

---

## **Menaces posées par les chevaux de Troie pour la santé de votre entreprise**

---

Comment protéger votre réseau des chevaux de Troie

Etablissant ce que sont les chevaux de Troie et des dangers qu'ils représentent pour vos réseaux, ce livre blanc décrit le besoin et les méthodes de protection de réseau contre les menaces de chevaux de Troie.

---

## Introduction

Ce livre blanc décrit ce que les chevaux de Troie sont et pourquoi ils posent un danger pour les réseaux d'entreprise. Dès 2001, un article de eWeek reportait que des dizaines de milliers de machines étaient infectées par des chevaux de Troie. Et cela est en forte hausse (InternetWeek.com, Janvier 2004). La grande menace des chevaux de Troie est qu'ils peuvent voler des informations de cartes de crédit, mots de passe, et autres données sensibles, ou bien lancer une attaque électronique contre votre entreprise. Le livre blanc décrit le besoin d'un scanner d'exécutables et de chevaux de Troie au niveau du serveur de messagerie en plus d'un anti-virus pour combattre cette menace.

Introduction.....	2
Ce que les agresseurs recherchent .....	2
Différents types de chevaux de Troie.....	3
Comment se faire infecter ? .....	5
Comment protéger votre réseau des chevaux de Troie.....	7
L'analyse d'exécutables malicieux – Un scanner de chevaux de Troie et d'exécutables.....	8
Protection de la passerelle .....	9
A propos de GFI Software.....	11

## Qu'est-ce qu'un cheval de Troie ?

Dans le monde de l'informatique, un cheval de Troie est utilisé pour pénétrer l'ordinateur d'une victime sans être détecté, autorisant l'agresseur à avoir accès libre aux données stockées sur cette machine et permettant de causer beaucoup de dommages à la victime. Un cheval de Troie peut être un programme caché qui s'exécute sur votre ordinateur sans que vous le sachiez, ou peut être « à l'intérieur » d'un programme légitime, ce qui veut dire que ce programme peut avoir des fonctions dont vous ne connaissez pas l'existence. (Pour un bref aperçu du fonctionnement des chevaux de Troie, veuillez aller à la page <http://kbase.gfi.com/showarticle.asp?id=KBID001671>).

---

## Ce que les agresseurs recherchent

Les chevaux de Troie peuvent être utilisés pour voler des informations confidentielles ou endommager la machine. Dans un contexte de réseau, un cheval de Troie est vraisemblablement utilisé pour espionner et voler des informations sensibles (espionnage industriel). Les intérêts des agresseurs peuvent inclure, sans pour autant y être limité :

- Information de cartes de crédit (souvent utilisées pour l'enregistrement de nom de domaine ou des achats en ligne)
- Tous détails des comptes (mots de passe email, connexion à distance, services Web, etc)
- Documents confidentiels
- Adresses email (par exemple, les contacts de clients)

- Images ou conception confidentielles
- Informations sur l'emploi du temps d'un utilisateur, sur ses déplacements
- Utiliser votre ordinateur avec des intentions illégales, comme hacker, scanner, noyer ou infiltrer d'autres machines sur le réseau ou sur Internet.

---

## Différents types de chevaux de Troie

Il y a de nombreux types de chevaux de Troie ; ils peuvent être répartis en sept catégories principales. Notez, cependant, qu'il est en général difficile de classer un cheval de Troie dans un seul groupe, car ils ont souvent des traits qui les placeraient dans plusieurs catégories. Ci-dessous sont les différentes fonctions qu'un cheval de Troie peut avoir.

### Cheval de Troie à accès distant

Ceux-ci sont probablement les chevaux de Troie les plus connus, car ils donnent aux agresseurs un contrôle total sur la machine de la victime. Par exemple, vous avez les chevaux de Troie Back Orifice et Netbus. Leur concept est de donner un accès TOTAL à l'agresseur sur la machine de la victime, et donc de donner plein accès aux fichiers, conversations privées, données de comptes, etc.

Le virus Bugbear qui a été introduit sur Internet en Septembre 2002, par exemple, installait un cheval de Troie sur la machine de la victime qui permettait un accès distant aux données importantes.

