GUIDE UTILISATEUR

Installation et Utilisation de

Outpost Firewall Pro

- Version 2.6 -

Date de publication : Mai 2005

agnitum

Sommaire

Introduction

Bienvenue dans ce guide qui vous aidera à installer et configurer

Outpost Firewall Pro

Nous vous remercions d'avoir acquis Outpost Firewall Pro.

Bien qu'Outpost soit très facile à installer et à configurer**,** ce guide vous aidera à en découvrir les multiples fonctionnalités, et à obtenir ainsi le meilleur niveau de protection.

Outpost Firewall Pro offre un arsenal de défense sophistiqué contre les infiltrations de votre PC en interdisant aux pirates les accès non autorisés, et en vous protégeant du vol de données, des attaques par déni de service, des violations de la vie privée, des chevaux de Troie, des spyware, etc..

Outpost Firewall Pro n'est pas un simple pare-feu, comme beaucoup existant déjà sur le marché, qui se cantonnent au blocage de tentatives d'intrusion externes. Outpost Firewall Pro est une firewall bidirectionnel qui bloque les menaces externes et internes tels que les chevaux de Troie qui exécutent une ouverture de port et une connexion frauduleuse vers l'extérieur depuis l'intérieur de votre PC.

En plus des traditionnels bloqueurs de pièces jointes pour les emails et du contrôle des "éléments actifs" des pages Internet (java, ActiveX, etc.), Outpost intègre entre autre :

- Une configuration "automatique" à l'installation des réseaux locaux (plus besoin de taper les adresses IP des autres machines),
- Un nouveau composant "anti-fuites" permettant un meilleur contrôle des tentatives de connexion des logiciels installés,
- Un dispositif de protection au démarrage de *Windows* qui empêche le lancement d'application suspectes,
- Un meilleur filtrage des « paquets » (unités de transmission des données sur le réseau),
- Des états des connexions plus détaillés,
- Un bloqueur de fenêtres pop up…

Assurez-vous tout d'abord que votre ordinateur dispose de la configuration requise :

Configuration requise minimum :
- Windows 98, 2000, ME, XP ou 2003
- 8 MB d'espace disque dur

Recommandations :
- Pour éviter toute instabilité du système et vous assurer que le programme fonctionne parfaitement, il est recommandé de désinstaller tout autre firewall avant l'installation de Outpost Firewall Pro.

I - Installation

Afin de démarrer l'installation, veuillez attendre l'ouverture de la fenêtre de lancement de l'installation lorsque vous insérez le cédérom ou bien cliquez sur l'icône nommée ***OutpostProInstall.exe.***

Ceci lancera l'installation…

1. Une fois l'installation démarrée, si l'application ne détecte pas votre installation Windows en Français, vous serez éventuellement invité à choisir la langue dans laquelle sera installé Outpost.

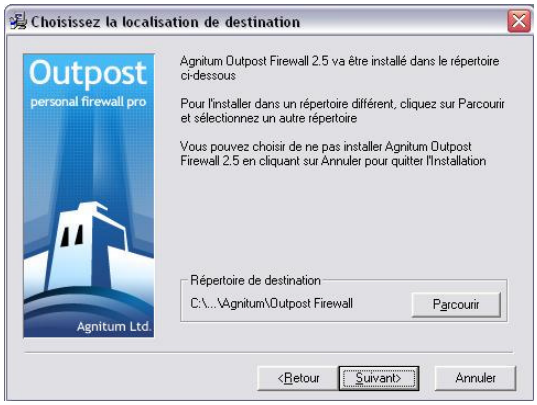
Nous choisirons ici le Français. Notez aussi que le fait de choisir le Français convertira toutes les fenêtres d'installation en français.

2. Nous voici dans le programme d'installation à proprement parler. Afin de réaliser cette dernière au mieux, veuillez suivre toutes les recommandations.

Après avoir pris connaissance des recommandations, cliquez sur **Suivant**

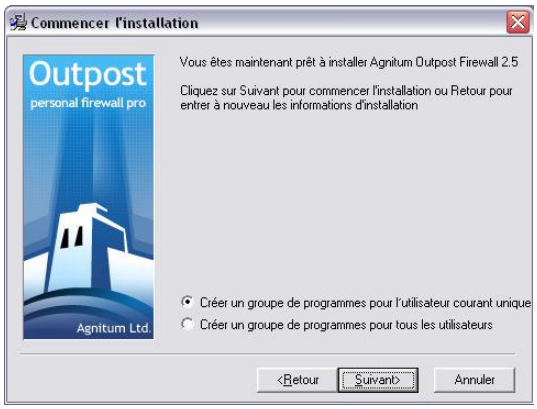
3. De même prenez le temps de lire les notes présentes lors de l'installation.

4. Choisissez ici le répertoire de destination. Nous recommandons à la plupart des utilisateurs de le laisser inchangé.



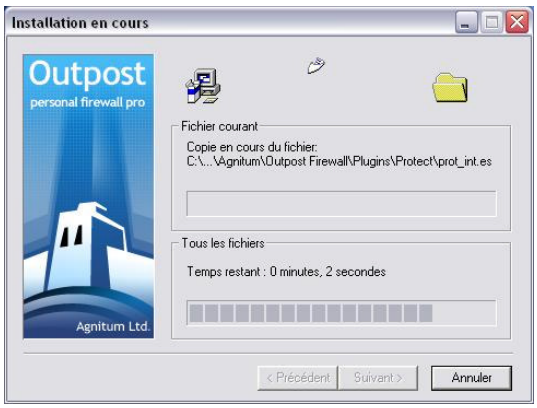
Pour choisir le répertoire d'installation cliquez sur **Parcourir***, puis, une fois la destination choisie, cliquez sur* **suivant**

5. Vous devrez définir ici si Outpost sera accessible pour tous les comptes utilisateurs existants, ou seulement pour le compte en cours lors de cette installation.



