SECTION INTERNET DU CLUB MEDERIC DE MARSEILLE

Internet Gazette

23 janvier 2006
Numéro 12

Sommaire

Google dote Gmail d'un antivirus

Google poursuit le développement de sa messagerie en ligne Gmail en l'enrichissant d'une solution antivirale. Jusqu'à présent, la technologie Gmail permettait d'interdire la réception de fichiers exécutables. Les utilisateurs du service de webmail peuvent donc désormais ouvrir et envoyer leurs courriels et pièces jointes en toute quiétude, a priori.

Si Gmail trouve un fichier porteur d'un virus (ou de tout autre agent malveillant), il tentera de l'éradiquer. S'il n'y parvient pas, il rendra purement et simplement impossible l'accès à la pièce jointe. Un fonctionnement valable dans les deux sens, tant pour la réception que l'envoi des courriers électroniques. Malgré ces avancées sécuritaires, la vigilance reste cependant la meilleure protection contre ces menaces.

Sur les traces de Yahoo Mail et Hotmail

En agrémentant Gmail d'une solution antivirale, Google rejoint donc les ténors de la messagerie en ligne que sont Yahoo Mail et MSN Hotmail. Ces deux acteurs exploitent respectivement les solutions de Symantec et Trend Micro. De son côté, Google n'a, pour le moment, pas précisé l'origine de sa technologie antivirale.

La diffusion frauduleuse d'adware (espions) en forte croissance

Une nouvelle forme de cybercriminalité a sévi en 2005: la diffusion frauduleuse d'adware, des programmes parasites qui affichent des pop-up publicitaires non sollicités. C'est l'une des principales observations du Club de la sécurité des systèmes d'information français (Clusif), qui a présenté le 12 janvier son "Panorama de la cybercriminalité 2005".

Pour propager ces programmes, certains internautes peu scrupuleux n'hésitent plus à utiliser massivement des "logiciels robots". C 'est en cela que leur diffusion prend un caractère frauduleux, car l'installation d'un adware doit normalement s'effectuer avec le consentement préalable de l'utilisateur.

Le robot est un programme malveillant qui s'installe discrètement sur des machines pour en prendre le contrôle à distance. Grâce à des robots, un attaquant peu se constituer rapidement une armée de milliers d'ordinateurs "zombies", qui

seront autant de cibles que de relais.

Le système qui héberge le robot peut également être utilisé pour diffuser à son tour l'adware vers d'autres ordinateurs présents sur le voisinage réseau, en exploitant une faille du système d'exploitation.»

744 dollars par jour avec 5.000 machines

L'appât du gain est la première motivation de ces actes malveillants, encouragés par la passivité des éditeurs d'adwares, activité tout à fait légal. Pas trop regardants sur les méthodes de distribution de leurs produits, ils ont recours à des «affiliés», un statut ouvert à n'importe quel internaute. Chaque affilié reçoit un identifiant qui lui servira à marquer chaque adware qu'il diffuse; l'éditeur le rétribue en conséquence.

Ces entreprises ne sont pas complices. Dans la plupart des affaires observées, ce sont d'ailleurs elles qui ont porté plainte contre des affiliés peu scrupuleux. Elles cherchent aujourd'hui à redorer leur blason.

En août 2005, la société américaine 180solutions a ainsi porté plainte contre des affiliés en Grande-Bretagne, en Australie, au Canada, au Liban, en Slovénie et en Hollande. Pour augmenter leurs gains (entre 7 et 50 cents par installation), ils auraient utilisé plusieurs réseaux de milliers robots. Un réseau de 5.000 machines permet de dégager un revenu de 744 dollars par jour, ou 22.346 dollars par mois.

Autre exemple: en octobre 2005, la police hollandaise a arrêté trois jeunes gens qui avaient pris sous leur contrôle plus de 1,5 million de machines et de serveurs grâce à des robots. Ils sont notamment accusés de diffusion d'adwares.

D'octobre 2004 à octobre 2005, il y a eu une augmentation de 400% du nombre de robots, De 5 à 10 millions de ces robots peuvent être simultanément en activité sur le web.

Un robot arrive la plupart du temps de la même manière qu'un virus, via un e-mail piégé ou en exploitant une faille de sécurité du système d'exploitation. Toutefois un système correctement "patché" et protégé par un antivirus mis à jour ainsi qu'un pare-feu est «immunisé à 95%.

Quoi de neuf dans Thunderbird 1.5 ?

Appréciée pour son filtre anti-spam ou encore son lecteur de fils RSS (Really Simple Syndication, qui s'ajoutent aux fonctionnalités classiques de messagerie), la nouvelle version de l'application ne se distingue guère, en apparence, de la précédente.

