



### Symantec Security Check

- Vérifiez tout de suite la sécurité de votre ordinateur en ligne avec le Symantec Security Check :  
<http://security.symantec.com/fr>

**Symantec France**  
Immeuble River Seine  
25, quai Gallieni  
92150 Suresnes



# DU PC AU TELEPHONE PORTABLE : QUELS SONT LES RISQUES ?



# LES MENACES INTERNET

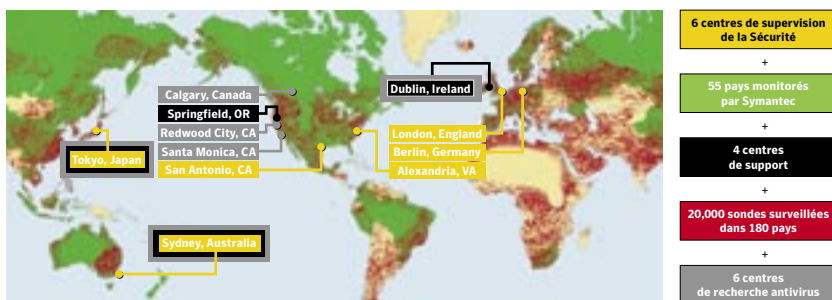
**Virus, vers, codes malicieux. Spam, phishing, chevaux de troie. Nos réseaux de communication ne sont pas sans faille. Mais pas non plus sans défense.**

## ANALYSER LES DANGERS

Tous les six mois, Symantec™ – leader mondial de la sécurité de l'information – répertorie et analyse l'activité des menaces Internet au sein d'un rapport, l'Internet Security Threat Report (ISTR). Ce guide vous offre une synthèse claire et précise de cette 7<sup>ème</sup> édition de l'ISTR, pour mieux comprendre les dangers qui vous entourent sur Internet, et mieux vous en prémunir.

## UN CENTRE DE GESTION ET DE CONNAISSANCE UNIQUE DES MENACES

20000 capteurs dans 180 pays + 190 Millions de clients Symantec dans le monde



Pour produire ce rapport sur les menaces liées à Internet, Symantec dispose d'une base de données parmi les plus exhaustives au monde : 9000 vulnérabilités répertoriées parmi 2000 fournisseurs dans 180 pays, et les remontées de ses 120 millions d'utilisateurs antivirus. Loin des spéculations théoriques, ces données réelles permettent à Symantec de protéger efficacement les systèmes, et mieux cerner les menaces émergentes.



## **NOUVELLES MENACES : LES DONNÉES CLÉS**

Les menaces pesant sur les informations confidentielles n'ont cessé d'augmenter au cours des trois derniers semestres.

**366 %** : le taux d'augmentation des tentatives de phishing (récupération d'informations confidentielles - voir p.8) sur le second semestre 2004.

**48 %** : c'est ce que représente les attaques contre les applications web sur toutes les vulnérabilités (voir p.4).

**7 360** : le nombre de nouvelles variantes de virus Windows 32 bits enregistrées.

Augmentation notable des vulnérabilités graves (voir p.4), facilement exploitables, même à distance.

# L' INFAILLIBILITE N'EXISTE PAS

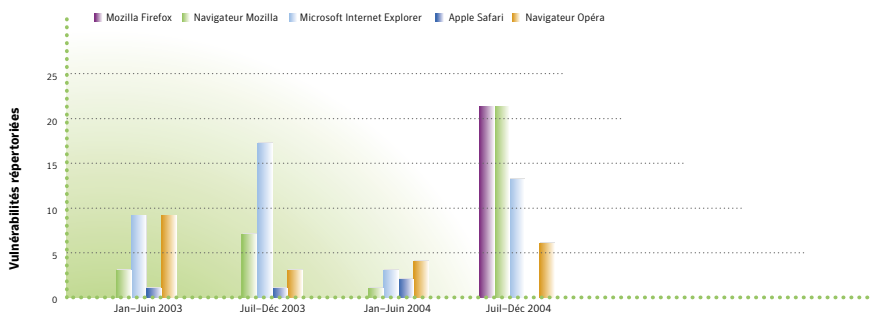
**Les ordinateurs qui composent le réseau Internet subissent chaque jour un nombre sidérant d'attaques malveillantes. Et même si tout problème a sa solution, tout va très vite sur Internet.**

