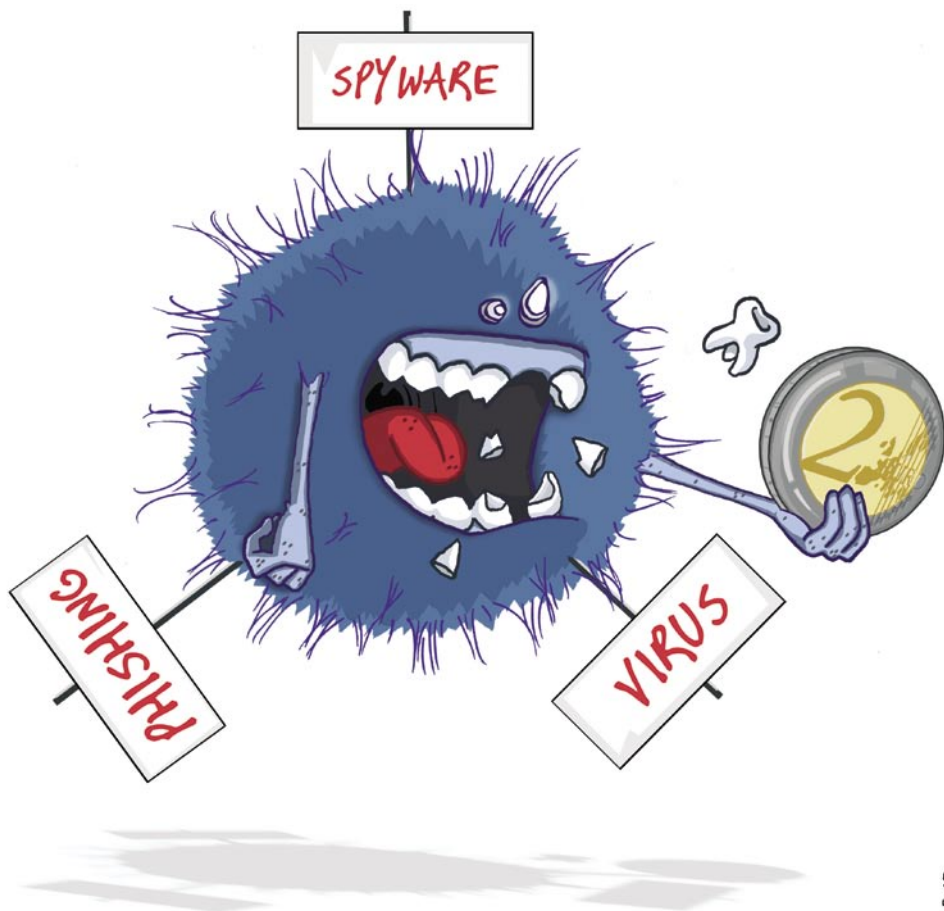


DU PC AU TELEPHONE MOBILE...

ILS EN VEULENT À VOTRE ARGENT !



F_05

VOTRE GUIDE DE LA SÉCURITÉ INFORMATIQUE PAR



symantec™

LES MENACES INTERNET

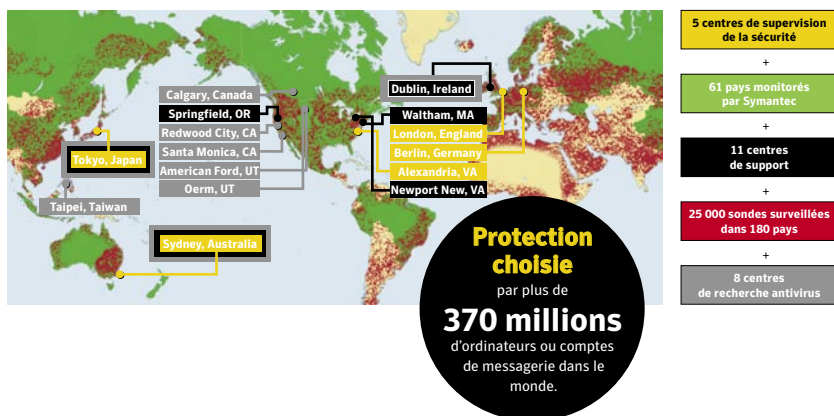
Les producteurs de codes malicieux, éleveurs de vers et autres inventeurs de virus ne manquent décidément pas d'énergie pour infecter le web. Mais les éclairages utiles et les parades efficaces existent bien. Pour les contrer, suivez le guide...