Le client ne s'en enrichit pas moins de quelques nouveautés bien pensées. A commencer par un nouveau détecteur de courriers frauduleux de type phishing qui signale automatiquement à l'utilisateurs les messages à l'origine douteuse.

Le traitement des flux RSS s'enrichit d'un accès au Podcast via une boîte de dialogue qui permettra de choisir l'application la mieux adaptée pour la lecture des fichiers multimédia (navigateur, lecteur indépendant...).

Soulignons encore la fonction de mise à jour automatique amélioré qui enlève à l'utilisateur le besoin de vérification manuelles des nouvelles versions.

Vérification orthographique à la volée

Bref, au lieu de parler de révolution en profondeur, il vaudrait mieux évoquer des évolutions d'ergonomie visant à augmenter la productivité et à faciliter l'usage de cette application alternative à Outlook Express de Microsoft.

Notons ainsi l'apparition de la vérification orthographique à la volée, la sauvegarde automatique des messages en cours de frappe (très utile en cas de plantage ou coupure électrique) et la très attendue possibilité de supprimer les pièces jointes des messages.

***Sécurité** - À défaut d'intégrer un calendrier, la nouvelle version de l'outil de messagerie de la Mozilla Foundation est enrichie d'une fonction anti-phishing, pour déjouer les tentatives d'escroqueries par e-mail.*

Rappelons que le principe du phishing consiste à duper l'internaute en l'amenant à communiquer lui-même des données personnelles, comme son numéro de carte de crédit, via un site internet factice, copie conforme du site d'une banque par exemple. Le plus souvent, une attaque par phishing utilise l'e-mail: l'internaute reçoit un faux message qui l'invite à cliquer sur un lien renvoyant vers le site factice.

La solution de Thunderbird 1.5 est de comparer un lien présent dans un message avec le véritable nom de domaine auquel il renvoie. Si, par exemple, l'intitulé du lien est "societegenerale.fr" mais que le nom de domaine est

"pirate123321.com", l'application estimera qu'il n'y a aucune corrélation et affichera le message suivant: «Thunderbird pense que ce message est peut-être frauduleux». L'utilisateur est ainsi mis en garde.

Nouveau système de mises à jour

Le code de Thunderbird étant à environ 80% identique à celui de Firefox, l'outil de messagerie bénéficie des avancées de Firefox 1.5 lancé en novembre dernier. La principale est l'intégration de mises à jour automatiques. Jusqu'à présent, lorsqu'une nouvelle version de Thunderbird était disponible, l'utilisateur était alerté par une icône sur laquelle il fallait cliquer afin de lancer le téléchargement d'une nouvelle version complète.

Avec Thunderbird 1.5, seuls les nouveaux composants sont ajoutés. Ils sont automatiquement téléchargés en tâche de fond dès leur disponibilité. L'utilisateur est ensuite alerté par une boîte de dialogue pour les installer.

Parmi les autres nouveautés: l'accession à des contenus de type Podcasts, la vérification de l'orthographe lors de la saisie des messages, la possibilité d'archiver des e-mails sans leur pièce jointe.
Enfin, petite fonction intéressante: lors de l'entrée d'une adresse mail, Thunderbird 1.5 propose une liste de contacts en saisie automatique, qui n'est plus pas classée par ordre alphabétique, mais selon les contacts les plus courants.

Retrouver l'icône du Bureau dans la barre de lancement rapide

Si vous avez supprimé par accident le raccourci vers le Bureau qui se trouve dans la barre de lancement rapide, voici comment le retrouver. Exécutez le bloc-notes puis recopiez-y les lignes suivantes :

[Shell]
Command=2
IconFile=explorer.exe,3
[Taskbar]
Command=ToggleDesktop

*Déroulez ensuite le menu **Fichier**, **Enregistrer sous**.*

*Dans la liste **Type**, sélectionnez l'option **Tous les fichiers**.*

*Saisissez ensuite **ShowDesktop.SCF** dans le champ **Nom du fichier***

*puis enregistrez le fichier dans le dossier **C:\ Documents and Settings\ [votre nom d'utilisateur]\ Application Data\ Microsoft\ Internet Explorer\ Quick Launch**.*

L'antimalware caché de Windows

Si vous avez Windows XP avec le SP2 installé, peut-être n'avez-vous pas remarqué la présence du programme de suppression de logiciels malveillants de Microsoft sur votre disque dur. Pourtant, ce logiciel est un excellent outil d'appoint en plus des utilitaires de protection traditionnels ! Penchons nous donc d'un peu plus près sur ce programme "caché"...