## VULNÉRABILITÉ

Il existe presque toujours un moyen (au moins) de détourner le fonctionnement normal d'une application. 70 % des failles répertoriées par Symantec sont d'ailleurs très facilement exploitables (bien souvent il suffit d'un simple outil trouvé sur Internet pour pirater un ordinateur), et 80 % d'entre elles le sont à distance. Quant aux navigateurs web, les pirates ayant d'abord ciblé Microsoft Explorer, nombre d'internautes ont choisi d'autres navigateurs – comme Mozilla, Opera ou Firefox. Bien évidemment, les cybercriminels se sont adaptés en recherchant les failles de ces navigateurs-là.

### 13% DE FAILLES EN PLUS SUR LE DERNIER SEMESTRE 2004

Les failles dans les applications web (logiciels résidant sur les serveurs Internet) sont particulièrement inquiétantes. Elles permettent aux attaquants de contourner les mesures de sécurité (« firewalls ») traditionnelles afin d'accéder à des informations confidentielles stockées sur d'autres parties d'un réseau, normalement inaccessibles depuis l'extérieur.



**LES VULNÉRABILITÉS RÉPERTORIÉES PAR NAVIGATEUR, JAN 2003 - DÉC 2004**

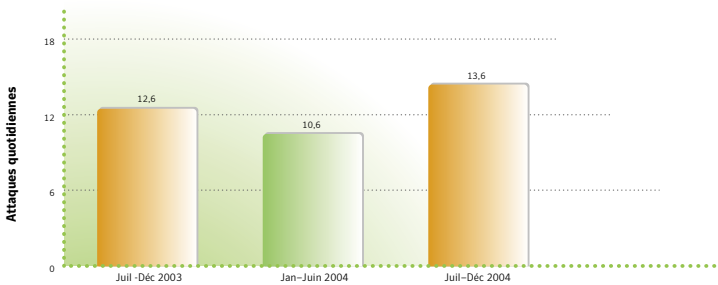
SOURCE : SYMANTEC CORPORATION

# ATTAQUE

Une attaque est une tentative d'exploitation d'une faille dans un système informatique ou un logiciel. Ces attaques peuvent être détectées par des systèmes de détection d'intrusion, ou par des pare-feu. Mais l'intrusion dans un système ne représente qu'un objectif possible, certaines attaques ayant uniquement pour but de mettre le système hors fonction.

## LES ROBOTS (OU « BOTS »)

Ce sont des logiciels qui viennent, à l'insu de l'utilisateur, s'installer sur un disque dur pour en permettre la commande à distance. Une fois infecté, l'ordinateur sert à lancer d'autres attaques.



### NOMBRE DE TENTATIVES D'ATTAQUES QUOTIDIENNES PAR ENTREPRISE

SOURCE : SYMANTEC CORPORATION

Juil-Déc 2004	Jan-Juin 2004	Pays	Juil-Déc 2004	Jan-Juin 2004
Rang	Rang		% d'évènement	% d'évènement
1	1	États-Unis	30 %	37 %
2	2	Chine	8 %	6 %
3	3	Allemagne	8 %	5 %
4	4	Corée du Sud	4 %	30 %
5	5	Canada	4 %	6 %
6	6	Grande Bretagne	4 %	4 %
7	7	France	3 %	4 %
8	-	Japon	3 %	-
9	9	Espagne	3 %	3 %
10	-	Italie	2 %	-

### TOP 10 DES PAYS EMETTEURS D'ATTAQUES

SOURCE : SYMANTEC CORPORATION



#### PRÉCAUTIONS DE BASE

- Tester la vulnérabilité de votre disque dur sur [www.symantec.com/securitycheck](http://www.symantec.com/securitycheck).
- Utiliser Windows XP Service Pack 2 de Microsoft.

