****
sateduc
****
Comment votre PC peut-il être piraté sur Internet ?

Comment votre PC peut-il être piraté sur Internet ?

Toujours le fait de personnes malveillantes, les risques inhérents à la sécurité informatique sont nuisibles à différents degrés.
Votre ordinateur est exposé à une multitude de risques de piratage via Internet qu'il est possible de regrouper selon deux catégories principales :

- La prise de contrôle à distance de votre ordinateur : bien souvent, un pirate prend le contrôle de votre PC (sans qu'aucun signe ne vous alerte) et l'utilise pour lancer une attaque beaucoup plus sévère contre un autre ordinateur connecté comme vous au réseau Internet. Son identité restera donc secrète puisque son méfait aura été lancé à partir de votre ordinateur.

- Le détournement d'informations vous concernant : dans ce cas, le pirate est capable de lire l'ensemble des fichiers enregistrés sur votre disque dur : courrier, documents personnels, liste d'adresses postales ou e-mails, etc. Outre la violation de votre vie privée, l'intrus peut récupérer des données beaucoup plus sensibles telles que des numéros de compte en banque, de cartes bancaires ou, dans le cas des entreprises, des informations confidentielles.

Le piratage nous concerne tous
Depuis l'avènement de l'ère Internet à la fin de années 90, le nombre d'ordinateurs connectés à Internet ne cesse d'augmenter. Internet étant un réseau mondial, libre de tout contrôle, il présente de nombreux avantages : échange gratuit d'information en temps réel, communication instantanée par e-mails, messagers ou par visioconférence, etc.
Malgré ses nombreux avantages, le plus grand des réseaux présente néanmoins des risques avérés en matière de sécurité informatique dont vous avez déjà probablement entendu parler. Ainsi, certaines personnes malveillantes n'hésitent pas à utiliser certaines failles logicielles et matérielles pour s'approprier des données personnelles ou confidentielles à votre insu. C'est également en utilisant cette voie que les pirates du Net diffusent virus et autres logiciels informatiques nuisibles quelques fois destinés à prendre le contrôle de votre ordinateur. Un ordinateur connecté à Internet sans aucune précaution s'expose donc à l'attaque de ses données.

Quel est le risque d'une connexion ADSL ou d'un modem câble ?
Si vous disposez d'une connexion haut débit ADSL ou via le câble actif en permanence, les risques sont plus grands car votre ordinateur n'est pas une cible mouvante. Ainsi, lorsque vous utilisez une connexion d'accès à distance, l'adresse réseau de votre ordinateur est différente à chaque fois ; avec une connexion ADSL ou câble, en revanche, l'adresse réseau est inchangée pendant de longues périodes de temps (24 h. maximum). Si cette connexion permanente est un avantage, l'adresse de votre ordinateur est encore plus exposée aux pirates. Il existe également un risque lié au partage de la connexion : les personnes qui, dans votre entourage, partagent le même service de câble, peuvent potentiellement accéder à votre ordinateur si vous ne disposez d'aucune protection par pare-feu (ou firewall).

Que peut faire un pirate qui s'est introduit dans mon ordinateur ?
Non seulement les pirates cherchent à accéder à des informations privées, telles que des enregistrements financiers ou des fichiers de mots de passe, mais ils se servent aussi des ordinateurs aux fins suivantes :

- Lancer des attaques de déni de service (DoS - Denial of Service) contre un site Web en vue.
Après en avoir pris le contrôle, le pirate peut contraindre votre ordinateur ainsi que des centaines, voire des milliers d'autres "zombies" à agir simultanément, ce qui surcharge un site populaire et provoque son indisponibilité.

- Distribuer des logiciels de façon illicite.
Après s'être approprié l'espace sur votre disque dur, ils permettent à d'autres d'accéder à votre ordinateur en tant que site "warez" et de télécharger des divertissements ou des applications piratées.