L'outil de suppression de logiciels malveillants Microsoft s'applique sur Windows 2000, Windows XP et Windows 2003. Si vous utilisez XP avec le SP2 installé, le programme est alors déjà présent sur votre système. Dans le cas contraire, vous pouvez télécharger le programme sur cette page.

*L'outil dont nous allons parler ici est MRT.exe que vous trouverez dans le répertoire system32 de Windows. Pour le lancer, il suffit donc de créer un raccourci de ce fichier sur votre bureau ou plus simplement d'aller dans **Démarrer**, **Exécuter…** et de taper la commande suivante :*

mrt

Le programme se lance directement (rien ne s'installe sur le disque)

*Cliquez sur **Suivant**.*
A noter que cette première fenêtre vous donne la possibilité de consulter la liste des logiciels malveillants que le programme peut détecter et supprimer en cliquant sur le lien correspondant.

CD et DVD gravés : durée de vie limitée, de 2 à 5 ans

A la différence des CD originaux pressés, les CD gravés ont une durée de vie limitée de 2 à 5 ans qui dépend de la qualité du CD

Kurt Gerecke, physicien et expert en stockage chez IBM, brosse un portrait alarmiste du stockage sur disque.

Entraînée par le frottement ou la chaleur, la dégradation physique de la couche teintée des disques optiques – en particulier les CD-R et CD-RW – serait à l'origine d'un processus de dégradation qui modifierait les données et rendrait leur lecture par le laser aléatoire.

Quel serait alors la durée de vie d'un support CD ou DVD gravé ? Selon Kurt Gerecke, 2 ans si le support a été acquis sous une marque ou un produit discount, 5 ans si la marque ou le produit sont de qualité.

Comment dans ces conditions augmenter la durée de vie des supports ? En les stockant dans un lieu frais et noir. Mais selon Kurt Gerecke, le gain de temps ne sera pas important !

Les disques durs sont soumis aux mêmes contraintes. Ne sont-ils pas conçus à l'aide de disques ré-enregistrables ? De nouveau, la durée de vie d'un disque dur dépendra de la qualité des disques qui le composent.

Vient s'ajouter sur les disque durs une contrainte mécanique, plus un disque tourne rapidement et plus sa dégradation sera rapide. Le conseil de Kurt Gerecke : utiliser des disques dont la rotation ne dépasse pas les 7200 révolutions à la minute.

Y a-t-il alors une solution pour conserver des données sur un support présentant une durée de vie raisonnable ?

Kurt Gerecke conseille d'utiliser des bandes magnétiques, dont la durée de vie serait de 30 à 100 ans, toujours selon la qualité du support. "Même si les bandes magnétiques restent sujettes à dégradation, elles sont encore le média de stockage supérieur."

La solution ? Elle serait pour les entreprises dans le maintient d'un plan de migration permanente vers les nouvelles technologies de stockage, "avec une stratégie d'archivage qui leur permet de migrer automatiquement vers les nouvelles technologies."

"Pour ceux qui sont assis sur des tera octets de données vitales, ce pourrait être un problème colossal."

Certes, le discours de Kurt Gerecke, expert d'IBM, a de quoi inquiéter. Les CD et DVD n'auraient donc pas une durée de vie proche d'un siècle (100 ans), comme l'affirment les vendeurs ? Encore semble-t-il ignorer l'existance des champignons qui se glissent dans les couches d'un média et grignotent les données, comme nous l'évoquions il y a trois ans déjà !

En revanche, par certains aspects, sa conclusion prend des allures bien marketing, susceptible sans doute de satisfaire le deuxième vendeur de solutions de stockage qu'est IBM en part de marché (lire nos articles).

Ou alors, pourquoi ne pas relancer un programme pharaonique de gravure de l'information dans la pierre ? Un projet qui aurait au moins le mérite de créer des millions d'emplois. Jusqu'à ce que les géants du stockages - dont IBM - ne développent des systèmes de gestion du cycle de vie de la gravure automatique de la pierre…

Comment changer rapidement les paramètres d'impression de votre imprimante

En installant deux fois son pilote.

En fonction du document à imprimer, vous devez changer certains paramètres d'impression tels que l'orientation, le format du papier, la qualité d'impression ou le contraste des couleurs. Vous pouvez également définir des paramètres par défaut qui seront appliqués à chaque type de document, par exemple les textes et les images. Il vous suffit alors d'installer une seconde fois le pilote de l'imprimante sous un autre nom. Vous modifierez ensuite les paramètres appliqués par défaut. Ensuite, dans une application, il vous suffira de changer le nom de l'imprimante utilisée dans la boîte de dialogue d'impression.