# LES CODES MALICIEUX

**Un nom générique pour ceux qu'on appelle communément « les virus ». Sur Internet, on les trouve partout.**

**Et Internet, c'est un peu chez vous.**

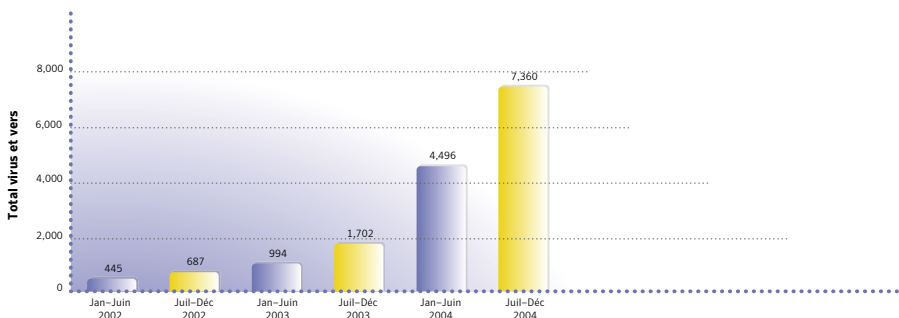
Vous avez certainement déjà reçu un courrier électronique d'origine inconnue contenant une pièce jointe. A l'intérieur se cachait très probablement un virus. Mais qu'est-ce qu'un virus ? C'est un programme inclus dans un format de fichier couramment utilisé qui va se stocker dans un système d'exploitation. Susceptible de s'exécuter tout seul, à un moment précis ou au lancement d'un logiciel, son objectif est de rendre le système hors d'usage, en détruisant certains fichiers indispensables ou en saturant les ressources de la machine. Mais attention, un virus peut prendre plusieurs formes (comme les vers, qui circulent de façon autonome sur Internet), et suivre différents itinéraires (messageries instantanées, lecteurs réseau, WIFI...).

Rang	Code
1	Netsky.P
2	Sober.I
3	Gaobot
4	Spybot
5	Beagle.AV
6	Beagle.X
7	Mydoom.M
8	Netsky.Z
9	Netsky.D
10	Beagle.AW

**TOP 10 DES CODES MALICIEUX 2004**

SOURCE : SYMANTEC CORPORATION

**7 360** nouveaux virus répertoriés ces 6 derniers mois



**NOMBRE DE NOUVEAUX VIRUS ET VERS WINDOWS 32 BITS**

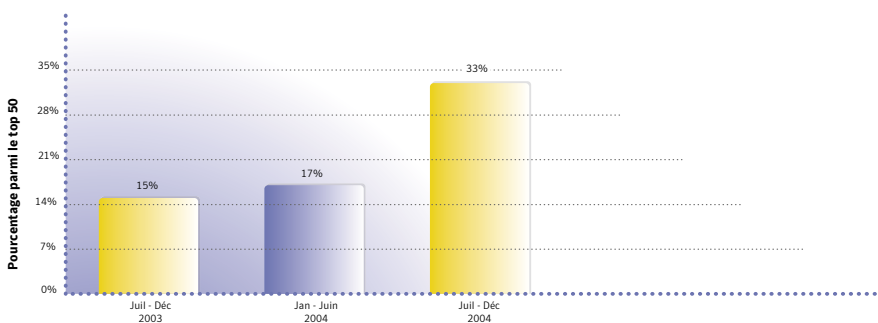
SOURCE: SYMANTEC CORPORATION

## LE CHEVAL DE TROIE

C'est un programme qui prend l'apparence d'un programme valide (par exemple un jeu, ou un utilitaire). En fait, il contient une fonction illicite cachée capable de contourner les mécanismes de sécurité. Il peut demeurer inoffensif jusqu'à la date programmée de son entrée en action. Son objectif : ouvrir une porte dérobée sur un ordinateur à l'insu de son utilisateur, permettant au pirate d'y accéder via Internet.

### 33% DES CODES MALICIEUX

Présents sur des sites exploitant les failles du navigateur Internet, ou encore intégrés à des virus, les chevaux de Troie représentent la pire menace pour vos données confidentielles.



#### PART DES CHEVAUX DE TROIE PARI MI LES 50 PREMIERS CODES MALICIEUX

SOURCE : SYMANTEC CORPORATION



#### PRÉCAUTIONS DE BASE

- Ne pas ouvrir une pièce jointe à un courrier électronique si vous avez un doute sur l'origine ou le contenu du message.
- Télécharger les correctifs fournis par les constructeurs/éditeurs pour pallier les failles.



