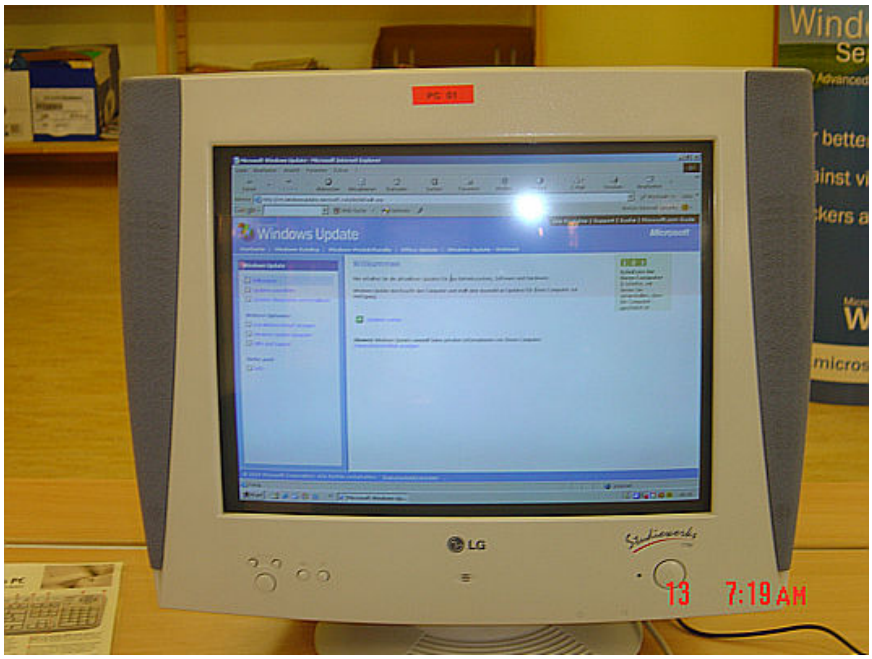


Pourquoi faut-il faire un „Update“?

Le mot « **update** » vient de l'anglais et veut dire « **mise à jour** », en abrévié « **MAJ** » ou « **maj** ».
Les « **updates** » (**mises à jour**) servent à renforcer la sécurité du système d'exploitation de votre PC.

On parle aussi de télécharger des « **patches** », des **rustines**. Comme le mot « **patches** » ou rustines le dit, ils servent à raccommoder des **vulnérabilités** (des **trous de sécurité**).

Ces vulnérabilités n'existent pas seulement chez **MICROSOFT**, mais aussi chez **LINUX** et **MACINTOSH**.

Voir aussi l'article suivant :

Compilation Sécurité PC & Internet

http://www.internetmonitor.lu/index.php?action=article&id_article=107178&id_rubrique=18315

Ces **vulnérabilités** (**trous de sécurité**) sont **exploitées par des programmeurs de code malicieux** pour **téléguider votre PC**, pour prendre le contrôle de votre machine à votre insu (sans que vous ne vous en apercevrez) ! Votre PC deviendra alors un « **PC-ZOMBIE** ».

Lire aussi l'article suivant :

Votre PC est-il un « ZOMBIE » à louer ?

http://www.internetmonitor.lu/index.php?action=article&id_article=67428

Maintenant, après avoir cliqué sur le lien ci-dessus et après avoir lu son contenu, vous comprendrez à quel point il est important de télécharger les mises à jour (**updates / maj**) !

Comment faire ces updates et quand ?

***MICROSOFT publie chaque 2ème mardi du mois ses updates*. Les autres fabricants, tels que LINUX et MACINTOSH publient de temps à autre des mises à jours sans date fixe.**

Pour faire ces mises à jour (**updates/MAJ**) il existe deux façons :

1. Les mises à jour (**updates**) automatiques (le Pc le fait automatiquement et les télécharge tous)
2. Les updates (**mises à jour/maj**) manuelles (à vous de le faire et de choisir lesquels)

Pour la mise à jour automatique je vous conseille de visiter un tutoriel à l'adresse suivante :

