SECTION INTERNET DU CLUB MEDERIC DE MARSEILLE

Internet Gazette

19 décembre 2005
Numéro 9

L'actualité Internet de la semaine

Nouveaux virus ou espions

Environ 72 % des PC connectés au Net étaient infectés par au moins un logiciel espion dans le courant du troisième trimestre 2005, selon le rapport trimestriel intitulé State of Spyware de la société de sécurité Webroot. Bien qu'élevé, ce taux d'infection est cependant en baisse il était respectivement de 83 et 88 % aux deux précédents trimestres 2005, avec un pic à 92 % d'infection au quatrième trimestre 2004 (pour une moyenne autour de 90 % dans l'année 2004).

Paradoxalement, le nombre de sites Web qui hébergent des spywares a progressé de plus de 26 % depuis le début de l'année. Parmi ceux-ci, 31 % sont américains, 17 % russes, 12 % chinois et 1,43 % français. En moyenne mondiale, chaque ordinateur infecté héberge 17 spywares (dont 14 % sont de forme "pernicieuse" comme les logiciels publicitaires, les chevaux de Troie et les agents de contrôle du trafic). Les Etats-Unis détiennent le triste record de plus de 24 logiciels espions détectés par PC, contre moins de 10 en France.

Evolution du phénomène

Webroot réalise son rapport sur la base d'un audit des ordinateurs effectué à partir de ses outils en ligne (SpyAudit). Il n'est donc pas forcément représentatif de la réalité mais reflète une évolution du phénomène qui a amené 86 % des utilisateurs à changer leur comportement en ligne, selon la société d'étude WebWatch (voir édition du 28 octobre 2005).

De son rapport, Webroot a extirpé les dix logiciels intrusifs (adwares et spywares) les plus virulents. AbetterInternet arrive en tête : il intervient sur les recherches Web, les pages d'accueil ou d'autres paramètres d'Internet Explorer. "Il est très souvent intégré à des logiciels gratuits de toutes origines", souligne le rapport. Ce BHO (Browser Helped Object) détrône CWS (CoolWebSearch) dont les variantes sont capables d'installer "des applications HTML pirates ou des failles sécuritaires s'attaquant au format Help HTML et aux machines Virtual Java Microsoft".

Des espions dissimulés dans des logiciels gratuits

Dans le même genre, EliteBar peut s'activer via une recherche Web, les pages d'accueil ou d'autres paramètres Internet Explorer et se propage au travers de boîtes de dialogue apparemment anodines ou des processus comportementaux. Il est également présent dans de nombreux logiciels gratuits. En affichant pop-up à caractère pornographique, ISTbar peut se révéler très embarrassant. D'autant qu'il affecte les pages d'accueil des utilisateurs et les recherches Internet.

Nombre de spywares se contenteront de pister la navigation Internet (Look2Me), d'afficher des fenêtres publicitaires (SurfSideKick, Virtumonde), de rediriger l'internaute vers des sites marchands (StopAtHomeSelect). D'autres vont plus loin en installant des barres d'outils (Web Search Toolbar) et autres programmes indésirables. C'est notamment l'une des options de 180Search Assistant (180SA) dont l'éditeur 180Solutions poursuit en justice le spécialiste de la sécurité ZoneLabs, auquel il reproche d'inviter ses utilisateurs à désinstaller son logiciel de leur machine (voir édition du 12 décembre 2005).

Gmail s'améliore encore un peu et scanne maintenant les mails

De plus en plus utilisé par les internautes, Gmail, à l'image de la totalité de Google et de ses services, continue de grandir à son rythme et, comme le bon vin, s'améliore en prenant de l'âge. Ainsi, le service mail de Google ne

se contente plus de proposer un espace de stockage colossal à ses utilisateurs, mais fait également dorénavant dans la sécurité, en incluant désormais un système d'antivirus capable de détecter les pièces jointes infectées.

Ce genre de service n'est pas réellement nouveau dans le monde des services mail sur Internet puisque Hotmail, le service de Microsoft, propose lui aussi cette option de quelques temps. D'ailleurs, certains se souviennent certainement de l'hilarante option proposant de télécharger quand même la pièce jointe détectée comme infectée.

Ici, à la manière de l'actuel système de sécurité de Hotmail, nous n'avons pas le choix de ce que nous comptons faire d'une pièce jointe infectée. Si un virus est détecté dans un mail reçu, la pièce jointe qui l'accompagne va automatiquement être bloquée, empêchant l'utilisateur de l'ouvrir.

Gmail va ensuite tenter de nettoyer la pièce jointe du virus qu'elle contient afin de pouvoir donner de nouveau accès à cette dernière. Si le nettoyage du fichier échoue, celui-ci sera alors purement et simplement supprimé.