#### CONSEILS TECHNIQUES

- Lancer régulièrement Windows Update ou le paramétrer en mode automatique.
- Installer une solution de sécurité complète (pas uniquement un antivirus) permettant de limiter les dégâts en cas « d'oubli » de téléchargement des correctifs.

# ATTEINTE A LA CONFIDENTIALITE

**Coordonnées bancaires, achats en ligne, adresses électroniques.**  
**L'objectif est simple : récupérer un maximum d'informations vous concernant.**

## LE SPAM, 60 % DES MESSAGES QUI TRANSITENT SUR INTERNET

C'est l'envoi massif de courriers électroniques, généralement publicitaires, non sollicités. Pour obtenir des coordonnées électroniques, les « spammeurs » utilisent des logiciels qui récupèrent sur Internet, dans les pages web ou les forums, tout ce qui peut ressembler à des adresses mail. Les messages spams proposent, souvent à faible coût, des produits ou des services plus ou moins légaux. Et même avec 0,001% de réponse, leur envoi est rentable. 1,2 milliard de spam (ou « courriers indésirables », « pourriels », « junk mails ») sont envoyés chaque semaine dans le monde.

**1,2** milliard de spam  
sont envoyés chaque semaine



### PRÉCAUTIONS DE BASE

- Divulguer au minimum votre adresse électronique – ne pas relayer les « messages en chaîne », ne pas laisser votre adresse e-mail sur des forums, sites de pétitions, newsgroups...
- Ne pas ouvrir les messages spams, qui confirmerait à l'expéditeur la validité de votre adresse.
- Créer une ou plusieurs « adresses-poubelles » servant uniquement à s'identifier sur des sites douteux.



### CONSEILS TECHNIQUES

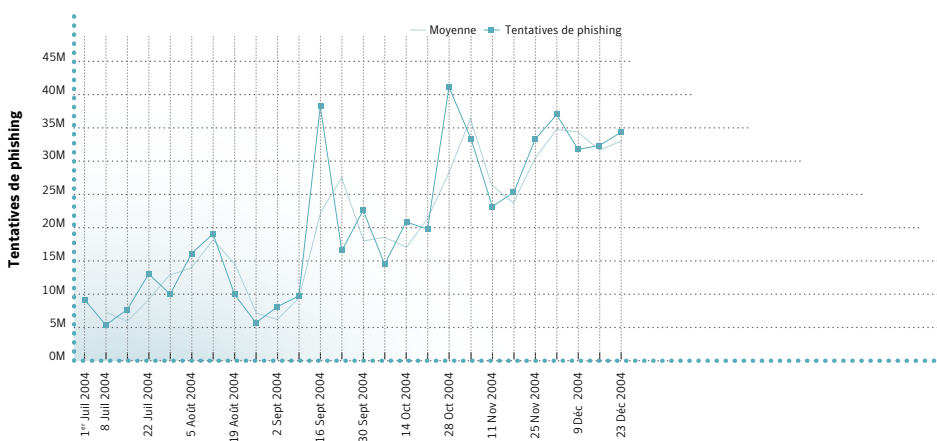
- Ne pas répondre, ni utiliser le lien en bas de page proposant de ne plus recevoir ce type de message, sous risque d'indiquer que votre adresse est active. Supprimez simplement le message.
- Mettre en place un logiciel anti-spam.

## LE PHISHING : 1 mail sur 250

C'est la récupération d'informations confidentielles (N° carte bleue, coordonnées bancaires...). Le « phishing » s'effectue par le biais d'un courrier électronique publicitaire (spam).

### Comment ça marche ?

L'internaute reçoit un e-mail usurpant l'identité d'une entreprise (notamment une banque, ou un site de commerce), l'invitant à se connecter sur une page web factice pour une mise à jour d'informations. Données qui, par exemple, permettront au « phisher » de transférer directement de l'argent sur un autre compte.



### NOMBRE DE TENTATIVES DE PHISHING BLOQUÉES PAR SYMANTEC

SOURCE : SYMANTEC CORPORATION



#### PRÉCAUTIONS DE BASE

- Ne pas ouvrir le lien contenu dans le mail, mais l'adresse d'accès au service.
- Contrôler soigneusement toute requête d'informations confidentielles.
- Ne pas divulguer les informations si vous avez un doute.



