

Figure 1.13 — Le puzzle proposé par le canular *Slider Joke* doit être résolu avant de pouvoir reprendre son travail

1.5 LES INFECTIONS INFORMATIQUES

Les infections informatiques sont de deux ordres. Nous sommes ici face à des programmes malveillants. On différencie :

- les programmes simples,
- les programmes auto reproducteurs.

1.5.1 Les programmes simples

Un programme simple contient une fonctionnalité malveillante qui est appelée à se déclencher à un instant donné et sur un critère donné. Il n'y a pas propagation.

Le programme doit être introduit (volontairement ou non) dans l'ordinateur ciblé. Même si un virus peut le véhiculer, l'utilisateur peut être amené à l'introduire sur sa machine en croyant installer un programme banal.

Lorsque qu'il s'exécute, la fonctionnalité malveillante (en anglais, *payload*) s'active. Une action destructive, pénalisante, ou simplement perturbatrice est alors

mise en œuvre. Selon son but, elle sera visible ou non par l'utilisateur. La première exécution du programme s'accompagne souvent d'une modification du système qui permet ensuite une réactivation automatique à chaque mise en route de la machine. Dans d'autres cas, le programme se termine une fois son but atteint.

On retrouve dans cette catégorie des programmes commerciaux indésirables dont l'usage a été détourné, des bombes logiques, des chevaux de Troie et des portes dérobées. Il existe aussi des outils de capture d'information, d'attaque réseau et d'appropriation de ressource.

Les anti-virus n'établissent généralement pas de distinction et tous ces programmes simples ; ils sont détectés en tant que *Trojans*.

Programmes commerciaux indésirables

Il s'agit généralement d'outils d'administration à distance ou de programmes indirectement dédiés à des tâches d'intrusion ou de piratage. S'ils ne sont pas légalement et volontairement utilisés leur usage s'apparente à de la malveillance. On classe aussi dans cette catégorie certains programmes du commerce qui peuvent être configurés pour être totalement invisibles aux yeux de l'utilisateur.

Même si elle est parfois contestable, l'origine de ces programmes est juridiquement légitime. S'ils avaient été créés dans un but purement malhonnête, ils apparaîtraient, pour la plupart, à la famille des chevaux de Troie.

Tout comme pour les canulars, nombre d'entre eux sont détectés par de nombreux anti-virus du commerce, si l'option de recherche adéquat est activée. On retrouve principalement dans cette catégorie des programmes permettant :

- d'arrêter un ordinateur à distance (*Remote Shutdown*),
- de rechercher ou de capturer des mots de passe (*DialPWD*),
- de modifier la page d'accueil d'Internet Explorer (*Adshow*),
- d'installer une application en tant que service NT (*FireDaemon*),
- d'analyser le trafic réseau (*Dsnif*),
- de contrôler un ordinateur à distance (*NetBusPro*),
- de composer des numéros téléphoniques à forte facturation (*PornDial*),
- d'intercepter les frappes clavier (*Silent Watch*),
- de contrôler l'activité d'un ordinateur (*WinGuardian*),
- d'envoyer massivement des e-mails (*Wyrvis from Wyrvious's Invis*),
- déprotéger des logiciels sous licence (*Crack-Generic*),
- de contourner les pare feux ou les anti-virus (*Firehole*, *Piorio*),
- de faire des envois massifs de cartes de vœux électroniques (*Friend Greeting*),
- de trafiquer en mode tunnellation (*Htthost*),
- d'effacer des données du BIOS (*KillCMOS*),
- de reconstruire des exécutables (*Pereb PE-rebuilder*),

- de rechercher des ports TCP/IP vulnérables (*Pest-PortScan*),
- de proposer des tests de personnalité (*PersonalityTest*),
- de détruire des données en cas d'utilisation non autorisée de logiciel (*FireAnvil*).

Parfois d'utilisation légitime, certains anti-virus tel que McAfee VirusScan sont capables d'affiner leur détection en fonction de critères tels que le nom de fichier ; une alerte n'étant émise qu'en cas d'utilisation de nom d'emprunt.

D'autres programmes commerciaux indésirables se rencontrent fréquemment, il s'agit des *adwares* et des *spywares*, ils méritent toute notre attention.

Adwares et Spywares

D'un point de vue étymologique, les mots *adware* (*Advertising Software*) et *spyware* (*Spying Software*) sont des acronymes anglais qui désignent deux classes particulières de logiciels. À ces 2 classes se mêlent parfois d'autres groupes d'outils d'origines diverses :

- Adware = Ads + ware (logiciel publicitaire).
- Spyware = Spy + ware (logiciel espion).
- BHO = *Browser Helper Object*.
- Hijacker = Outils de re-direction.

Citons à titre d'exemple :

- *Adware-Cydoor* (Adware).
- *Spyware-eBlaster* (Spyware).
- *Adware-NavHelper* (BHO).
- *Galorion* (Hijacker).

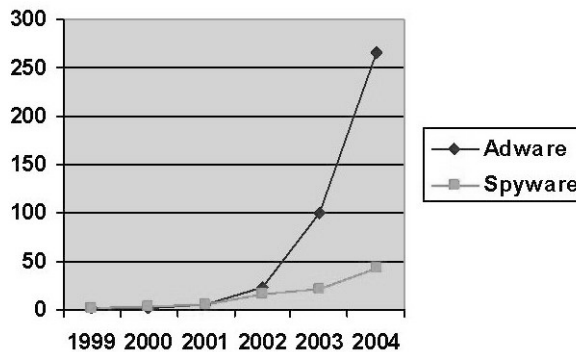


Figure 1.14 – Nombre cumulé d'adwares et de spywares (source *PestPatrol*¹)

1. Pest Patrol Graph Generator : <http://research.pestpatrol.com/graphs/form.jsp>.