Si vous êtes le seul utilisateur, ou qu'il n'existe pas d'autre compte utilisateur pour le moment, choisissez la création pour un utilisateur unique. Une fois votre choix effectué, cliquez sur **Suivant**

6. L'installation débute alors, vous devrez alors patienter jusqu'à la fin de celle-ci.



7. Vous serez ensuite invité à choisir la configuration d'Outpost « par défaut », à savoir la configuration qui sera enregistrée et chargée à chaque démarrage d'Outpost. Il est à noter que la plupart des utilisateurs seront très bien protégés par la configuration standard automatique.

Choisissez la méthode de configuration que vous souhaitez appliquer lors de l'installation. Nous vous recommandons la configuration automatique.

8. Vous avez terminez l'installation cliquez sur OK pour redémarrez votre ordinateur

Cliquez sur **OK** *pour redémarrer votre ordinateur et activer Outpost, ou sur* **Annuler** *pour revenir sous Windows sans redémarrer. Attention il vous faudra tout de même redémarrer l'ordinateur pour rendre Outpost opérationnel.*

II. Utilisation quotidienne

2.1 Politique de protection

Cliquez sur l'onglet "Politique" :

Cet onglet vous permet de choisir la stratégie globale de fonctionnement d'*Outpost* en fonction de la manière dont vous souhaitez vous protéger et de l'activité envisagé.

- ***Option «Mode Désactiver»*** : *Outpost* ne filtre plus vos connexions.

- ***Option «Autoriser la plupart» :*** Si vous sélectionnez cette option, vos logiciels disposeront d'une grande liberté pour se connecter au réseau et seuls certains ports seront bloqués. Ce choix est vivement déconseillé pour un usage "normal".

- ***Option «Assistant de règles» :***. Chaque fois qu'un logiciel tentera de se connecter vous aurez le choix d'autoriser cette connexion, de la bloquer ou de créer une "règle". **Ce choix est vivement recommandé.**

- ***Option «Bloquer la plupart» :*** Seules les connexions que vous aurez spécifiquement autorisées par des "règles" (onglet "Application") seront possibles. Toutes les autres seront bloquées.

- ***Option «Mode tout arrêter» :*** Aucune connexion entrante ou sortante ne sera possible. A utiliser en cas d'attaques intensives menés par un tiers externe ou quand vous n'avez pas besoin de vous connecter à Internet.

Note : En cliquant avec le bouton droit sur l'icône d'*Outpost* dans la barre des tâches vous pourrez changer de stratégie à la volée.

2.2 Fonctionnement après installation et création de règles

Outpost Pro est un pare-feu "à apprentissage continu avec règles", c'est-à-dire qu'il gère vos connexions grâce à des règles spécifiant pour chaque application, quels ports et quels protocoles (langages de communication) utiliser. En principe, vous utiliserez surtout l'assistant à la création de règle lorsqu'il vous demandera que choisir quand un logiciel s'exécute ou lors d'une tentative de connexion.

Lorsqu'un nouveau logiciel veut se connecter à Internet, Outpost affiche une fenêtre de ce type :

Cinq options vous sont proposées :

- ***Autoriser toutes les activités pour cette application :*** Le logiciel en question pourra se connecter comme il le veut en utilisant n'importe quel port et protocole.

- ***Bloquer toutes les activités pour cette application :*** Le logiciel en question ne pourra pas se connecter.

- ***Créer les règles en utilisant les paramètres prédéfinis :*** Choisissez dans le menu déroulant l'option qui semble correspondre le mieux pour votre logiciel (ex.: Adobe Acrobat Reader pour notre exemple). Ainsi, le programme considéré ne pourra utiliser que certains ports et certains protocoles pour communiquer.

Note : si vous choisissez ***«Personnaliser »*** dans le menu déroulant, vous aurez alors la possibilité de préciser exactement les ports et protocoles autorisés. Cette option est conseillée uniquement aux utilisateurs expérimentés.

- Agnitum met à jour régulièrement sa liste de "modèles" afin d'adapter facilement Outpost Firewall à tous les programmes les plus connus.

- ***Autoriser une fois :*** L'application considérée pourra se connecter comme elle l'entend cette fois et cette fois seulement. La prochaine fois que vous la lancerez, vous devrez à nouveau choisir le paramètre à appliquer.

- ***Bloquer une fois :*** L'application considérée ne pourra pas se connecter cette fois et cette fois seulement ! La prochaine fois que vous la lancerez, vous devrez à nouveau choisir le paramètre à appliquer.