Mais ce n'est pas tout puisque le service se charge également de contrôler les fichiers sortants afin de s'assurer que rien de douteux ne puisse être envoyé à vos contacts.
De cette manière, si un fichier que vous tentez d'envoyer s'avère être infecté, il vous sera alors impossible d'envoyer votre message en l'état, et ce tant que vous n'aurez pas retiré la pièce jointe infectée du message. Une sécurité supplémentaire donc pour le service mail de Google, qui gagne encore un peu de terrain sur la concurrence...

Comment retirer le bon Dr Watson ?

Prendre un point de contrôle pour pouvoir restaurer en cas de problème

Allez dans la base de registre :

- *Démarrer --> Exécuter puis tapez **regedit**.*
- *Recherchez la clé HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug*
- *Supprimez la clé AeDebug.*
- *Fermez la base de registre.*

Redémarrer l'ordinateur

Outlook Express 5 et 6 : protéger la configuration de ses comptes de messagerie

*Pour empêcher la modification des paramètres des comptes de messagerie, vous devez intervenir dans le **Registre** de Windows. Commencez par fermer Outlook Express. Déroulez ensuite le menu **Démarrer, Exécuter** , tapez **regedit** et appuyez sur la touche **Entrée.***
*Développez successivement les clés **HKEY_ LOCAL _MACHINE, Software, Microsoft, Outlook Express.** Cliquez avec le bouton droit de la souris dans le volet droit de la fenêtre. Sélectionnez la commande **Nouveau, Valeur DWORD.** Donnez à la nouvelle valeur (aussi appelée clé) le nom **No Modify Accts** sans oublier les espaces entre les mots. Double-cliquez sur ce nom afin d'y affecter la valeur **1.** Quittez le **Registre** et relancez Outlook Express : la commande **Comptes** a disparu du menu **Outils.** Pour la faire réapparaître, refaites les manipulations ci-dessus en affectant, cette fois, la valeur **0** à la clé **No Modify Accts.***

Quoi de neuf sur le site Médéric?

http://aviquesnel.free.fr/Mederic

En rubrique Sécurité, un nouveau document général de 28 pages sur les nouveaux outils de séurité, antivirus Avatr et pare-feu Kerio Personal Firewall.

Eviter les pièges des hoax (canulars)

Qui n'a pas reçu un jour un avis de recherche d'une personne disparue, un appel à l'aide d'un jeune malade ou une info explosive qui changerait la face du monde ? Et peut-être avez-vous transféré ce courriel à vos correspondants... comme suggéré par le message ? Dans ce cas, vous êtes tombé dans le panneau ! Car, sur Internet, les canulars vont bon train par courrier électronique : on les appelle des hoax (prononcez hauks).

Vous connaissez à coup sûr quelques-unes des histoires qu'ils racontent... Celle de cette fillette de 7 ans, Amy Bruce, dont les multiples tumeurs nécessitent un traitement coûteux qu'une fondation s'engage à financer pour peu que l'histoire fasse le tour (virtuel) de la Terre. Ou celle du jeune Brian, petit Argentin, qui ne

sera sauvé que par la générosité des internautes qui, en renvoyant l'e-mail, financeront les 11 millions de dollars nécessaires à son opération (sic).

Il y a aussi quelques vieilles légendes urbaines remises au goût du jour, des histoires de seringues infectées par le VIH, dissimulées dans des sièges de cinéma, ou de terroristes invitant l'ami d'un ami d'un ami à ne pas prendre les transports en commun tel ou tel jour.

Mais ces histoires bidons sont vite dépassées par la rumeur, qui vise des personnalités ou des entreprises. Miss France est un homme, Bernard Kouchner s'est fait pincer à 240 km/h au volant d'une Ferrari, Nokia ou Alcatel offrent des téléphones portables à qui veut, Tommy Hilfiger exploite des Africains pour confectionner ses vêtements...

Bien sûr, tous ces courriels sont des tissus de mensonges, seulement... le mal est fait.

Des récits entre bidonnage...

Le plus cocasse, c'est que, contrairement au spam que vous recevez de la part d'illustres inconnus, le hoax vous est envoyé par des amis, soucieux de vous faire partager de bien malheureuses (ou croustillantes) histoires ! Impossible, donc, d'y échapper. Pourtant, si le hoax peut être exaspérant, parce qu'il joue sur la corde de l'émotion, du scandale ou de l'avidité, il reste a priori inoffensif pour un PC car il ne contient ni virus, ni spyware. Du moins en théorie, car il existe des exceptions : les « viroax » .

Il s'agit de messages dits « de sécurité », alarmistes, bien construits et utilisant un langage technique, qui invitent l'internaute à supprimer lui-même un fichier au coeur de son ordinateur sous prétexte qu'il serait un dangereux virus.

Ainsi, en 2001 et 2002, quelques milliers d'internautes ont reçu des messages leur demandant de rechercher, puis de supprimer, les fichiers sulfnbk.exe ou jdbgmgr.exe et de faire passer l'information. Ceux qui se sont exécutés ont détruit un composant, heureusement inoffensif, de Windows ! Les petits malins à l'origine de ces messages doivent en rire encore. Mais... justement, qui sont-ils ? Sans doute quelques farceurs qui se lancent un défi.