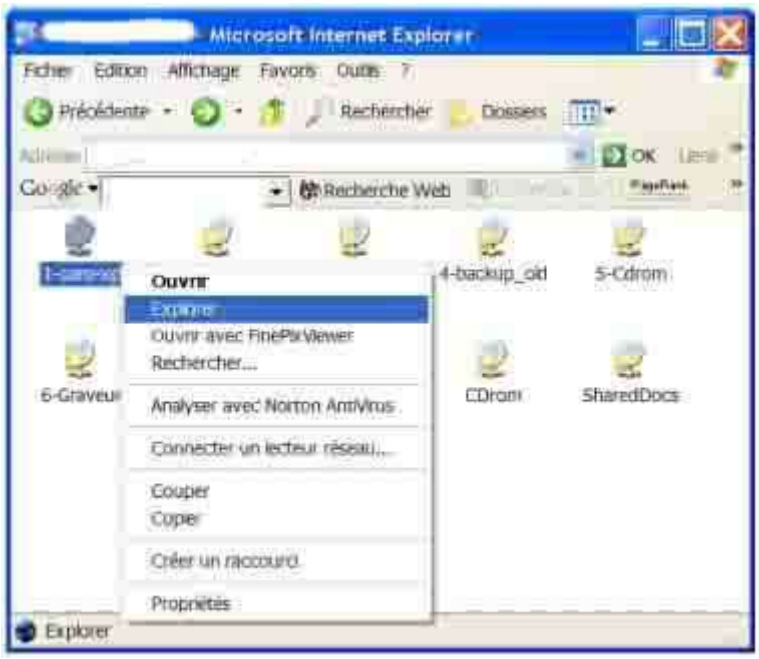
le piratage par l'attaque IP

De nombreux particuliers possédant un ordinateur personnel estiment ne pas avoir besoin de protéger les données contenues sur leurs disques durs. Il est en effet peu probable qu'un pirate de l'Internet s'intéresse à la photo du chat ou des enfants. En effet, le vrai pirate s'attaque en général aux serveurs afin d'en récupérer les données qu'il pourra revendre par la suite. Mais il est une catégorie de pirates amateurs qui se feront le plaisir de s'entraîner sur un ordinateur personnel avant de passer à l'échelon supérieur. C'est de cette catégorie qu'il est nécessaire de se protéger.
Vous êtes un particulier et vous doutez encore ? Suivez attentivement notre exemple :

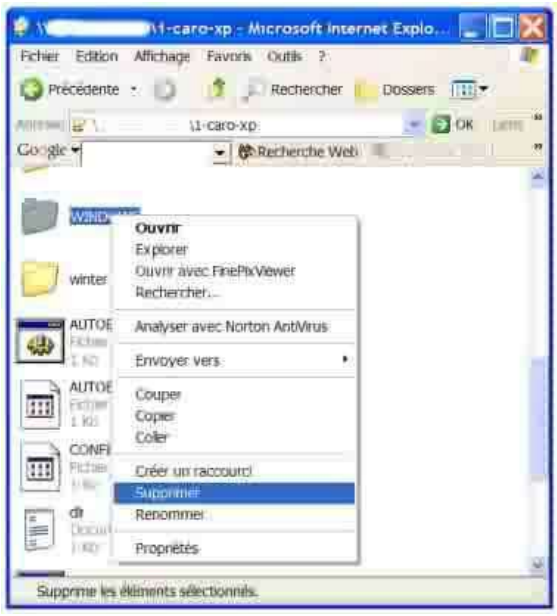
Etape 1 :vous trouverez très facilement sur Internet un logiciel permettant de récupérer les adresses IP de chaque ordinateur connecté au réseau Internet. L'IP est une sorte d'immatriculation ou d'adresse de votre ordinateur à un instant t sur le réseau internet. Ce récupérateur d'adresses IP appelé scanner invotorie donc toutes les adresses IP utilisées par les ordinateurs connectés à Internet au même moment. Le nombre d'IP étant de plus plusieurs milliards, la recherche d'IP se fait par tranche d'adresse : ici de 212.194.132.1 à 212.194.132.254. ATTENTION : l'utilisation d'un scanner de port ou d'IP est considéré en soi comme un acte de piratage même si vous ne pénétrez pas au

sein des ordinateurs dont l'IP est listée. cette exemple est à but pédagogique et ne doit pas être en aucun cas considéré comme une incitation au piratage.

Etape 2 : Certains de ces ordinateurs connectés peuvent contenir des répertoires ou des disques durs partagés. Il s'agit d'éléments communs accessibles par plusieurs utilisateurs au sein d'un réseau. Le logiciel que nous utilisons permet également de savoir si un ordinateur contient ce type de répertoire ou ce type de disque.
Il suffit alors de taper l'adresse IP de l'ordinateur en question dans un navigateur Internet (Internet Explorer par exemple) pour pouvoir afficher ses ressources partagées et y entrer comme si vous exploriez un des répertoires situés sur votre ordinateur.
Ici le contenu d'un ordinateur relié à Internet. Son utilisatrice qui s'appelle probablement Caroline possède plusieurs disques durs partagés dont le disque dur principal "Caro-XP" (Nous supposons qu'il s'agit du disque contenant le système d'exploitation Windows XP). La navigation entre les répertoires et les données sur un ordinateur distant est identique à celle que vous utilisez couramment sur le votre.

