

34. Pourquoi faut-il faire un “update”?

Le mot “update” vient de l’anglais et veut dire “mise à jour”, en abrégé “maj”. Les (mises à jour) “updates” servent à renforcer la sécurité du système d’exploitation de votre ordinateur. 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 la fiche N° 30: Compilation Sécurité PC & Internet.

Ces vulnérabilités (trous de sécurité) sont exploitées par des programmeurs de code malicieux pour téléguider votre ordinateur, pour prendre le contrôle de votre machine à votre insu (sans que vous ne vous en apercevez)! Votre ordinateur deviendra alors un “PC-zombie”. Lire aussi l’article http://www.internetmonitor.lu/index.php?action=article&id_article=67428. Après avoir lu l’article mentionné ci-dessus, vous comprendrez à quel point il est important de télécharger les mises à jour (updates/maj)!

Comment et quand faire ces updates?

Microsoft® publie chaque 2^{ème} 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 (l’ordinateur 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 nous vous conseillons de visiter les didacticiels suivants:

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 ce didacticiel pas à pas:

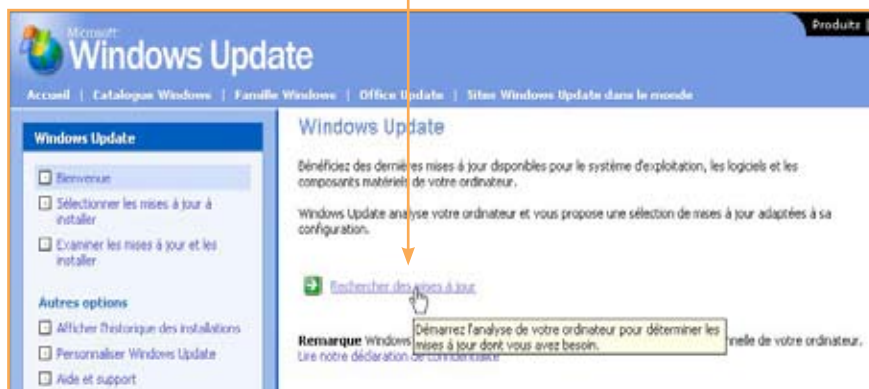
Veuillez saisir dans votre navigateur l’adresse de l’Internet Monitor: <http://www.internetmonitor.lu> et puis naviguez vers le bas de la page internet.

Ensuite cliquez sur “WINDOWS UPDATE (FR)”.

Pour ceux qui veulent faire le téléchargement en allemand, veuillez cliquer le lien juste au-dessus “WINDOWS UPDATE (DE)”.

Windows® va chercher maintenant automatiquement sur votre ordinateur la dernière mise à jour et la comparera avec la nouvelle version de téléchargement.

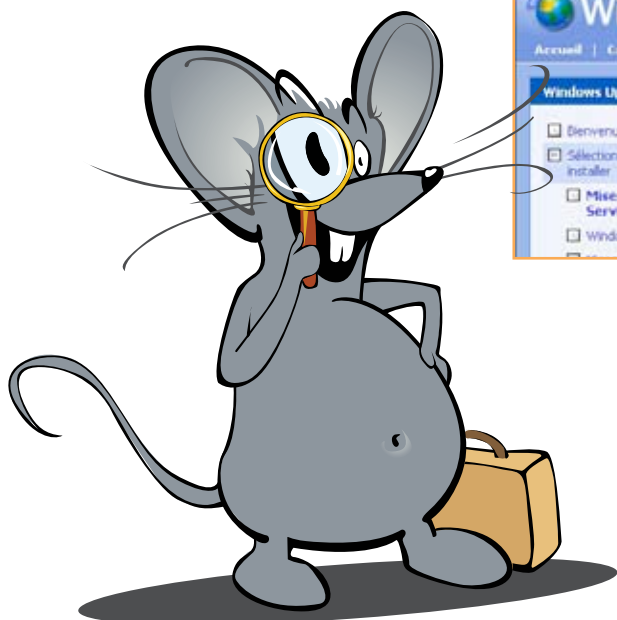
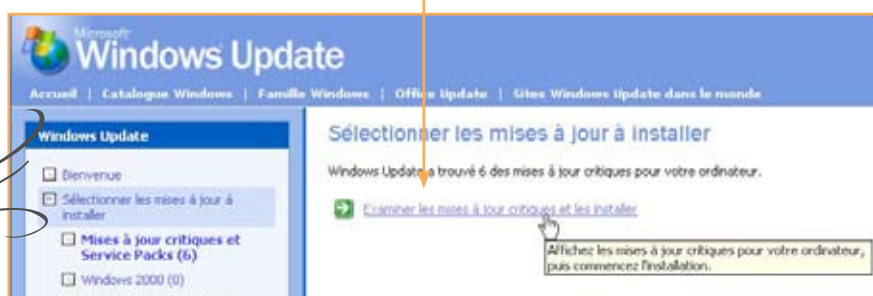
Pour faire cette recherche automatique, nous devons cliquer le lien suivant:



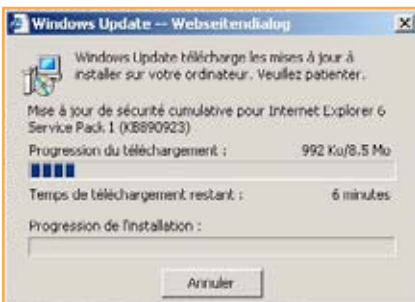
Votre ordinateur affichera la fenêtre ci-dessous et par l'intermédiaire des “% effectué” vous êtes au courant de l'évolution de la recherche. Microsoft® scanne votre ordinateur sur les correctifs déjà installés et les compare avec sa liste actuelle.