#### CONSEILS TECHNIQUES

- Si vous saisissez des informations sensibles, assurez-vous que l'adresse dans la barre du navigateur commence par https, de l'affichage d'un petit cadenas dans la barre d'état (en bas de votre navigateur), et que l'adresse correspond bien à celle annoncée (en vérifiant l'orthographe).

# LES NOUVELLES CIBLES

**Internet est aujourd'hui accessible de partout et de bien des façons.**

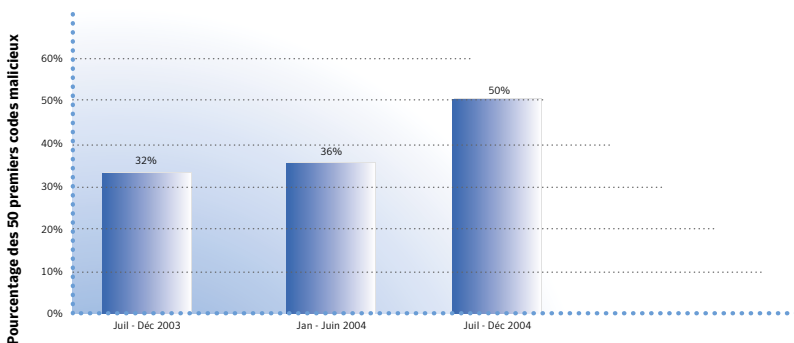
**Téléphones mobiles, assistants personnels : tous les appareils sont désormais logés à la même enseigne.**

## LA TELEPHONIE MOBILE

Qu'il s'agisse d'un simple téléphone utilisant le WAP ou du dernier « smart phone », la nouvelle génération de téléphones mobiles exploitant certains logiciels grâce à un véritable système d'exploitation, de nouveaux virus apparaissent, ciblant spécifiquement ces appareils. S'ils sont encore peu développés, ils connaissent une nette progression – en juin 2004 il n'en existait qu'un, ils sont 43 en avril 2005...

## LES RESEAUX PEER TO PEER

Les réseaux peer to peer (échange de fichiers informatiques via internet sans transit par un serveur) restent un moyen privilégié de propagation pour les codes malicieux. Les plus répandus (Netsky, MyDoom, Beagle et leurs variantes) utilisent tous, en plus du courrier électronique, le peer to peer pour se diffuser.



**PART DES VIRUS DU TOP 50 SE PROPAGEANT VIA PEER-TO-PEER ET MESSAGERIE INSTANTANÉE**

SOURCE : SYMANTEC CORPORATION

## ADWARE et SPYWARE

Les logiciels publicitaires et les logiciels espions, en forte croissance, représentent des risques supplémentaires en matière de sécurité. Ils s'installent sur votre disque dur en même temps qu'un autre programme, ou simplement durant une connexion, et transmettent à des serveurs des informations sur vos activités Internet. Ils sont également capables d'afficher des fenêtres publicitaires, de changer la page de votre navigateur et même, dans certains cas, d'enregistrer ce que vous tapez sur le clavier, y compris vos mots de passe.

## LES FUTURES TENDANCES SELON SYMANTEC

- Les robots (« bots ») vont être de plus en plus nombreux.
- Les codes malicieux visant les terminaux mobiles vont augmenter en nombre et en gravité.
- Les menaces cachées à l'intérieur des fichiers audio et vidéo vont fortement se développer.
- Les attaques ciblant les systèmes Mac OS vont s'accroître – suivant la croissance commerciale des ordinateurs et produits Apple.
- Les risques liés aux logiciels espions et publicitaires : la prochaine législation ne sera probablement pas assez efficace pour enrayer ces risques, qui vont donc continuer à sévir...

En juin 2004 il n'existait  
qu'un virus pour mobile,  
en avril 2005 ils sont

**43**



### PRÉCAUTIONS DE BASE

- Si vous téléchargez un logiciel, prenez garde à l'installation éventuelle d'un spyware. Avant de cliquer sur « oui, j'accepte les conditions d'utilisation », vérifiez les conditions de confidentialité des données – l'accord doit stipuler clairement les fonctions du logiciel, et proposer un logiciel de désinstallation.