Pour WINDOWS XP :

http://www.cases.public.lu/pratique/solutions/patch_systeme/wxp2/index.html

Pour WINDOWS 2000 :

http://www.cases.public.lu/pratique/solutions/patch_systeme/w2000/index.html

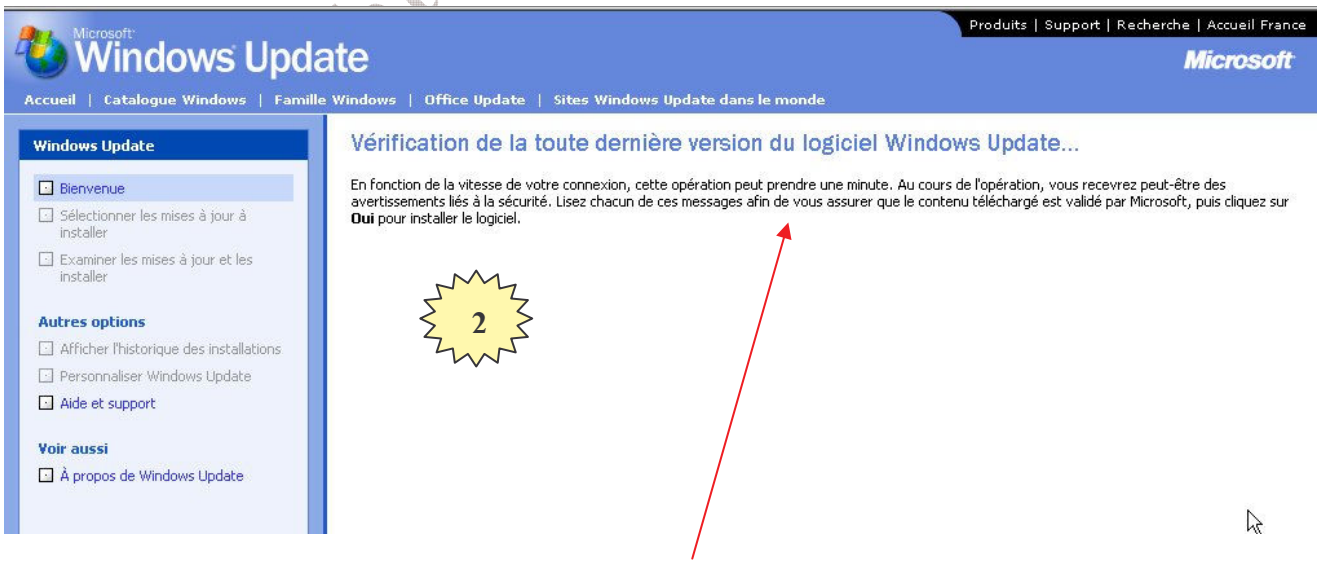
En ce qui concerne la mise à jour manuelle, veuillez suivre mon tutoriel pas à pas :

Veuillez saisir dans votre navigateur l'adresse de mon « **Internet Monitor** » :

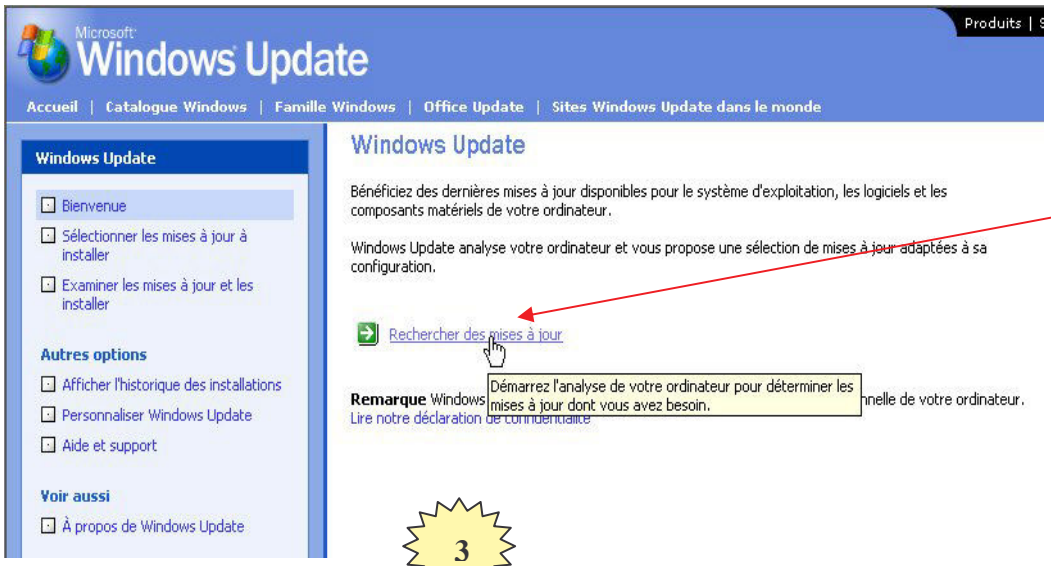
http://www.internetmonitor.lu

et puis naviguez vers le bas de la page Internet.