En général, les chevaux de Troie agissent en tant que serveur et espionnent à partir d'un port qui devait être disponible aux pirates Internet. Les attaquants peuvent désormais utiliser une connexion inverse pour atteindre les hôtes backdoor de façon à ce qu'ils atteignent le serveur même lorsqu'un pare-feu est activé. Certains chevaux de Troie peuvent aussi se connecter automatiquement au IRC et peuvent être contrôlés grâce à des commandes IRC de façon presque anonyme, sans que ni l'agresseur ni la victime ne procèdent à une connexion TCP/IP réelle.

### Chevaux de Troie transmetteurs de données (mots de passe, touches de clavier etc.)

L'objectif de ces chevaux de Troie est d'envoyer des données au hacker contenant des informations comme des mots de passe (ICQ, IRC, FTP, http) ou des informations confidentielles telles que les détails de carte de crédit, log de discussions, listes d'adresses, etc. Le cheval de Troie recherche des informations spécifiques dans des endroits particuliers, ou peut installer un log de clés et uniquement envoyer les touches de clavier enregistrées au hacker (qui, par la suite, peut extraire les mots de passe de ces données).

Un exemple le virus d'email Badtrans.B (publié en Décembre 2001) peut enregistrer les frappes de touches des utilisateurs.

Les données capturées peuvent être envoyées à l'adresse email de l'agresseur, qui dans le plupart des cas est un fournisseur d'email gratuit sur Internet. Alternativement, les données capturées peuvent être envoyées en se connectant sur le site Web d'un hacker – probablement un hébergeur Web gratuit – et envoyer les données par un formulaire en ligne. Ces deux méthodes passent inaperçues et peuvent être faites à partir de n'importe quelle machine sur votre réseau, qui a un accès Internet et email.

Les hackers internes et externes peuvent utiliser des chevaux de Troie qui envoient des données pour obtenir des informations confidentielles sur votre société.

### **Chevaux de Troie destructifs**

La seule fonction de ces chevaux de Troie est de détruire et de supprimer des fichiers. Cela rend très simples à utiliser. Ils peuvent automatiquement supprimer tous les fichiers du cœur du système (par exemple, les fichiers .dll, .ini ou .exe, et peut-être d'autres sur votre machine). Le cheval de Troie peut soit être activé par l'agresseur ou peut fonctionner comme une bombe à retardement qui démarre un certain jour, à une certaine heure.

Un cheval de Troie destructif est un danger pour tout réseau informatique. Il est similaire en beaucoup de points à un virus, mais le cheval de Troie destructif a été créé pour spécifiquement vous attaquer, et, par voie de fait, a peu de chance d'être détecté par votre logiciel anti-virus.

### **Chevaux de Troie de Denial of service (DoS)**

Ces chevaux de troie donnent à l'agresseur le pouvoir de démarrer une attaque de 'distributed denial of service' (DDoS) si il y a suffisamment de victimes. L'idée principale est que, si vous avez 200 utilisateurs ADSL et que vous attaquez les victimes en même temps, ceci va générer un trafic LOURD (supérieur à la bande passante de la victime, dans la plupart des cas), causant l'arrêt de son accès Internet.

WinTrinoo est un outil de DDoS qui est récemment devenu très populaire; par son biais, un agresseur qui a infecté plusieurs utilisateurs ADSL peut amener des sites Internet populaires à s'arrêter ; les premiers exemples datent de février 2000, quand un nombre de grands sites commerciaux comme Amazon, CNN, E\*Trade, Yahoo et eBay étaient attaqués.

Une autre variation d'un cheval de Troie DoS est le cheval de Troie de bombe de courrier électronique, qui a pour objectif principal d'infecter autant d'ordinateurs que possible, puis d'attaquer une ou plusieurs adresses email spécifique avec des sujet pris au hasard et des contenus qui ne peuvent être filtrés.

De nouveau, un cheval de Troie DoS est similaire en beaucoup de points à un virus, mais le cheval de Troie DoS a été créé pour vous attaquer particulièrement, et, par voie de fait, a peu de chance d'être détecté par votre logiciel anti-virus.