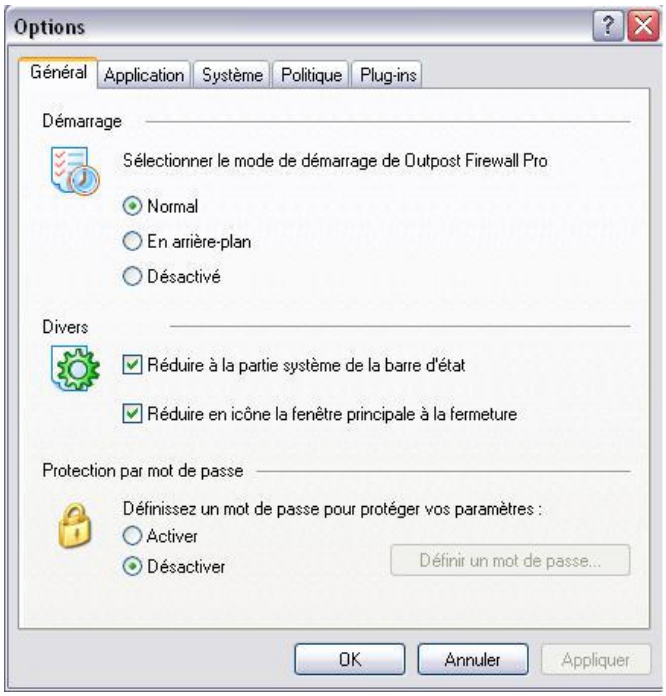
- **Création de règles nouvelles :** Quand vous optez pour une création **«manuelle»** de règle (dans la section **«Application»** en choisissant **«Ajouter»** ou avec **l'Assistant de création de règle** quand vous choisissez **«Personnaliser»,** vous avez la possibilité de régler comme vous l'entendez les connexions d'un logiciel particulier.

III. Configuration

Vous trouverez ci-dessous les éléments qui permettront aux utilisateurs de gérer leur application Outpost et aux utilisateurs avertis de modifier profondément leur configuration en fonction de leurs choix de protection.

3.1 Général

Allez dans le menu **«Options/Général».** Cette fenêtre s'affiche alors :



- ***Démarrage :*** Vous permet de sélectionner le type de démarrage. **Normal**, **en Arrière-plan** ou **Désactivé**.

- ***Divers :*** Permet de choisir les différentes options d'interfaces.

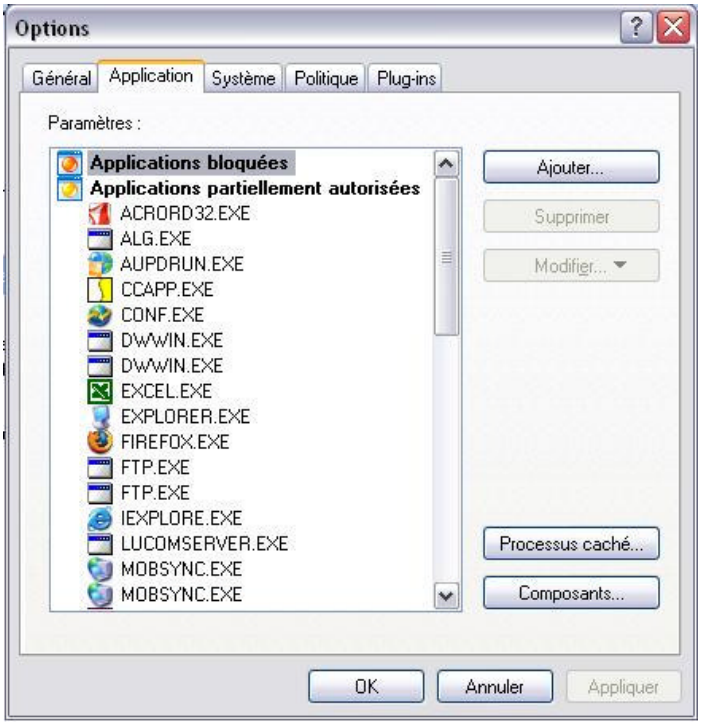
- **Réduire à la partie système de la barre d'état** : Permet de placer l'icône d'Outpost dans la barre des tâches lorsque vous "minimisez" ses fenêtres. **Il est recommandé de maintenir la case cochée**.

- **Réduire en icône la fenêtre principale à la fermeture** : A l'instant où vous cliquez sur l'icône **«Fermeture»** (la petite croix en haut à droite) d'une fenêtre d'Outpost Firewall, l'interface est seulement "minimisée" et non "fermée". **Il est recommandé de maintenir la case cochée**.

- ***Protection par mot de passe :*** Permet de définir un mot de passe pour protéger vos paramètres. Si vous êtes le seul utilisateur de l'ordinateur, cette option est facultative.

3.2 Applications

Cliquez sur l'onglet **«Application»** :



Nous voici au coeur d'Outpost. Ici sont répertoriés les applications filtrées par le firewall (la première fois que vous ouvrirez cette liste, elle sera vierge. Nous verrons comment la remplir un peu loin dans ce guide). Les programmes que vous utilisez pendant vos incursions sur Internet sont classés en trois catégories :

- ***Applications bloquées :*** Tous les logiciels auxquels vous interdisez absolument le moindre contact avec l'extérieur. Ils ne peuvent utiliser aucun port et aucun protocole pour se connecter à Internet.