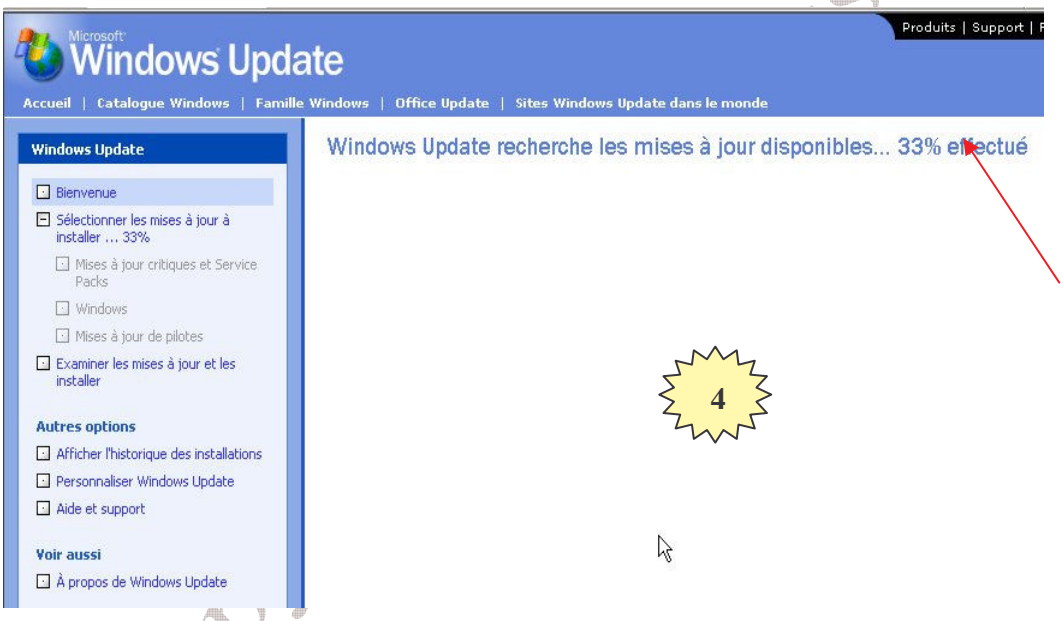
Ensuite cliquez sur
Pour ceux qui veulent faire le téléchargement en allemand, veuillez cliquer le lien juste au-dessus (DE).



WINDOWS va chercher maintenant automatiquement sur votre PC la dernière mise à jour et la comparaîtra avec la nouvelle version de téléchargement.

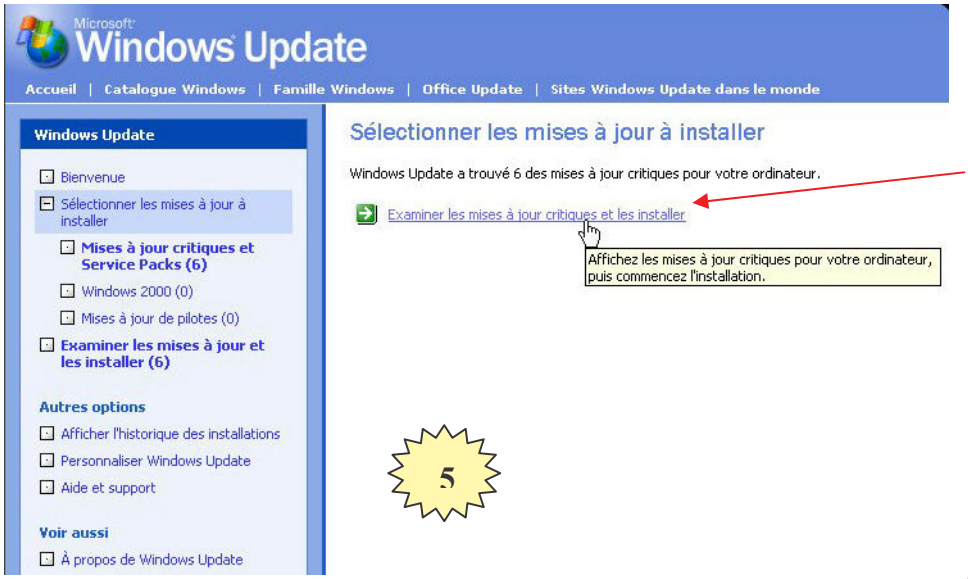


Pour faire cette recherche automatique, nous devons cliquer le lien suivant



L'écran suivant s'affichera et il faudra patienter un peu.