LA TOILE SOUS OBSERVATION

Tous les 6 mois, Symantec™ - leader mondial de la sécurité de l'information - édite l'**Internet Security Threat Report (ISTR)** qui recense et analyse les menaces circulant sur Internet. Ce guide vous en livre une synthèse qui se résume en 3 mots : comprendre, anticiper et se prémunir.

UN CENTRE DE GESTION ET DE CONNAISSANCE UNIQUE DES MENACES

180 pays - 190 millions de clients sous protection - 2 millions d'adresses électroniques leurres



Cette veille semestrielle permet non seulement de répertorier les menaces mais surtout d'en mesurer les évolutions. Véritable baromètre de la sécurité, l'Internet Security Threat Report vous permet de comprendre les dangers actuels comme ceux à venir. Tirez-en profit et suivez les « trucs et astuces » de ce guide pour vous protéger intelligemment des dangers d'Internet.



LA TENDANCE FORTE : VOTRE ARGENT LES INTÉRESSE

- **Récupération de vos données** : le phénomène remarqué dans l'édition précédente se confirme. Les tentatives de corruption des machines et des utilisateurs sont en plein boom.
- **Accroissement du "phishing"** : les messages électroniques non sollicités progressent. Parallèlement, leur objectif pécuniaire se renforce : abuser l'internaute pour lui soutirer des informations bancaires confidentielles.

CHIFFRES PARLANTS : LES MENACES EN HAUSSE PREMIER SEMESTRE 2005

De 2,99 millions à 5,70 millions
de messages de "phishing" par jour pour la même période par rapport
au second semestre 2004

59 % des failles repertoriées concernent les applications web

10 866 nouveaux virus Windows 32 bits ont été recensés

A L'AFFUT DE LA FAILLE

Triste record ce semestre, le nombre de failles a explosé. Notamment en raison d'applications web trop fragiles face aux attaques subies. Il est temps de colmater les fissures...

LA BRÈCHE OÙ S'ENGOUFFRER

La faille est comme son nom l'indique un point de faiblesse du système informatique. Son exploitation à des fins malveillantes présente des risques sérieux : atteinte à la confidentialité, au contrôle de l'ordinateur, à la stabilité du système d'exploitation, etc. Les attaques se concentrent sur un point d'accès vers l'extérieur : les logiciels web.

1862 NOUVELLES FAILLES SUR LES SIX DERNIERS MOIS

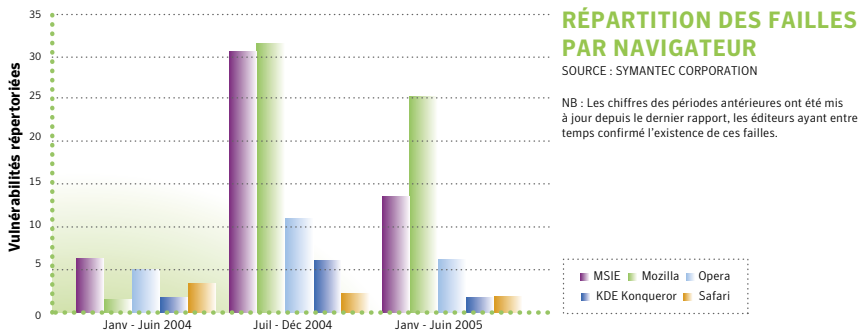
Un record depuis que Symantec mène ce baromètre. Ce phénomène inquiétant s'amplifie pour une moyenne de 18 nouvelles failles répertoriées chaque semaine.

59% DES FAILLES CONCERNENT LES APPLICATIONS WEB

Face à la sécurisation croissante des autres périmètres informatiques, les pirates se concentrent sur une catégorie moins résistante : les navigateurs et les serveurs web.

FIREFOX/MOZILLA, LE PLUS FAILLIBLE DES NAVIGATEURS

Placée devant Internet Explorer, l'application Firefox se révèle la plus perméable au danger, même si à ce jour aucune faille de Firefox n'a été utilisée.



DES ROBOTS À L'ATTAQUE

LES « BOTS »

Se greffant sur le disque dur à l'insu de l'utilisateur, le logiciel robot permet de prendre le contrôle de votre ordinateur à distance au moment voulu. L'ordinateur infecté sert alors de relais pour lancer des attaques vers de nouvelles cibles.