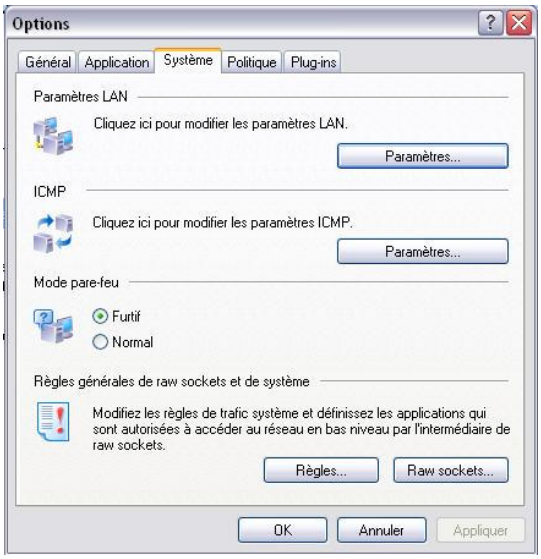
- ***Applications partiellement autorisées :*** Les logiciels qui peuvent se connecter, mais ne peuvent employer que certains ports et certains protocoles, précisés par des règles spécifiques. Cette section devrait répertorier la plupart de vos programmes usuels (navigateur, client courrier, etc.).

- ***Applications sécurisées :*** Les logiciels qui ont plein accès au réseau par le biais de n'importe quel port, et/ou de n'importe quel protocole. Cette liste devrait être la plus courte possible, car accorder de tels privilèges à une application est potentiellement dangereux et peut nuire à votre sécurité en ligne.

Notez aussi la présence des boutons «***Ajouter», «Supprimer »*** qui vous permettent de modifier manuellement la liste.

3.3 Système

Cliquez sur l'onglet **«Système»** :



- ***Paramètres LAN :*** Ces paramètres sont automatiquement détectés lors de l'installation. **Nous recommandons à la plupart des utilisateurs de ne pas les modifier.**

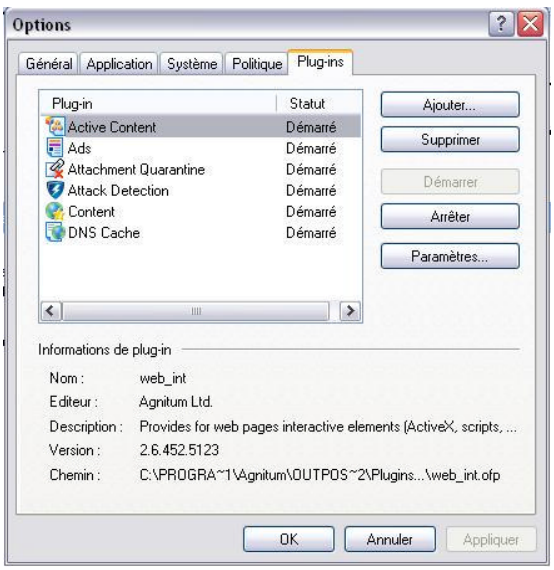
- ***ICMP :*** Ces paramètres sont automatiquement détectés lors de l'installation. **Nous recommandons à la plupart des utilisateurs de ne pas les modifier.**

- ***Mode Pare-feu :*** Permet de définir le mode de fonctionnement d'Outpost. **Nous recommandons aux utilisateurs de rester en mode furtif.**

- ***Règles générales de raw sockets et de système :*** **Nous recommandons à la quasi-totalité des utilisateurs de ne pas modifier ces paramètres.**

3.4 Plug-ins

Cliquez sur l'onglet **«Plug-ins» :**



.

Outpost est un logiciel "ouvert" dans le sens où il accepte des modules externes qui peuvent être conçus par tout un chacun... pourvu que l'on soit pourvu d'un solide bagage en programmation. De ce fait **nous vous recommandons de ne pas modifier ces paramètres manuellement**, et de laisser Outpost se configurer automatiquement si vous souhaitez rajouter des plug-ins.

IV. GLOSSAIRE ETENDU

[A]

ActiveX
Active X est la réplique de Microsoft à l'égard du langage Java et des plugs-ins. Les contrôles Active X peuvent être des modules additionnels du navigateur pour l'exploitation de certaines ressources (Active Movie par exemple) ou des programmes téléchargeables. Les contrôles Active X sont des standards de développement pour Windows adaptés à l'univers Internet. VBScript est le langage utilisé pour manipuler les objets Active X dans les pages Web.

Adresse IP
Numéro unique de la forme XXX.XXX.XXX.XXX (XXX étant un nombre entier compris entre 0 et 255) qui identifie chaque ordinateur connecté à Internet ou à tout autre réseau utilisant le protocole TCP/IP. Indispensable aux échanges d'informations entre les différentes machines, l'adresse IP peut être fixe, c'est-à-dire attribuée pour une durée indéterminée à un même ordinateur, ou bien dynamique, c'est-à-dire attribuée à chaque nouvelle connexion (cas de la majorité des fournisseurs d'accès grand public). Enregistrée dans les fichiers log des serveurs visités, l'adresse IP permet généralement de remonter jusqu'à l'identité physique de l'internaute par le biais de son fournisseur d'accès, dans le cadre d'une procédure judiciaire.

Adware
Logiciel dont l'auteur se rémunère par l'affichage de bannières publicitaires, sans pour autant recueillir de données personnelles sur ses utilisateurs (les Adwares sont régulièrement confondus par erreur avec les Spywares).