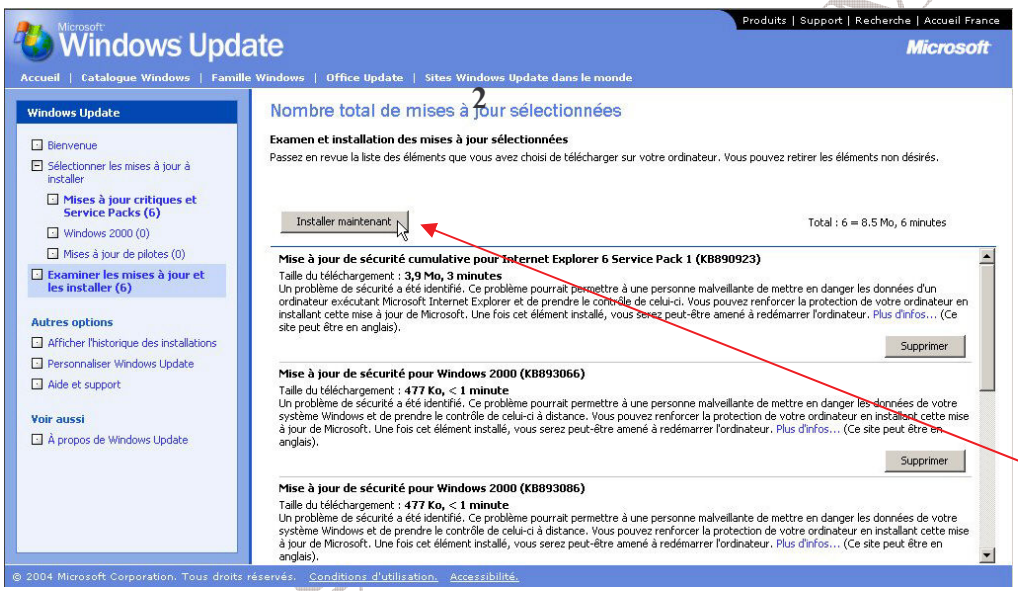
Votre PC affichera la fenêtre ci à gauche et par l'intermédiaire des « **% effectué** » vous êtes au courant de l'évolution de la recherche.
MICROSOFT scan votre PC sur les correctifs déjà installés et les compare avec sa liste actuelle.



Après ce temps d'attente, la fenêtre affiche le résultat suivant à gauche.