## **Chevaux de Troie de proxy**

Ces chevaux de Troie transforment les ordinateurs des victimes en serveur Proxy, le rendant disponible au monde entier ou à l'agresseur seul. Il est utilisé pour des connexions Telnet Anonymes, ICQ, IRC, etc., pour faire des achats avec des cartes de crédit volées, et pour d'autres activités illégales. Il donne à l'agresseur un anonymat complet et l'opportunité de tout faire à partir de votre ordinateur, y compris lancer des attaques sur votre réseau.

Si, cependant, les activités de l'agresseur sont détectées et suivies, la trace est dirigée sur vous, et non l'agresseur – ce qui peut amener votre organisation à avoir des problèmes juridiques. Au sens strict, vous êtes responsable de votre réseau et de toute attaque qui est lancée à partir de celui-ci.

## **Chevaux de Troie FTP**

Ces chevaux de Troie ouvrent un serveur FTP sur la machine de la victime qui pourrait contenir et servir un logiciel illégal et/ou des données importantes, et aussi permettre aux agresseurs de se connecter à votre machine grâce à un FTP.

## **Désactiveurs de logiciel de sécurité**

Ceux-ci sont des chevaux de Troie qui sont destinés à stopper/tuer les programmes comme les anti-virus, pare-feu, etc. Une fois ces programmes désactivés, le hacker est capable d'attaquer votre machine plus facilement.

Le virus Bugbear a installé un cheval de Troie sur les machines de tous les utilisateurs infectés et était capable de désactiver les logiciels antivirus et de pare-feu. Le ver destructif Goner (Décembre 2001) est un autre virus qui incluait un cheval de Troie qui supprimait les fichiers d'antivirus.

Les désactiveurs de logiciels de sécurité visent en général un logiciel client comme pare-feu personnel, et sont par voie de fait moins viables dans un environnement de réseau d'entreprise.

---

## **Comment se faire infecter ?**

Pour un utilisateur réseau qui est protégé par un pare-feu et ceux qui ont des connexions ICQ ou IRC désactivées, les infections vont très probablement arriver par un attachement d'email ou par un logiciel téléchargé à partir d'un site Web.

Beaucoup d'utilisateurs disent qu'ils n'ouvrent jamais de logiciels en attachement ou de téléchargement d'un site Web inconnu, cependant des techniques d'ingénierie sociale utilisées par les hackers peut tromper la plupart des utilisateurs à lancer les attachements ou téléchargements de logiciel malicieux sans qu'ils suspectent quoi que ce soit.

Un exemple de cheval de Troie qui fait usage d'ingénierie sociale était le cheval de Troie

Septer, qui était transmis par email en Octobre 2001. Il était déguisé sous forme d'une donation à la Croix Rouge Américaine et demandait aux destinataires de compléter un formulaire, incluant leurs numéros de carte de crédit. Le cheval de Troie codait ces détails et les envoyait vers le site Web du hacker.

### **Infection via pièces jointes**

Le nombre de personnes qui sont infectées en lançant une pièce jointe envoyée vers leur boîte aux lettres est impressionnant. Imaginez le scénario suivant : La personne qui vous vise sait que vous avez un ami nommé Alex et connaît aussi l'adresse email d'Alex. L'agresseur déguise un cheval de Troie en tant que contenu intéressant, par exemple une blague en Flash, et vous l'envoie par email au nom de votre ami. Pour faire cela, l'agresseur utilise un serveur relais mail pour falsifier le champ DE et faire croire qu'Alex est l'expéditeur. L'adresse email d'Alex est alex@exemple.com, donc le champ DE de l'agresseur est changé en alex@exemple.com. Vous vérifiez votre email, voyez qu'Alex vous a envoyé un attachement contenant une blague, et le lancez sans même penser qu'il puisse être malicieux « parce qu'Alex ne ferait pas une chose pareille, c'est un ami ! »

L'information est le pouvoir : Uniquement parce que l'agresseur sait que vous avez un ami nommé Alex, et savait et a deviné que vous apprécieriez une blague, il est arrivé à infecter votre machine !

Différents scénarii sont possibles. Le point est qu'il suffit d'UN SEUL utilisateur réseau pour infecter votre réseau entièrement.