Antivirus
Utilitaire capable de rechercher et d'éliminer les virus informatiques et autres Malwares. La détection se fait selon deux principes : une analyse par signatures qui permet de détecter avec d'excellents résultats les virus connus pour peu que les définitions de virus soient régulièrement mises à jour, ou une analyse heuristique qui permet de détecter avec des résultats variables les virus inconnus à partir de leur logique de programmation et le cas échéant de leur comportement à l'exécution. Les antivirus fonctionnent eux-mêmes selon deux principes : un scanner qui permet à l'utilisateur de lancer une analyse d'un disque ou d'un fichier lorsqu'il le souhaite ("on demand"), ou un moniteur qui surveille le système en temps réel ("on access") et empêche l'utilisateur d'ouvrir un fichier infecté. La plupart des antivirus comportent un scanner et un moniteur, mais il existe des produits analysant seulement "à la demande" (ex.: antivirus en ligne) ou ne disposant que d'un moniteur (ex.: antivirus génériques).

Antispyware
Utilitaire capable de rechercher et d'éliminer les «espiogiciels» (logiciels espions). Il s'agit le plus souvent d'un scanner à la demande utilisant une analyse par signatures pour identifier les espiogiciels connus et les désinstaller. Un antispyware est utile pour s'assurer qu'aucun espiogiciel n'est présent sur un ordinateur, ou pour éliminer un espiogiciel récalcitrant lorsque l'utilisateur ne souhaite plus utiliser le logiciel associé. Par contre, l'utilisation de certains antispywares qui permettent de bloquer ou de neutraliser un spyware tout en continuant à utiliser son logiciel associé est assimilable à du piratage, les contrats de licence faisant généralement du spyware une contrepartie obligatoire à l'utilisation gratuite du logiciel associé.

Archie
Logiciel permettant de localiser un fichier FTP sur Internet. De moins en moins utilisé depuis l'apparition des moteurs de recherches sur Internet.

ARPANET (Advanced Research Project Administration Network)
Développé dans les années 1960-1970 par le département de la défense du gouvernement américain (DoD), c'est l'ancêtre de l'Internet.

ASCII (American Standard Code for Information Interchange)
Caractères de base (de A à Z en minuscules et majuscules, plus les chiffres et signes de ponctuation).

Attachment
Fichier ou pièce jointe numérique à un email.

[B]

Backdoor (= Bkdr, Porte dérobée, Trappe arrière)

Moyen non documenté permettant d'obtenir des droits privilégiés dans une application ou un ordinateur.

Dans le cas d'une application, Backdoor est souvent une partie de code ajoutée par les développeurs pour contourner toute procédure de sécurité et faciliter ainsi les tests ou le dépannage. Présente dans la version finale du programme, Backdoor permet à qui en a connaissance d'exécuter l'application sans autorisation ou de s'introduire dans le système.

Dans le cas d'un ordinateur, Backdoor est un petit programme installé automatiquement par un virus ou manuellement par une personne malveillante. A l'insu des utilisateurs, Backdoor permet de prendre le contrôle à distance du système, ou lors d'une intrusion de revenir ultérieurement sans avoir à en forcer à nouveau la sécurité. Les antivirus pouvant assez facilement être pris en défaut par les Backdoors, le meilleur moyen pour s'en prémunir reste de ne pas exécuter les logiciels ou fichiers joints douteux et d'installer un pare-feu afin de surveiller les entrées/sorties.

Bande passante (Bandwidth en anglais)

Quantité de données que peut véhiculer un canal de communication. Plus le débit est important, plus les données peuvent être transmises rapidement. Exprimé en bps (Bits par seconde).

Bit

La plus petite unité informatique (0 ou 1).

Butineur (synonyme anglais : Browser)

Programme permettant de lire les documents multimédia du Web. Navigator de Netscape et Internet Explorer de Microsoft sont les deux Browsers les plus utilisés. Les Québécois parlent de fureteur, survoleur ou butineur, les Français plutôt de navigateur.

[C]

Composeur

Equivalent français de «dialer». Pour plus d'informations, reportez-vous à la définition du mot «dialer».

Cheval de Troie (Trojan Horse)

Programme qui s'introduit dans une séquence d'instructions normales et prend l'apparence d'un programme valide. Le Cheval de Troie contient en réalité une fonction illicite cachée, grâce à laquelle les mécanismes de sécurité du système informatique sont contournés. Une personne malveillante peut alors pénétrer par effraction dans des fichiers pour les consulter, les modifier ou les détruire. A la différence d'un ver, le Cheval de Troie ne se réplique pas : il peut demeurer inoffensif, à l'intérieur d'un jeu ou d'un utilitaire, jusqu'à la date programmée de son entrée en action.

Client

Type de programme utilisé pour contacter un serveur (voir ce terme). On parle alors de modèle client/serveur. Un même serveur peut être contacté par des clients fonctionnant sur des systèmes d'exploitations différents (PC, Macintosh ou Unix).

Cookie

Un cookie est un enregistrement d'informations par le serveur dans un fichier texte situé sur l'ordinateur client, informations qui peuvent être lues ultérieurement.

Courriel

Abréviation québécoise de courrier électronique. Synonyme anglais : Electronic Mail, E-Mail, Mail. En France, on utilise mél comme synonyme d'Electronic Mail (boite aux lettres électronique d'une personne).