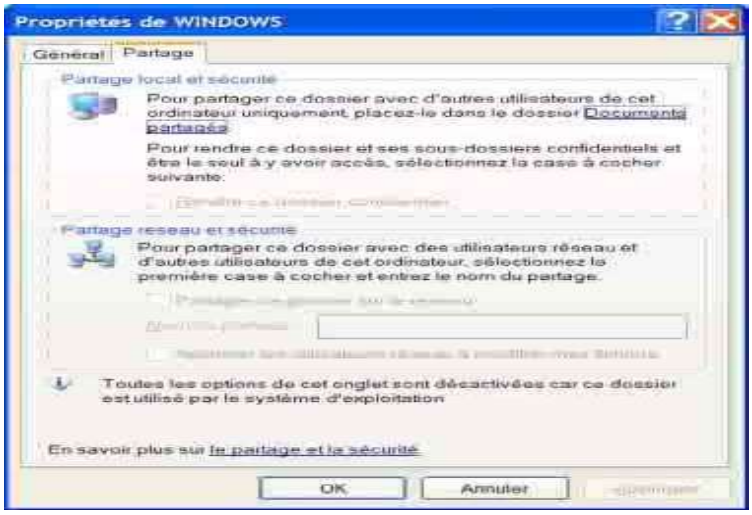


Etape 3 : Le disque dur Caro-XP contient le répertoire Windows ainsi que les fichiers utilisés lors du démarrage de l'ordinateur. Il est alors possible d'effectuer sur ces éléments toute sorte d'opérations ; modification du nom du dossier ou suppression de ce répertoire par exemple. L'utilisatrice de cet ordinateur ne pourrait de ce fait plus démarrer son ordinateur. Nous n'irons pas bien sûr jusque là, le but de notre exemple étant de vous montrer que les données de vos disques durs, même les plus importantes sont vulnérables dés lors que vous surfez sur Internet sans aucune protection. Notez qu'un mauvais pirate supprime vos données… un pirate qui se respecte vous prévient en créant ou en renommant un fichier, guère plus.

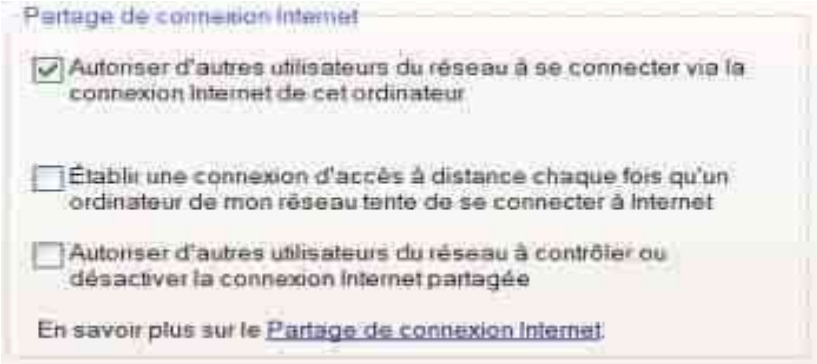


Comment se protéger des attaques par Internet

Protection des partages de fichiers
Windows XP utilise un modèle d'accès réseau appelé "partage de fichiers simple" où toutes les tentatives de connexion à l'ordinateur à distance sont contraintes d'utiliser le compte Invité.
Dans le modèle de partage de fichiers simple, il est possible de créer des partages de fichiers pour que l'accès à partir du réseau soit limité à la lecture ou étendu à la lecture, la création, la modification et la suppression de fichiers. Ce modèle est destiné à une utilisation en réseau domestique et derrière un pare-feu tel que celui fourni par Windows XP. Si vous êtes connecté à Internet sans être protégé par un pare-feu, vous devez garder à l'esprit que tous les partages de fichiers que vous créez risquent d'être accessibles à n'importe quel utilisateur d'Internet.
Pour contrôler les partages de fichiers, ouvrez votre Explorateur Windows.
Faites un clic avec le bouton droit de la souris sur le dossier de votre choix, ce peut être le disque dur lui même, puis cliquez sur l'onglet Partage et sécurité. Dans la fenêtre Propriétés, activez les options de partage de votre choix. Cliquez sur le bouton Appliquer afin de prendre en compte les modifications.
Il est néanmoins fort déconseillé d'autoriser les utilisateurs distants à modifier vos données. Ces derniers peuvent être des collègues de travail dont l'ordinateur est en réseau avec le votre ou des internautes cherchant à vous pirater.