On peut certainement trouver d'autres explications en posant la question « à qui profite le crime ? » Ainsi, Bernard Kouchner expliquait en mars 2005, dans le journal Le Parisien , que la rumeur le concernant, lancée par l'extrême droite, le poursuivait depuis vingt ans. Or, le site hoaxbuster a constaté que cette rumeur avait refait surface en février 2005 sous la forme d'un message électronique, au moment même où un sondage le plaçait en tête des hommes politiques préférés des Français !

... rumeur et marketing !

Autre exemple, celui qui annonçait l'arrivée de nouvelles pièces turques ressemblant tellement aux pièces de 2 euros que nous en aurions bientôt plein les poches. Une « gigantesque escroquerie » selon les termes du message, évoquant même une « fausse monnaie européenne ». Et s'il s'agissait d'une campagne antiturque, en cette période de négociation avec l'Union européenne ?

En poussant les choses plus loin, on peut aussi imaginer que certaines marques sont à l'origine de hoax les mettant en accusation, même si rien n'est prouvé. L'intérêt ? Se voir cité, puis disculpé, sur des sites tels Hoaxbuster (lire l'encadré : Chasseur de hoax) ou ses équivalents anglo-saxons, puis par la presse lorsque l'affaire s'ébruite.

Le marketing viral, en plein boom, se révèle d'ailleurs bien plus rentable qu'une campagne publicitaire classique, comme le montre un exemple récent. Celui du site www.transatlantys.com qui annonçait la construction d'un tunnel ferroviaire sous-marin pour relier Paris à New York en huit heures. Derrière cette fausse information se cachait le site www.voyage-sncf.com qui souhaitait communiquer sur sa vente de billets d'avion !

Autre exemple de marketing viral, une vidéo amateur montrant une jeune fille lancée dans un panier de basket. Le film, qui a fait le tour du Net, était un faux. Le site Internet associé à la vidéo, bien vrai quant à lui, participait au lancement d'un film.

Ainsi va le hoax. Humour, déstabilisation et, depuis peu, opération marketing. Parions qu'il a encore de beaux jours devant lui !

Le ciné, c'est toute l'année !

S'il suffisait de renvoyer cet e-mail à sept personnes pour recevoir un pass cinéma d'un an, ça se saurait, non ? Combien sont tombés dans le panneau ?

Le clan des hoaxiens

Les malheurs de Penny Brown, Rachel Arlington, etc. les ont rendus célèbres. Pourtant, ils n'existent pas ! Ils sont ce qu'on appelle des hoaxiens !

Profession : chasseur de hoax

Guillaume, cofondateur du site Hoaxbuster (www.hoaxbuster.com) chasse sans relâche les hoax depuis mars*

2000. Il répond à nos questions.

Micro Hebdo : Comment est né Hoaxbuster, et comment fonctionnez-vous ?

Nous en avions assez de recevoir des e-mails bidons envoyés par nos amis. Comme les gens ont très peu de recul par rapport à ce qu'ils reçoivent et que les hoax sont faciles à démonter, nous avons créé cette base de données francophone.

Après réception des e-mails envoyés par les internautes, nous vérifions les numéros de téléphone et adresses e-mail, ainsi que les informations avec les organismes cités. Ensuite nous publions nos conclusions.

Le phénomène est-il en expansion ?

Oui. Simplement parce qu'aucun hoax n'a de date de péremption. Les anciens réapparaissent régulièrement, s'ajoutant aux nouveaux. Quant à la diffusion, elle est assurée par un nombre toujours croissant d'internautes. Bon nombre de hoax sont réactivés en toute bonne foi par les internautes eux-mêmes. Solidaridad con Brian et Rachel Arlington circulent ainsi depuis quatre ou cinq ans.

Quel intérêt à créer des hoax ?

L'amusement, la volonté de récolter des adresses pour des campagnes de spam (lorsque le hoax fonctionne très bien et revient dans la boîte de son créateur), la déstabilisation politique ou économique. Plus récemment, le secteur a été investi par le marketing viral.

Certains hoax ont-ils eu une incidence dramatique ? Plusieurs cas d'appels à témoin un peu précipités ont été lancés en ligne après des fugues d'adolescentes. Hélas, ils continuent à être diffusés plusieurs années après alors que, dans certains cas, les fugueuses étaient revenues à leur domicile. Résultat, ce genre d'affaire empoisonne la vie des intéressées.

Quel conseil donneriez-vous aux internautes ?

Il est utile de vérifier sur Hoaxbuster si le courriel qu'on s'apprête à faire suivre n'est pas un hoax. C'est en général le cas.

* *www.hoaxbuster.com*

Un CV sur Internet qui en jette

http://www.pixelpharmacy.com/