De plus, si vous n'utilisez pas de logiciel de sécurité email qui peut détecter certains exploits, alors les pièces jointes peuvent être lancées automatiquement, ce qui veut dire qu'un hacker peut infecter un système uniquement en envoyant un cheval de Troie en pièce jointe, sans intervention de la part de l'utilisateur.

### **Téléchargement de fichiers Internet infectés**

Les chevaux de Troie peuvent aussi être « distribués » à partir d'un site Internet. Un utilisateur peut recevoir un email avec un lien vers un site intéressant, par exemple. L'utilisateur visite le site, télécharge des fichiers dont il pense avoir besoin ou qu'il veut, et, sans le savoir, un cheval de Troie est installé et prêt à être utilisé par l'agresseur. Un exemple récent est le cheval de Troie ZeroPopUp, qui était disséminé par un envoi de spam et permettait aux utilisateurs de télécharger le cheval de Troie, le décrivant comme un produit qui pourrait bloquer les publicités. Une fois installé, le cheval de Troie envoie un email à tout le monde dans le carnet d'adresse de l'utilisateur promouvant l'URL de ZeroPopUp et le logiciel. Comme cet email est envoyé à partir d'un ami ou collègue, quelqu'un va vraisemblablement vérifier l'URL et télécharger le logiciel.

De plus, il y a des milliers d'archives de « hacking/sécurité » sur des hébergeurs de sites Web comme Xoom, Tripod, Geocities et bien d'autres. Ces archives sont pleines de programmes de

hackers, scanners, bombes mail, logiciels de flood et autres outils. Souvent, beaucoup de ces programmes sont infectés par des personnes qui ont créé le site. De nouveau, un simple utilisateur peut infecter l'intégralité de votre réseau.

En janvier 2003, TruSecure, la firme de management de risques à qui appartient ICSA Labs et InfoSecurity Magazine, prévenait que les développeurs de code malicieux vont de plus en plus déguiser des chevaux de Troie comme distractions d'adulte, par exemple, et poster ces programmes sur des sites pornographiques ou groupes de nouvelles, afin de viser de nouveaux utilisateurs. Des utilisateurs spécifiques vont aussi être visés de cette manière, comme l'agresseur peut envoyer l'URL contenant les programmes malicieux déguisés à une victime qui ne se méfie pas.

De manière similaire, le cheval de Troie Migmaf ou « mafia nomade » qui est sorti en juillet 2003 a détourné environs 2000 PC sur Windows avec un accès Internet à grande vitesse, leur autorisant à être utilisés pour envoyé des publicités à caractère pornographique. Le cheval de Troie Migmaf transforme l'ordinateur de la victime en un serveur proxy qui sert d'intermédiaire entre les personnes qui cliquent sur un email à caractère pornographique ou de lien vers un site Internet – Il utilise la victime pour chercher des publicités sur un serveur caché et passe les publicités vers d'autres ordinateurs soit par un email de spam, soit grâce à un Web browser.

---

## **Comment protéger votre réseau des chevaux de Troie.**

Comment protéger votre réseau contre les chevaux de Troie ? Une idée fausse courante est qu'un antivirus offre toutes les protections dont vous avez besoin. La vérité est qu'un antivirus n'offre qu'une protection limitée. Les logiciels antivirus ne reconnaissent seulement qu'une partie des chevaux de Troie connus, et ne reconnaît pas les chevaux de Troie inconnus.

Même si la plupart des scanners de virus détectent un grand nombre de chevaux de Troie publics/connus, ils sont incapables de scanner les chevaux de Troie inconnus. Ceci est dû au fait qu'un logiciel antivirus se base sur la reconnaissance de la « signature » de chaque cheval de Troie. Cependant, parce que le code source de beaucoup de chevaux de Troie est facilement disponible, un hacker avancé peut créer une nouvelle version de ce cheval de Troie, une signature qu'aucun scanner antivirus ne peut avoir.

Si la personne qui prévoit de vous attaquer découvre quel logiciel antivirus vous utilisez, par exemple par le biais d'un disclaimer automatiquement ajouté aux mels par un logiciel antivirus, il créera un cheval de Troie qui passera automatiquement au travers de votre moteur antivirus.