RETOUR EN FORCE : 10 352 ROBOTS ACTIFS/JOUR DANS LE MONDE

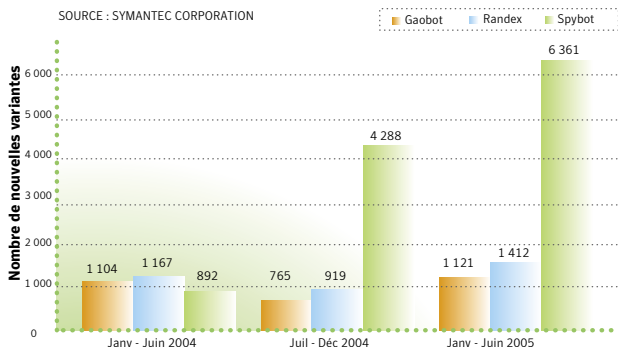
En diminution auparavant (sûrement en raison de la réduction des failles grâce aux patches fournis par les éditeurs), leur nombre croît de nouveau. Les pirates se sont tournés vers une autre voie pour placer ces "bots" sur les ordinateurs.

DES FICELLES AU CORDON DE LA BOURSE

Les pirates qui contrôlent ces "bots" le font pour de l'argent. Car un robot, ça rapporte. Les pirates les louent ou les revendent à d'autres qui s'en servent pour lancer des attaques ciblées (envoi de spams, phishing, etc.). Un réseau comprenant jusqu'à 150 000 bots est loué pour environ 300 \$ US. Un coût léger pour le pirate au regard de ce que cela rapporte. Un coup sérieux pour l'internaute en revanche.

NOMBRE DE NOUVELLES VARIANTES DE BOTS

SOURCE : SYMANTEC CORPORATION



On distingue 3 grandes familles de "bots" :

Gaobot, Randex et Spybot, dont le nombre de variantes a augmenté de plus de 700% en 1 an !



PRÉCAUTIONS DE BASE

- Installer le Service Pack 2 pour Windows® XP de Microsoft®.
- Télécharger régulièrement les correctifs ("patches") mis à disposition par les éditeurs de logiciels sur leur site web.
- Faire un test de vulnérabilité sur le site de Symantec pour connaître le degré d'exposition de son ordinateur : <http://security.symantec.com/fr>
- S'assurer que son pare-feu filtre également le trafic sortant (voie utilisée par les robots pour communiquer).

LES CODES MALICIEUX

Un nom générique pour plusieurs types de menaces.
Face à leur virulence, mieux vaut ne pas baisser sa garde.

Virus, vers, chevaux de Troie, etc. Les codes malicieux désignent ces programmes malveillants qui nuisent au bon fonctionnement de l'ordinateur. Dans le pire des cas, ils le rendent totalement inopérant ou détruisent les données.

PLUS MALINS, PLUS INTÉRESSÉS, TOUJOURS PLUS NOMBREUX

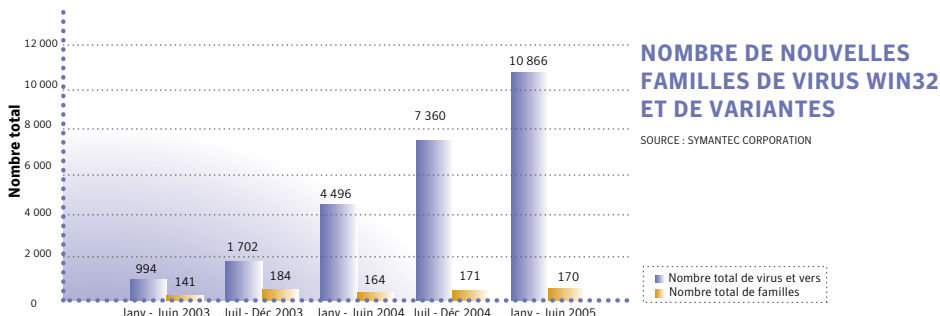
- **Intéressés** : 74 % des 50 premiers codes malicieux les plus répandus ont été des menaces mettant en danger les informations personnelles, notamment bancaires, contre 54 % au semestre précédent.
- **Futés** : seuls 2 virus dans le Top 10 empruntent la forme classique connue de tous, la pièce jointe à un courrier électronique. (Sober.O et Netsky.P)

Rang	Code
1	Netsky.P
2	Sober.I
3	Gaobot
4	Tooso.F
5	Tooso.B
6	Redlof.A
7	Lemir
8	Lineage
9	Sober.O
10	KillAV

TOP 10 DES CODES MALICIEUX
SOURCE : SYMANTEC CORPORATION

10 866
 nouveaux virus sont apparus
+142 % par rapport
 au premier semestre 2004

- On observe **une augmentation importante des variantes de virus**, Ex. : le très célèbre virus MyTob a connu **97 variantes en un mois** seulement.