[D]

Dialer (Composeur, Dial, Numéroteur)
Programme permettant de composer un numéro de téléphone. Certains dialers sont fournis par les fournisseurs d'accès pour créer ou simplifier la connexion Internet de leurs clients. D'autres sont des logiciels douteux ou malveillants qui se présentent à l'internaute de manière plus ou moins trompeuse lors de l'accès à un service payant (notamment comme moyen d'accéder à des sites de charme "sans carte bancaire") ou qui s'installent à son insu pour se substituer au numéroteur de Windows et se connecter à Internet via un numéro surtaxé. Les antivirus et antispywares tels que SpyBot recherchent et éliminent généralement ce genre de dialers.

Domaine
Le domaine identifie un groupe d'ordinateurs hôtes ou de réseaux locaux qui, sous une même entité administrative, sont branchés sur le réseau Internet. Le nom des domaines se compose de sections séparées par des points. Par exemple, **uqac.uquebec.ca** désigne la composante Université du Québec à Chicoutimi de l'Université du Québec au Canada. Chaque section du nom identifie donc le domaine allant de l'information la plus particulière (**uqac**) à la plus générale (**ca**) pour Canada. Lors d'une communication entre deux ordinateurs du réseau Internet, les noms des ordinateurs et des domaines sont traduits en adresses numériques par un serveur de noms de domaine (ou *Domain name server* ou DNS).

[E]

Espiogiciel (logiciel espion)
Equivalent français de spyware.

Extranet
Partie d'un intranet accessible par des gens de l'extérieur de l'entreprise. Par exemple, une entreprise pourra donner accès à ses inventaires à des clients sélectionnés, alors que l'information ne serait pas normalement accessible à partir de l'Internet.

[F]

FAQ (Frequently Asked Questions ou Foire aux Questions)
Fichier questions-réponses. Acronyme anglais de *Frequently Asked Questions* désignant des fichiers de texte qui regroupent les questions les plus courantes sur un sujet donné. Il est fortement recommandé d'en prendre connaissance avant de poser des questions dans le cadre d'un forum. L'expression fichier FAQ (prononcer fac) fait partie du vocabulaire courant des utilisateurs d'Internet. L'équivalent français : foire aux questions.

Forum
Permet l'échange d'informations d'utilisateurs ayant un même pôle d'intérêt.

Freeware
Logiciel que son auteur a choisi de rendre absolument gratuit (pour le tester ou en faire profiter la communauté).

FTP (File Transfer Protocol)
Protocole d'échange de fichiers. Permet le téléchargement de tous types de fichiers entre une machine distante et une machine locale ou inversement. Les sites ouverts au public le sont le plus souvent en mode "anonyme".

[H]

Host (ou Hôte)
Dans un environnement réseau, l'hôte est un ordinateur habituellement de moyenne ou grande capacité sur lequel se branchent des ordinateurs clients dans le but de lui faire exécuter des logiciels particuliers ou d'y consulter de l'information. Dans le monde Internet, l'ordinateur client est souvent branché sur un premier ordinateur hôte par une ligne téléphonique. Cet ordinateur hôte établit ensuite les communications nécessaires avec d'autres ordinateurs pour trouver les logiciels ou les informations demandées.

HTML (HyperText Markup Language)
Sigle de *HyperText Markup Language* désignant le langage de création des pages-écrans sur Internet, ce qui se compare aux styles dans un logiciel de traitement de texte. HTML est un sous-ensemble plus convivial du *Standard Generalized Markup Language* (SGML).

HTTPS
Protocole de communication utilisé pour l'accès à un serveur Web sécurisé. Si l'on indique HTTPS dans l'URL au lieu de la mention HTTP normale, le message sera adressé vers un port d'entrée sécurisé du serveur. Le dialogue entre le navigateur Web et le serveur sera alors géré avec des contraintes de sécurité. En particulier, les échanges de données seront cryptés et le serveur sera identifié.

Hypertexte
Organisation d'un document textuel informatisé et caractérisé par l'existence de liens dynamiques (*hot links*) entre ses différentes sections. Dans un navigateur Web, les liens sont créés à l'aide de mots soulignés ou d'icônes sur lesquelles on clique à l'aide de la souris. Ils ont pour but de faciliter le cheminement du lecteur dans le document, ou vers un autre lien, une autre page Internet, une application…. En effet, deux lecteurs d'un même document ne consultent pas nécessairement le même contenu.

[I]

Internet
Ensemble ouvert de réseaux d'ordinateurs reliés entre eux à l'échelle de la planète qui, à l'aide de logiciels basés sur le protocole TCP/IP, permet aux utilisateurs de communiquer entre eux et d'échanger de l'information

Intranet
Les mêmes concepts et les mêmes types de service que l'Internet mais appliqués à un certain nombre d'utilisateurs. L'accès restreint à un Intranet est le plus souvent réalisé par un identifiant, un mot de passe et parfois l'adresse IP des machines.

[J]

Java
Langage de programmation développé par SUN qui permet de développer de petites applications modulaires (appelées, en anglais, *applets*) pouvant être exécutées à l'aide d'un logiciel de navigation sur n'importe quelle plate-forme

[K]

Keylogger
Logiciel qui enregistre les frappes au clavier pour voler, par exemple, un mot de passe.