A part le manque de détection des chevaux de Troie inconnus, les scanners de virus ne peuvent pas détecter tous les chevaux de Troie non plus – La plupart des développeurs d'antivirus ne recherchent pas activement de nouveaux chevaux de Troie et des recherches ont montré que chaque moteur antivirus recherche des chevaux de Troie différents. Afin de détecter un pourcentage plus important de chevaux de Troie connus, vous devez déployer de

multiples antivirus, ce qui augmentera de beaucoup le pourcentage de chevaux de Troie connus capturés.

Pour protéger votre réseau de manière effective contre les chevaux de Troie, vous devez suivre une stratégie de sécurité à plusieurs niveaux :

1. Vous devez implémenter une passerelle de moteur antivirus et de vérification du contenu dans le périmètre de votre réseau pour les emails, HTTP et FTP – Il ne sert à rien de n'avoir qu'une protection d'antivirus si un utilisateur peut télécharger un cheval de Troie à partir d'un site Web et infecte votre réseau.
2. Vous devez implémenter de multiples moteurs antivirus sur la passerelle – Même si un bon moteur antivirus détecte habituellement tous les virus connus, c'est un fait que plusieurs moteurs antivirus vont reconnaître plus de chevaux de Troie connus qu'un seul moteur.
3. Vous devez mettre en quarantaine/vérifier les exécutables qui entrent votre réseau par email et Web/FTP au niveau de la passerelle. Vous devez analyser ce que l'exécutable peut faire.

Heureusement, il existe des outils disponibles qui permettent d'automatiser une grande partie de ce processus.

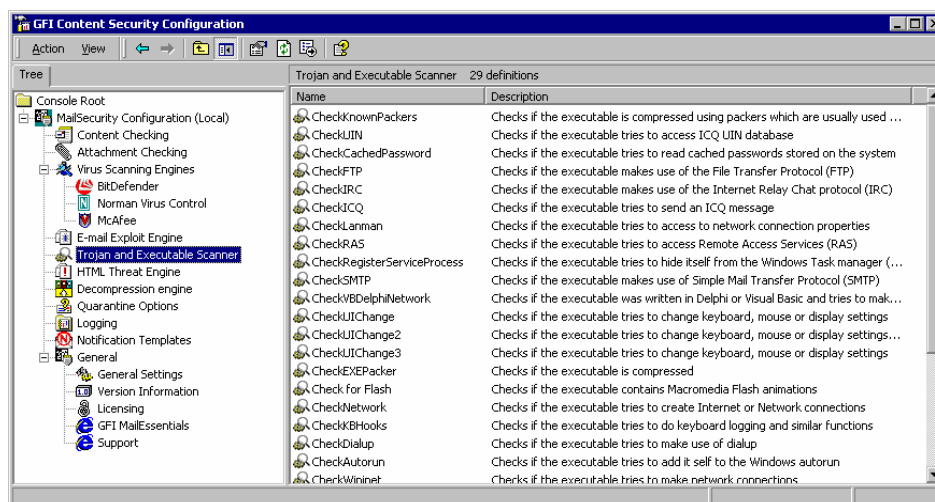
---

## **L'analyse d'exécutables malicieux – Un scanner de chevaux de Troie et d'exécutables.**

Détecter des chevaux de Troie inconnus peut seulement être fait manuellement en révisant les exécutables, ou en utilisant un scanner de chevaux de Troie et Exécutables.

Le processus de revue des exécutables est long et prend beaucoup de temps, et peut être sujet à des erreurs humaines. Il est donc nécessaire de s'attaquer à ce processus de manière intelligente et d'en automatiser une partie. C'est le but d'un analyseur de chevaux de Troie et d'exécutables.

Un scanner d'exécutables analyse de manière intelligente ce que l'exécutable fait et lui assigne un niveau de risque. Il désassemble les exécutables et détecte en temps réel ce que cet exécutable peut faire. Il compare ces actions à une base de données d'actions malicieuses et ensuite détermine le niveau de risque de l'exécutable. De cette manière, des chevaux de Troie potentiellement dangereux, inconnus, ou utilisés qu'une fois peuvent être détectés. Le scanner de chevaux de Troie et d'exécutables se joue des hackers avancés qui créent leurs propres versions de chevaux de Troie, dont la signature est inconnue des logiciels d'antivirus.