LES RISQUES SUPPLÉMENTAIRES À LA SÉCURITÉ

••••• Spyware et adware, l'avancée furtive

Généralement invisible pour l'utilisateur, leur installation se fait en parallèle de celle de logiciels légitimes, gratuits ou de démonstration... Selon les cas et les usages, les logiciels espions ou publicitaires ne présentent pas tous les mêmes risques de sécurité. La difficulté de cette lutte tient notamment à l'absence de norme établissant la frontière entre logiciel à usage marketing ou frauduleux.

- **60 % des spywares** se greffent lors de l'installation d'un logiciel légitime.
- **Plus de la moitié des adwares** s'installe après affichage d'un accord de licence validé par l'utilisateur.
- **8 adwares sur 10 et 6 spywares sur 10** peuvent s'installer via un navigateur web.
- **Dans le Top 50 des codes malicieux**, 8 % d'entre eux sont des adwares.

MÉTHODES D'INSTALLATION DES LOGICIELS PUBLICITAIRES ET ESPIONS

Nom du programme	Affiche un accord de licence	S'installe avec un logiciel légitime	Utilise un navigateur web
180Search	Oui	Oui	Parfois
BetterInternet	Oui	Oui	Oui
CoolWebSearch	Non	Non	Oui
EliteBar	Non	Non	Oui
Gain	Oui	Oui	Parfois
Apropos	Non	Oui	Oui
CometCursor	Non	Oui	Oui
e2give	Non	Non	Oui
Goidr	Non	Oui	Non
lsearch	Non	Oui	Oui

SOURCE : SYMANTEC CORPORATION ■ ADWARE ■ SPYWARE



PRÉCAUTIONS DE BASE (Codes malicieux)

- Ne pas ouvrir une pièce jointe à un courrier si un doute sur son origine subsiste.
- Télécharger les correctifs des constructeurs/éditeurs pour réduire les failles.

PRÉCAUTIONS DE BASE (Spyware/Adware)

- Si vous téléchargez un logiciel, gare 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.



CONSEILS TECHNIQUES

- Lancer régulièrement Windows® Update ou activer son mode automatique.
- Utiliser une protection à plusieurs niveaux : anti-virus + pare-feu (firewall) personnel.
- Penser à mettre régulièrement à jour ses définitions de virus.

LA CONFIDENTIALITE MENACEE

SPAM ET PHISHING : UN TRAFIC QUI S'ACCROÎT

Le phishing désigne la récupération d'informations confidentielles (numéro de carte bleue, coordonnées bancaires...). Il s'effectue par le biais d'un courrier électronique publicitaire appelé spam.

Le spam correspond à l'envoi massif de courriers électroniques, généralement publicitaires et non sollicités. Pour obtenir des coordonnées électroniques, les "spammeurs" récupèrent tout ce qui peut ressembler à des adresses mail dans les pages web ou les forums d'Internet.

61 % du trafic
de courrier électronique
sur Internet est du spam



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, ce 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.
- Supprimer simplement le message.
- Installer un logiciel anti-spam.

LE PHISHING : LA FAUCHE EN RÈGLE

1 message sur 125 est une tentative de phishing.

Un utilisateur qui reçoit en moyenne 25 messages par jour reçoit forcément une tentative de phishing par semaine.

Cela représente 5,7 millions de messages par jour

dans le monde, soit une hausse de 96% par rapport au précédent semestre - avec des pointes allant jusqu'à 13 millions de messages par jour.

240 \$, c'est la perte moyenne des consommateurs dont le numéro de carte bancaire a été volé sur Internet. (2004 - source : FBI)

2 millions de dollars, c'est la somme qu'a réussi à récolter un groupe de "phishers" en envoyant de simples courriers électroniques à travers le monde en 2004. (source : FBI)

Les techniques évoluent

pour tromper les personnes et leurrer les dispositifs de filtrage : on trouve des messages qui affichent directement le numéro de compte et demandent à cliquer sur un lien pour confirmer que les informations sont correctes. Les "phishers" utilisent également des noms de domaine dits "cousins" pour induire la victime en erreur. Exemple : www.ma.banque.fr au lieu de www.mabanque.fr

1,04 milliard
de tentatives de phishing
bloquées par Symantec

+ 90 %
par rapport au précédent
semestre



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 vos informations si vous avez le moindre doute.