Il nous faut maintenant cliquer sur le lien suivant

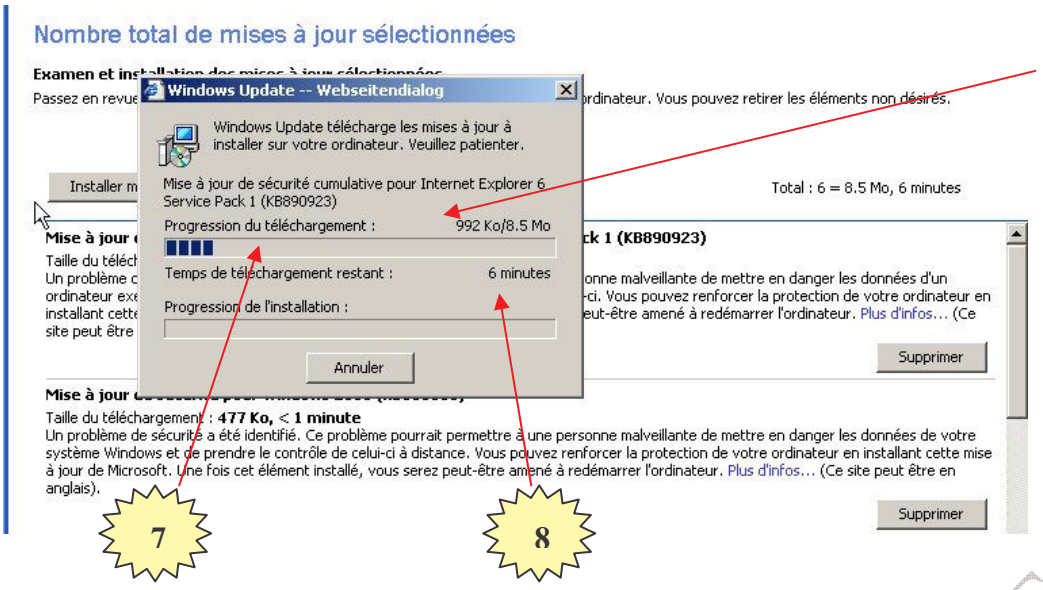
5



Maintenant vous voyez tous les fichiers à télécharger possibles. Dans notre exemple à gauche se sont les **mises à jour** du 14.04.2005.

Il nous faut cliquer maintenant sur le lien suivant

6



WINDOWS va maintenant télécharger automatiquement toutes les **mises à jour**.

Maintenant il faut être patient. Selon le nombre et le poids (en MB) des correctifs à télécharger, cela peut prendre quelques minutes. Dans notre exemple, ❽, environ 6 minutes !

Après ce téléchargement, **WINDOWS** vous avertira que les mises à jour ont été téléchargées avec succès et qu'il vous faut redémarrer le PC. Pour faire ceci vous cliquerez sur le bouton « OK » de la fenêtre du message.

Au point de vue « **Système d'exploitation** » **(O.S.)** votre PC est sécurisé au maximum possible actuellement (**jusqu'aux prochaines alertes**)!

Dès qu'il y a de nouveaux « **patches** » de disponible, ils seront annoncés par **MICROSOFT chaque 2ème mardi du mois**. À ce moment là, vous suivez la même procédure que décrite dans ce tutoriel !

Récapitulatif :

Les « MAJ/maj/patches/updates/rustines » sont obligatoires pour une bonne sécurité de votre PC, indépendant du système d'exploitation (MAC OS, LINUX, WINDOWS) !

Chaque 2ème mardi du mois, vérifiez s'il y a des « MAJ » à télécharger et le cas échéant, téléchargez les !

P.S. N'oubliez pas qu'en dehors de ces **téléchargements** il faut vérifier aussi que votre **anti-virus** et votre **firewall (pare-feu)** sont mis à jour (**MAJ**) régulièrement !

Glossaire :

Patch/rustine/MAJ/maj	: Fichier correctionnel
Vulnérabilité	: Partie non sécurisée
O.S.	: Système d'exploitation (WINDOWS, MAC, LINUX)
Malware	: Expression regroupant les virus, vers, troyens, dialer, etc.
Firewall (pare-feu)	: le portier de votre PC (contrôle le trafic entrant et sortant des données informatiques)
Téléchargement	: Download en anglais. Copier et transférer un fichier et/ou logiciel d'Internet sur votre PC
PC ZOMBIE	: PC téléguidé et non sécurisé
Botnet	: Réseau(x) de PC-ZOMBIES

F.A.Q. :

1. ***Pourquoi est-ce que WINDOWS ® est plus attaqué que les autres systèmes d'exploitation ?***

WINDOWS ® est le système d'exploitation le plus utilisé mondialement.

WINDOWS : 90-91 %
AUTRES : 4,9 %
MAC OS : 2,5 %
LINUX : 1,3 %

Chiffres au 18.04.2005.

2. ***Pour quelle raison sont les PC et les MAC attaqués ?***

Pour des raisons lucratives, bien entendu (**£, $, €**), mais il est plus **lucratif** pour la **MAFIA INFORMATIQUE** d'attaquer les systèmes **WINDOWS** que les autres. La « SAGA » que les autres systèmes d'exploitation (**LINUX** et **MAC OS**) ne **sont vulnérables** ne tient plus ! Aussi ces systèmes sont vulnérables, spécialement en ce qui concerne la **possibilité pour téléguider un ordinateur** (Remote access) ! **LINUX** et **MAC OS** sont moins vulnérables du point de vue de leurs structures internes, mais **vulnérables quand même** !

Les programmeurs de **malware** (**virus, vers, dialer, etc**.) le font dans un but lucratif (pour gagner de l'argent) !