### Configuration du scanner des chevaux de Troie exécutables

La protection au niveau de la passerelle, avec de multiples moteurs antivirus et un scanner de chevaux de Troie et d'exécutables protégera votre réseau contre les dangereux effets des chevaux de Troie.

## Protection de la passerelle

Deux produits qui offrent une protection de la passerelle, incluant de multiples antivirus et un scanner de chevaux de Troie et d'exécutables, avec d'autres fonctions de sécurité sont :

GFI MailSecurity for Exchange/SMTP est une solution de vérification du contenu, détection d'exploits, scanner de chevaux de Troie et d'exécutables, analyse de menaces et antivirus, qui enlève tout type de menaces basées sur les emails avant qu'elles n'affectent vos utilisateurs de messagerie. Les fonctions de GFI MailSecurity incluent plusieurs moteurs d'antivirus, pour une indépendance des moteurs antivirus et une meilleure sécurité, quarantaine d'attachements et de contenus dangereux ; un bouclier contre les exploits, pour détecter les emails avec des exploits d'application et de système d'exploitation : un moteur de menaces HTML, pour désactiver les scripts HTML ; et un scanner de chevaux de Troie et d'exécutables, pour détecter des exécutables potentiellement dangereux. Pour un complément d'information, lisez et téléchargez une version d'évaluation sur <http://www.gfsfrance.com/fr/mailsecurity/>.

GFI WebMonitor est un utilitaire pour Microsoft ISA Server qui permet aux administrateurs de surveiller les sites visités par les utilisateurs et aussi les fichiers qu'ils téléchargent – en temps réel. En plus de ça, il peut bloquer l'accès aux sites réservés aux adultes et effectuer un balayage antivirus pour tous les téléchargements. GFI WebMonitor est la solution parfaite pour effectuer un contrôle d'accès invisible sur les habitudes de navigation des utilisateurs et aussi d'assurer le bon respect réglementations – d'une manière qui n'isolera pas les utilisateurs du

réseau. Pour un complément d'information, lisez et téléchargez une version d'évaluation sur <http://www.gfsfrance.com/fr/webmon/>.

---

## A propos de GFI Software

GFI est l'un des leaders dans le domaine de la réalisation de logiciels qui fournit une seule source intégrée permettant aux administrateurs de résoudre les problèmes de sécurisation de réseaux, de contenu et de messageries. Grâce à sa technologie innovatrice, une stratégie agressive de commercialisation et sa concentration sur le marché de petites et moyennes entreprises, GFI répond aux besoins de continuité d'affaires et de productivité des entreprises et d'autres organisations sur une grande échelle. Fondée en 1992, GFI est une entreprise internationale qui possède des bureaux à Malte, à Londres, Raleigh, Hong Kong, Adelaïde et à Hambourg avec plus de 200.000 installations de ses logiciels à travers le monde. GFI est une entreprise spécialisée et possède un réseau de plus de 10.000 partenaires à travers le monde. Partenaire stratégique de Microsoft, GFI est membre certifié du partenariat Microsoft Gold Certified Partner. Pour plus d'informations à propos de GFI, visitez le site <http://www.gfsfrance.com>.

© 2007 GFI Software. Tous droits réservés. L'information contenue dans ce document représente le point de vue actuel de GFI sur les questions abordées à la date de sa publication. Etant donné que GFI doit répondre aux conditions dynamiques du marché, il ne devrait pas être interprété comme un engagement de la part de GFI, et GFI ne peut pas garantir l'exactitude d'aucune information présentée après la date de la publication. Ce livre blanc est seulement à titre informationnel. GFI NE FAIT AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, DANS CE DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor et leurs logos de produit sont des marques déposées ou des brevets commerciaux de GFI Software aux Etats-Unis et/ou dans d'autres pays. Tous les noms de produit ou d'entreprises mentionnés ci-dessus peuvent être les marques déposées de leurs propriétaires respectifs.