CONSEILS TECHNIQUES

- Si vous saisissez des informations sensibles (bancaires), assurez-vous que :
 - l'adresse dans la barre du navigateur commence par https,
 - un petit cadenas s'affiche dans la barre d'état - en bas de votre navigateur,
 - l'adresse correspond bien à celle annoncée (en vérifiant l'orthographe).
- Dans le doute, se connecter directement au site sans passer par le lien dans l'e-mail.

LES NOUVELLES CIBLES

Données numérisées, équipements électroniques, miniaturisation et nomadisme... Les avancées technologiques favorisent l'interconnexion et le partage entre individus. Cela n'a pas échappé aux pirates en quête de nouveaux territoires à investir.

LES MOBILES INFECTÉS

Les téléphones mobiles se dotent de véritables systèmes d'exploitation, devenant ainsi la proie des virus qui visent à se propager. Ce risque évoqué dans le précédent rapport Symantec se confirme aujourd'hui.

De plus, les virus ne se transmettent plus exclusivement via technologie Bluetooth. Ils s'affranchissent désormais du besoin de proximité entre le téléphone infecté et le nouvel hôte, aggravant ainsi les risques de propagation entre les terminaux...

..... MMS : C msg ki véikul D risk

Le premier virus se transmettant par MMS est apparu en mars dernier.

Le problème devient similaire aux courriers électroniques contenant un virus en pièce jointe. Par rapport à la propagation via Bluetooth, le mode de diffusion est donc accéléré et ne nécessite plus forcément que les téléphones soient dans un périmètre de 10 mètres. La force de frappe des virus dans l'univers mobile se rapproche donc de plus en plus des virus informatiques classiques.

Septembre 2005

Virus "mobile" : 54 menaces dans 14 familles de virus différentes ont été identifiées

Octobre 2005

Trojan.PSPBrick : 1^{ère} menace ciblant la console de jeux PSP de Sony



PRÉCAUTIONS DE BASE

- Ne pas laisser la fonction Bluetooth de son téléphone en mode détectable.
- Mieux vaut la désactiver si vous n'en avez pas l'usage.

VoIP ET MENACES PAR VOIE ORALE

La téléphonie via ordinateur (Voice Over Internet Protocol) compte peu d'attaques jusqu'à présent. Néanmoins, Symantec prévoit un risque croissant dans les mois à venir. Le succès de logiciels comme Skype ou des offres *Internet + téléphone* fait craindre l'intérêt des hackers : actuellement : 23 millions d'utilisateurs Skype, prévision fin 2006 : 160 millions, soit une croissance de près de 700 %.

(Source : Etude Evalueserve « The Impact of SKYPE on Telecom Industry »)

••••• Des exemples de risques potentiels pour la VoIP :

- Spams vocaux
- Phishing vocal
- Attaque par saturation des serveurs vocaux

LES FUTURES TENDANCES SELON SYMANTEC

Les codes malicieux deviennent “modulaires”. Après avoir contourné l'anti-virus et infecté l'ordinateur, ces programmes téléchargent des modules supplémentaires pour développer de nouvelles fonctionnalités. C'est déjà le cas du cheval de Troie : Tooso.l par exemple.

Augmentation du nombre de bots et des menaces liées, notamment les attaques par saturation. Symantec prévoit également la formation de réseaux de bots de plus en plus furtifs et élaborés qui aboutiront à des attaques de plus en plus sophistiquées.

Développement du phishing, qui devrait s'accompagner de nouvelles méthodes pour tromper les victimes, dont le renouvellement régulier des messages pour leurrer les filtres de détection automatiques.

L'environnement mac exposé : même si l'on ne répertorie aucune exploitation importante de failles sous Mac OS X, ses utilisateurs doivent cependant demeurer vigilants. L'augmentation des mordus de la Pomme laisse craindre des attaques beaucoup plus importantes que celles relevées jusqu'à présent.



Symantec Security Check

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



Vous pouvez télécharger la version PDF de ce guide sur
<http://www.symantec.com/region/fr/resources/gdpublic.html>

Symantec France
Immeuble River Seine
25, quai Gallieni
92150 Suresnes