C'est une nouvelle sorte de criminalité, la « **cybercriminalité** » ! Déjà que, dans notre monde, le monde réel, la criminalité est **difficile à combattre**, elle l'est encore beaucoup plus dans le monde virtuel, ce qui est Internet !

Sachez aussi que la réalisation de « **botnets** » avec des « **PC-ZOMBIES** » n'est principalement réalisable (possible) qu'avec des PCs non mis à jour (**sans updates**), donc avec des **vulnérabilités O.S.** !
Dû à une vulnérabilité de l'O.S. (**O**perating **S**ystem / **Système d'exploitation**) un PC peut être pris en main et téléguidé par quelqu'un d'autre, par l'intermédiaire d'une connexion Internet !

Les estimations sur les « botnets » :

Les experts de sécurité informatique observent actuellement (25.04.2005.) **35 réseaux actifs ! Ces réseaux se composent de 100 à 50.000 « PC-ZOMBIES » interconnectés selon besoin.**
Selon le « **HONEYNET PROJECT** », il pourrait y avoir même **plus qu'un million (>1.000.000.) de ces « PC-ZOMBIES » !**
Source de cet extrait : **Traduction de PC TIPP / MAI 2005 / page 18**

Le but de ces « botnets » :

Ces réseaux (**botnets**) sont employés pour faire des actions criminelles, par exemple :
Faire des **attaques du type DDOS**, c'est-à-dire, bombarder un serveur avec un maximum de données afin qu'il ne puisse réagir (plus digérer la masse d'informations envoyées) et à ce moment il n'est plus présent sur Internet. Cette méthode est employée pour nuire à un concurrent où pour faire du chantage.

Une deuxième méthode consiste à employer ces botnets pour envoyer du **SPAM** (courrier non sollicité) en masse sans révéler son origine, etc.

Comment combattre ces « botnets » et »PC-ZOMBIES » ?

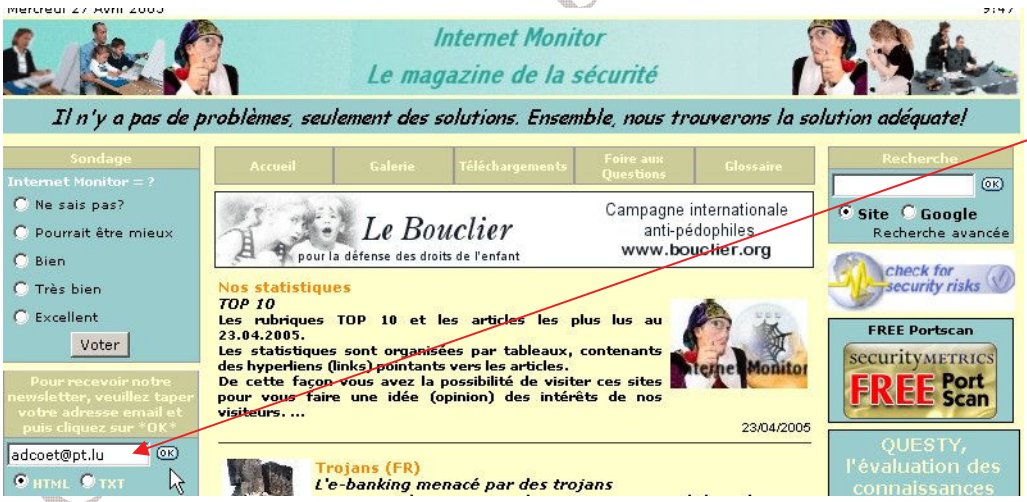
Rien de plus facile que ça. Les combattre et/ou carrément éviter pour qu'il n'y en ait pas est seulement dépendant de nous. Il suffit que tout le monde fasse les « **updates** » (**mises à jour**) et installe un « **anti-virus** », ainsi qu'un « **Firewall** » (**pare-feu**) !

À vous-même de réagir !

Si tout le monde aurait installé ces updates, ainsi qu'un « Firewall » et aussi un « Anti-virus », il n'existerait pas de « PC-ZOMBIES », ni de « Botnets » !

Pour être informé sur les nouveaux updates et les actualités de la « Sécurité PC & Internet », je vous conseille de vous inscrire à notre « Newsletter ».

Visitez notre site http://www.internetmonitor.lu et inscrivez-vous.



Tapez votre adresse e-mail dans le champ suivant et puis cliquez sur le « bouton » OK.

Vous recevrez nos prochaines nouvelles par courrier électronique.