédérale américaine de régulation en charge de la protection des consommateurs et de la concurrence (pour plus de détails, voir le paragraphe 4.3.) a été, depuis bientôt 2 ans, le principal acteur en ce domaine :

- Le 1er juillet 2006, la société Claria (ex Gator) annonçait qu'elle cessait la diffusion de ses pop-ups GAIN et proposait désormais des outils pour les désinstaller [21].
- En septembre 2006, plusieurs sociétés de téléchargement de vidéos payantes, dont Movieland, étaient poursuivies pour avoir proposé à leurs

[20] Le paysage des menaces : les dix prévisions de McAfee Avert Labs pour l'année 2008: http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_avert_predictions_2008_fr.pdf

[21] Claria wants you to uninstall their software: http://blogs.zdnet.com/Spyware/?p=834

clients la mise en place d'un logiciel à l'essai dont le processus de désinstallation est apparu pour le moins contestable. Le logiciel provoquait l'apparition de pop-ups publicitaires et de messages sonores. Lorsque le propriétaire de la machine demandait à le supprimer avant la fin de la période d'essai, une somme de 99 dollars lui était réclamée. Les sociétés incriminées furent condamnées à payer chacune une amende de 500.000 dollars. Movieland vient de se décider à régler son contentieux avec le FTC [22].

- En octobre 2006, ERG Ventures était condamnée à verser 330.000 dollars pour diffusion d'un programme s'installant sans réel consentement. Il modifiait la page d'accueil du navigateur Internet, analysait les habitudes de navigation et dégradait les performances de la machine. L'amende est sur le point d'être réglée [23].
- Après avoir accepté de payer une amende de 1,5 million de dollar à la FTC, on annonce en octobre 2007 la disparition de l'éditeur de logiciels publicitaires Direct Revenue [24].

Tout n'est cependant pas réglé, alors que les « sociétés respectables » hésitent de plus en plus à créer ou à simplement utiliser les adware. D'autres entités moins regardantes du coté de la déontologie prennent la relève. Il est parfois de plus en difficile de définir une frontière entre programmes malveillants et programmes simplement indésirables. De nouveaux adware commencent à être développés par des structures criminelles organisées qui les utilisent pour promouvoir leurs propres réseaux de distribution (produits pharmaceutiques douteux, faux produits de sécurité, faux utilitaires, produits de luxe contrefaits).

Même s'ils sont moins nombreux, la technologie des adware progresse (usage de plus en plus fréquent de rootkits) et leur implantation passe plus fréquemment par l'exploitation de vulnérabilités. Leur installation risque de devenir plus systématiquement silencieuse.

Alors que le nombre de programmes indésirables diminue, celui des programmes malveillants est indéniablement orienté à la hausse.

---

[22] Movieland Defendants Settle FTC Charges: http://www.consumeraffairs.com/news04/2007/09/ftc_movieland.html

[23] FTC settles with ERG Ventures for $330,000 : http://tech.monstersandcritics.com/news/article_1361927.php/FTC_settles_with_ERG_Ventures_for_$330000

[24] Direct Revenue is dead and gone: http://sunbeltblog.blogspot.com/2007/10/direct-revenue-is-dead-and-gone_24.html