[M]

Mailbomb

Message envoyé en de multiples exemplaires lors d'une opération de mailbombing. Il s'agit d'un courrier électronique vide, revendicatif voire injurieux, souvent accompagné d'un fichier joint volumineux afin d'encombrer plus rapidement la boîte aux lettres de la victime. Ce fichier joint peut être un virus, ce qui est surtout symbolique car face à un bombardement de messages par centaines le destinataire comprend en général instantanément qu'il est la cible d'une attaque.

Mailbombing

Attaque basique qui consiste à envoyer des centaines, des milliers ou des dizaines de milliers de messages appelés "mailbombs" à un unique destinataire dans un but évidemment malveillant. Ce dernier va du simple encombrement de boîte aux lettres, avec possibilité de perte de données en cas de saturation de la capacité de stockage, jusqu'au crash machine ou déni de service. Comme en cas de spamming, il est éventuellement possible d'identifier l'agresseur et de porter plainte, mais les fournisseurs d'accès peuvent également spontanément détecter de telles attaques par la hausse d'activité suspecte voire la dégradation de performance qu'elles entraînent. Le mailbombing est illégal et sévèrement puni par la loi : le 24 mai 2002, un internaute français a été condamné à quatre mois de prison avec sursis et 20 000 euros de dommages intérêts pour avoir voulu ainsi se venger d'un rival amoureux.

Malware

Contraction de "malicious software", le terme Malware désigne les programmes spécifiquement conçus pour endommager ou entraver le fonctionnement normal d'un système, tels que les virus, les vers, les chevaux de Troie, ainsi que certains java scripts ou applets java hostiles. Cette famille ne doit pas être confondue avec les spywares (espiogiciels), autre famille de logiciels dont le fonctionnement est également contestable mais dont le but premier n'est pas de nuire à l'intégrité d'un système. Les antivirus détectent et éliminent une grande partie des Malwares sans toutefois pouvoir jamais atteindre 100% d'efficacité 100% du temps : il reste donc indispensable de n'exécuter un programme ou un fichier joint que si sa sûreté est établie avec certitude, le doute profitant toujours aux Malwares.

[N]

Navigateur

Logiciel de navigation sur Internet. Le premier logiciel de ce type, Mosaic, a été conçu par le NCSA (*National Center for Supercomputing Agency* à l'Université de l'Illinois) dans l'environnement Unix. On en trouve des versions gratuites (selon certaines conditions) pour Windows et Macintosh. Quelques logiciels de navigation Web concurrents gagnent maintenant la préférence de nombreux utilisateurs. Mentionnons Netscape Communicator qui domine le marché et Microsoft Internet Explorer

Numéro de version (d'un logiciel)

Les éditeurs de logiciels cherchent souvent à améliorer leurs produits pour les doter par exemple de nouvelles fonctionnalités. Le nom d'un logiciel ne change pas pour autant mais il est suivi d'un numéro incrémentiel qui identifie la version du produit parmi celles déjà distribuées ou en cours de développement (ex. : Internet Explorer 6.0 est une version plus récente du navigateur Internet Explorer 5.5). Lorsque plusieurs versions d'une même application sont disponibles, il est en général recommandé de ne pas opter pour la toute dernière si celle-ci est très récente (sauf si elle corrige une faille importante), du fait d'un nombre de bogues potentiellement importants, ni pour les plus anciennes, pour lesquelles il n'est généralement plus publié de correctif, ou dont les failles ne sont même plus annoncées.

Numéroteur

Equivalent français de dialer.

[P]

Page Web
Unité de base du regroupement de l'information sur Internet. Une page Web est un document regroupant du texte, des images, des formulaires ou d'autres composantes multimédias. Une page est accessible grâce à son adresse URL.

Paquet
De l'anglais *packet*, désigne le regroupement d'un certain nombre d'octets (caractères ou données) transitant ensemble sur le réseau Internet. Une communication est généralement composée de plusieurs paquets qui voyagent indépendamment sur le réseau et sont regroupés au point d'arrivée.

Passerelle
De l'anglais *Gateway*, désigne un ordinateur dont la fonction est de relier deux ou plusieurs ordinateurs ou réseaux en effectuant les traductions nécessaires pour que les données soient reconnues par les différents systèmes.

De l'anglais *bridge*, désigne un équipement de télécommunication qui fait le lien entre deux sections d'un réseau.

Polluriel
Equivalent français de email Spam (Spam par courrier électronique).

Porte dérobée
Equivalent français de Backdoor.

Pourriel
Nom générique - contraction de "poubelle" et de "courriel" - désignant les courriers électroniques inopportuns ou intempestifs qui finissent à la poubelle dès réception. D'après l'OQLF, le pourriel comprend les courriels envoyés par spamming (essentiellement les publicités sauvages) et par mailbombing (notamment les messages infectés par certains virus capables de s'envoyer en plusieurs dizaines d'exemplaires aux mêmes internautes en un temps réduit). On peut également y ajouter les hoax, ces "canulars du Web" qui devraient constituer la prochaine bête noire des internautes. Pourriel est également utilisé comme synonyme français de Spam.

[R]

Réseau
Ensemble d'ordinateurs rassemblés par un lien de communication à un ou plusieurs ordinateurs serveurs. Un réseau local (LAN pour *Local Area Network*) relie des ordinateurs situés à proximité les uns des autres. Il peut être relié à d'autres réseaux dans un même édifice (réseau local d'un immeuble ou BAN pour *Building Area Network*) ou dans plusieurs villes (réseau étendu ou WAN pour *Wide Area Network*). Un réseau local, quelle que soit son envergure, peut être relié au réseau Internet dès que l'un de ses ordinateurs y est branché.