Utilisez le partage de connexion pour les connexions Internet partagées
Windows XP vous donne la possibilité de partager une même connexion Internet entre plusieurs ordinateurs d'un réseau domestique ou de petite entreprise grâce à la fonctionnalité de partage de connexion Internet. L'un des ordinateurs, appelé hôte, se connecte directement à Internet et partage sa connexion avec les autres ordinateurs du réseau. Les ordinateurs clients dépendent de l'hôte pour obtenir l'accès à Internet. Ce fonctionnement améliore la sécurité dans la mesure où seul l'hôte est visible sur Internet :
Pour activer le partage de connexion internet, cliquez avec le bouton droit sur une connexion Internet dans Connexions réseau, cliquez sur Propriétés, cliquez sur l'onglet Avancé, puis cochez la première case.



Utilisation d'un pare-feu ou Firewall
Des millions d´ordinateurs sont aujourd'hui connectés au réseau Internet, du simple particulier à la grosse entreprise. Or être connecté signifie ouvrir son ordinateur au monde extérieur. La fonction de base d´un pare feu (ou firewall) est simple : il bloque tous les échanges entre un ordinateur et l´extérieur (que cela soit un réseau local ou Internet). C´est l´utilisateur qui, par la suite, détermine les autorisations d´accès aux programmes communiquant avec l´extérieur.
Principe du Firewall ou pare-feu
A chacune de vos connexions au réseau Internet, une adresse IP (x.x.x.x) est attribuée à votre ordinateur par le fournisseur d'accès auquel vous avez souscris un contrat de connexion. Cette adresse permet d'identifier l'ordinateur sur le réseau. Elle est unique et dynamique, c'est à dire qu'elle change à chaque reconnexion (sauf cas particuliers : certains ordinateurs d'entreprise ont une adresse IP fixe).

Cette adresse est utilisée par les pirates pour pénétrer, ou tenter de le faire sur un ordinateur. Dès que l'adresse IP d'un ordinateur est trouvée, il suffit de scanner les ports pour voir quels sont ceux qui sont ouverts.
Un ordinateur PC sous Windows dispose de 65000 ports soit 65000 portes d'entrée différentes pour y accéder. Si tous ces ports ne sont pas accessibles, certains peuvent être utilisés pour pénétrer à l'intérieur d'un ordinateur. Il faudra toutefois qu'il y ait un programme présent sur l'ordinateur, permettant d'en prendre le contrôle de l'extérieur. Ici intervient le concept de Cheval de Troie (Trojan Horse). Un Cheval de Troie est un programme installé sur l'ordinateur, souvent à l'insu de son utilisateur. Ce programme pourra être "activé" de l'extérieur, en utilisant un des ports de l'ordinateur. Une fois activé, il permettra à l'utilisateur de l'ordinateur distant, de prendre tout ou partie du contrôle de l'ordinateur local.

Pour éviter cela, il faut :
- vérifiez la présence ou non d'un Cheval de Troie sur votre ordinateur avec un antivirus.
- utiliser un firewall pour bloquer les ports et ainsi empêcher l'intrusion ou la prise de contrôle à distance de votre PC.
- Il est également vivement recommandé de mettre à jour fréquemment son Windows en utilisant Windows Update. Ceci corrigera les éventuelles failles découvertes dans le système d'exploitation.

Le firewall bloque les ports disponibles, et ne laisse ouverts que ceux qui sont nécessaires à l'utilisateur.

Les ports utilisés fréquemment par votre ordinateur
Ports 20 et 21 : FTP téléchargement de fichiers
Port 25 : SMTP envoi de courrier
Port 80 : HTTP navigateur Internet
Port 110 : POP3 réception de courrier
Port 119 : NNTP forums de discussion
Port 1014 : Utilisé pour le partage de fichiers sous le logiciel Kazaa

A signaler qu'AOL utilise les ports 5190 à 5193 (c'est pour cette raison qu'il n'est pas possible d'utiliser Outlook Express avec une connexion de ce fournisseur d'accès).

Merci a l'auteur

& également un grand Merci à …stephil…

****

sateduc

****