Après ce temps d'attente, la fenêtre affiche le résultat ci-dessous. Il nous faut maintenant cliquer sur le lien suivant, marqué d'une flèche sur fond vert.



Maintenant vous voyez tous les fichiers à télécharger possibles. Dans notre exemple à gauche ce sont les mises à jour du 14.04.2005. Il nous faut cliquer maintenant sur le lien suivant:



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, environ 6 minutes (avec une connexion DSL)!

Après ce téléchargement, Windows® vous avertira que les mises à jour ont été téléchargées avec succès et qu'il vous faut redémarrer l'ordinateur. Pour faire ceci vous cliquerez sur le bouton "OK" dans la fenêtre du message.

Au point de vue "Système d'exploitation" (O.S.) votre ordinateur 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 2^{ème} mardi du mois. À ce moment-là, vous suivez la même procédure que décrite dans ce didacticiel!



RÉCAPITULATIF:

Les “MAJ/maj/patches/updates/rustines” sont obligatoires pour une bonne sécurité de votre ordinateur et surtout la sécurité des autres, indépendamment du système d’exploitation (MacOS®, Linux®, Windows®)! Chaque 2ème mardi du mois, vérifiez s’il y a des “maj” de chez Microsoft® 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 antivirus et votre firewall (pare-feu) soient mis à jour 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 ordinateur (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 ordinateur
PC-zombie: ordinateur téléguidé et non sécurisé
Botnet: Réseau(x) de PC-zombies

F.A.Q. :

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 %
MacOS:	2,5 %
Linux:	1,3 %

Chiffres au 18.04.2005.

Pour quelle raison les PC et les Mac sont-ils 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 rumeur que les autres systèmes d'exploitation (Linux® et MacOS®) ne soient point vulnérables ne tient plus! Ces systèmes aussi sont vulnérables, spécialement en ce qui concerne la possibilité pour téléguider un ordinateur (Remote access)! Linux® et MacOS® 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 de l'internet! Cette "cybercriminalité" se moque des frontières, sur Internet les frontières sont inexistantes!

Sachez aussi que la réalisation de "botnets" avec des "PC-zombies" n'est principalement réalisable (possible) qu'avec des ordinateurs non mis à jour (sans updates), donc avec des vulnérabilités O.S.! Dû à une vulnérabilité de l'O.S. (Operating System/Système d'exploitation) un ordinateur peut être pris en main et téléguidé par une tierce personne, 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 l'extrait *Les estimations sur les "botnets"*. Traduction de PC TIPP (CH) / 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, appelé aussi pourriel (courrier non sollicité) en masse sans révéler son origine, etc.

Comment combattre ces "botnets" et "PC-zombies"?

Rien de plus facile! Les combattre et/ou carrément éviter qu'il y en ait dépend seulement de nous. Il suffit que tout le monde fasse les "updates" (mises à jour) et installe un "antivirus", ainsi qu'un "firewall" (pare-feu)!



À vous d'agir!

Si tout le monde avait installé ces updates, ainsi qu'un "firewall" et aussi un "antivirus", 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", nous vous conseillons de vous inscrire à la newsletter de www.internetmonitor.lu.

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.

Ou bien, pour ceux qui utilisent la technologie *RSS*, veuillez vous servir du lien suivant: <http://www.internetmonitor.lu/syndication.rss> ou pour les utilisateurs du "Atom reader", le lien suivant: <http://www.internetmonitor.lu/atom.xml>

C'est quoi la technologie *RSS*?

Pour ceux qui ne connaissent pas les *RSS*, veuillez consulter la fiche N°06. Fils *RSS* et blogs.



www.cte.lu

www.myschool.lu

www.mysecureit.lu

www.etwinning.lu



MINISTÈRE DE L'ÉDUCATION NATIONALE
ET DE LA FORMATION PROFESSIONNELLE
Centre de technologie de l'éducation



Copyright © 2005, www.myschool.lu

Tous droits réservés. Ce document est la propriété de *mySchool!* (CTE) et peut être reproduit pourvu qu'aucune modification ne soit effectuée et que cette notice soit préservée. Les informations véhiculées par la présente fiche le sont dans l'espoir qu'elles seront utiles. La responsabilité des auteurs ne pourra être engagée à aucun moment.