Réseau numérique à intégration de service (RNIS)
Lien de communication à haute vitesse utilisant tout de même les lignes téléphoniques existantes et permettant la transmission simultanée de la voix et des données. En anglais: *Integrated Service Digital Network* (ISDN). D'abord destiné aux entreprises, ce lien devient financièrement de plus en plus accessible aux particuliers. Une communication RNIS de base est dotée d'une bande passante de 128 kbs (deux canaux de 64 kbs).

[S]

Serveur
Ordinateur dont les logiciels, les données ou certaines ressources (comme une imprimante ou un modem) sont partagés par les utilisateurs de micro-ordinateurs reliés au même réseau. Dans le monde Internet, serveur désigne parfois les ordinateurs hôtes.

Spam
Message intempestif envoyé à une personne ou à un groupe de personnes lors d'une opération de spamming. Il faut prendre l'habitude de supprimer ce genre de messages sans les lire et en ne cliquant sur aucun lien (y compris le lien de désabonnement), afin de ne pas encourager cette pratique et ne pas en recevoir soi-même davantage. Spam est également couramment employé pour désigner le seul polluriel (email Spam).

Spamming
Usage abusif d'un système de messagerie électronique ou de traitement automatisé de données destiné à exposer délibérément et généralement de manière répétée tout ou partie de ses utilisateurs à des messages ou à des contenus non pertinents et non sollicités couramment appelés "Spams", en faisant en sorte de les confondre avec les messages ou les contenus habituellement échangés ou recherchés par ces utilisateurs. Le spamming s'accompagne souvent de la part du spammer d'une ou plusieurs pratiques généralement reconnues comme illégales au niveau mondial (usurpation d'identité, collecte déloyale de données personnelles, contrefaçon de marque, escroquerie, entrave volontaire à un système,...), mais ces pratiques sont à considérer comme des circonstances aggravantes et non des caractéristiques intrinsèques du spamming. Sont par exemple considérés comme des actes de spamming le fait d'envoyer un courriel à un inconnu pour lui demander de visiter un site ou d'acheter un produit, ou encore le fait de poster dans un forum des messages sans rapport avec le thème abordé.

Spyware
Programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

[T]

TCP/IP
Sigle de *Transmission Control Protocol/Internet Protocol*, protocole de commande de transmission/protocole Internet.

Telnet
Protocole permettant à l'utilisateur de relier par modem son ordinateur à un ordinateur central et de le faire fonctionner comme s'il s'agissait d'un terminal.

Trappe arrière
Equivalent français de Backdoor.

[U]

Utilitaire de désinfection
Petit programme permettant de rechercher et d'éliminer un nombre limité de virus. Il s'agit exclusivement d'un scanner à la demande utilisant une analyse par signatures et dont les définitions de virus ont été limitées à un seul ou quelques virus. Mis à disposition par les éditeurs d'antivirus, principalement lors des épidémies importantes, il permet aux utilisateurs ne possédant pas d'antivirus ou dont l'antivirus aurait été rendu inutilisable de tout de même désinfecter leur ordinateur. Ne disposant pas de moniteur pour surveiller le système en temps réel, l'utilitaire de désinfection est incapable d'empêcher une nouvelle contamination si l'utilisateur exécute à nouveau un fichier contaminé ou s'il ne comble pas la faille logicielle possiblement utilisée par le virus pour s'exécuter automatiquement.

[V]

Virus
Programme ou code malicieux inclus généralement dans un format de fichier couramment utilisé et stocké dans un système d'exploitation à l'insu de son utilisateur. Ce code est susceptible de s'auto exécuter à un moment précis ou lors du lancement d'un logiciel. Objectif : rendre le système hors d'usage en détruisant certains fichiers indispensables ou en saturant les ressources de la machine.

Ver (Worm)
Type de virus particulier. Concrètement, il s'agit de programmes capables de se répliquer à travers les terminaux connectés à un réseau, puis d'exécuter certaines actions pouvant porter atteinte à l'intégrité des systèmes d'exploitation.

[W]

World Wide Web (WWW)
Concept de présentation de l'information en mode hypertexte dans Internet. C'est la façon par excellence de naviguer dans Internet en termes de facilité d'usage, de qualité de présentation et de variété de contenus. Les documents WWW, conçus à l'aide du langage HTML, peuvent regrouper du texte, des images, du son, de la vidéo ou des adresses menant à d'autres sites. Le CERN, un centre suisse de recherche en physique, avait mis au point le WWW pour ses propres besoins et, ensuite, le concept s'est largement répandu.

Editeur :
Agnitum Ltd
Acropoleos Avenue 8
Mabella Court
Nicosia, Cyprus
info@agnitum.com.

Distributeur en France :
ATHENA Global Services
20 allée Louis Calmanovic
93320 Les Pavillons-sous-bois
Tel 01 55 89 08 88
Email athena@athena-gs.com
Site Web www.athena-gs.com

Support Technique :
Tel 01 55 89 08 88
Fax 01 55 89 08 89
Email supportoutpost@athena-gs.com
Site Web www.agnitum.com/support (site en anglais)