



CASES articles

Internet en vacances

Des surprises d'un autre genre

Pour plus de sécurité, adoptez les réflexes CASES !

Photos, virus, spyware – Un voyage aux conséquences désagréables

Virus informatiques et malwares – qui peut encore les ignorer ? Ils empoisonnent la vie des usagers d'Internet. Mais qu'advient-il de ces programmes malveillants pendant les vacances ? Hôtels, cybercafés ou magasins photos : nombreux sont les endroits où des ordinateurs sont à la disposition des voyageurs. La prudence y est toutefois de rigueur. Les utilisateurs n'ont souvent aucune idée de ce que l'on peut trouver sur les ordinateurs en libre-service. L'utilisation de supports de données pour le stockage ou l'impression de photos peut ainsi avoir de désagréables conséquences.

Le voyage est réservé, la valise est prête, le taxi attend devant la porte. Au bout de quelques heures, le rêve de vacances se réalise enfin : les montagnes, la plage ou même un voyage par-delà les océans. Les amis et membres de la famille qui sont restés à la maison ne doivent bien sûr pas être oubliés. Grand-mère reçoit une carte postale, la collègue de travail un e-mail comportant un lien vers les photos de la dernière fête sur la plage et les copains de l'équipe de foot auront le plaisir de visionner les photos de la sortie en canoë, envoyées dans une enveloppe portant le cachet du bureau de poste du pays. Impossible de trouver encore du temps pour virer le loyer au propriétaire avant de partir, mais pas de souci puisque cela peut être fait aisément depuis l'hôtel, avant le petit-déjeuner. Dans un cybercafé, par un bel après-midi ensoleillé, on peut aussi donner l'ordre de vendre



son paquet d'actions. La meilleure amie est avisée tous les soirs des aventures de la journée au cours d'une longue séance de chat sur MSN. Toutes ces actions sont rendues possibles grâce à l'ordinateur et à Internet.

De nombreux voyageurs profitent de ces services. Cependant ils ne peuvent jamais être vraiment sûrs que les ordinateurs de l'hôtel ou du cybercafé ne sont pas infectés par des logiciels malveillants, tels que des spywares par exemple. Ces programmes recueillent des informations personnelles sur l'utilisateur de la machine et l'espionnent. Comment un voyageur peut-il être sûr que l'ordinateur du magasin de photos n'est pas infecté par des virus ? De même, un support de données remis pour le développement de photos peut aisément être infecté par des logiciels malveillants.

Titre intermédiaire : **Comment fonctionne un spyware ?**

Les spywares ont pour vocation principale d'épier les habitudes d'un usager d'Internet. Les informations ainsi collectées sont transmises à des tiers à l'insu de l'utilisateur via Internet en général. [Dans le cas d'un ordinateur public, dans un cybercafé par exemple, les pirates peuvent également se faire passer pour des utilisateurs normaux et ainsi collecter périodiquement, directement sur place, les données sur l'ordinateur concerné.]

Sur son propre ordinateur, l'utilisateur contracte habituellement ce genre de programmes en surfant sur Internet ou en téléchargeant des logiciels publicitaires ou d'autres programmes gratuits. Les spywares sont ainsi très souvent présents dans les applications audio, les programmes peer-to-peer ou encore

les programmes de messagerie instantanée.

Différentes formes de spyware peuvent être distinguées. Les « spywares utilisés à des fins publicitaires » sont, par exemple, employés pour collecter des données sur l'utilisateur. Ils interagissent toutefois de manière visible avec ce dernier. Cela se traduit notamment par l'affichage de bandeaux publicitaires ciblés, de fenêtres pop-up ou de liens publicitaires spécifiques sur les pages consultées.

Les « espions » recueillent des données sur l'utilisateur, mais cette fois-ci de façon masquée. La collecte des données et l'éventuelle utilisation de celles-ci s'effectuent à l'insu de l'utilisateur. La présence de ces espions est ici délibérément dissimulée. Les données recueillies subrepticement peuvent, entre autres, être utilisées à des fins statistiques, de marketing ou de surveillance du cyberspace.

Les « spywares intégrés » sont intégrés aux codes sources d'une application logicielle. Ils possèdent une fonctionnalité propre de collecte et de transmission de données via Internet. Ils peuvent par exemple être dissimulés dans des logiciels gratuits, proposés au téléchargement sur le net. Le spyware collecte les informations pendant que l'utilisateur est en train de surfer, il examine les applications installées sur l'ordinateur ainsi que les données présentes et détermine leur exploitabilité.

Le « spyware externe » est un programme autonome. Son but est de collecter et de transmettre des données. Ainsi, le programme Gator permet de recueillir le nom de l'utilisateur, les mots de passe ainsi que les informations relatives aux cartes bancaires utilisées sur des sites d'e-commerce. Bien que cryptées, ces données peuvent être extraites par Gator ou par des intrus.

La multiplication des types de spywares démontre qu'ils représentent une réelle menace, que ce soit pour la confidentialité ou pour l'intégrité des données. De plus, ils constituent une atteinte à la

vie privée. Les spywares fonctionnent à l'insu de l'utilisateur et ne sont que difficilement décelables, même à l'aide de moyens techniques ; ils constituent donc des instruments très appréciés des cybercriminels.

Titre intermédiaire : **Voleurs de données en vacances**

Les pirates sont parfaitement conscients de la grande popularité d'Internet pendant les vacances. Naguère, les estivants imprudents devenaient les victimes de pickpockets experts ; de nos jours, les criminels se sont créé un domaine d'activités supplémentaire très lucratif : le vol de données. Ce sont en particulier les mots de passe, les numéros de cartes de crédit et autres données bancaires qu'ils cherchent à obtenir.

L'utilisateur d'ordinateurs publics, que ce soit dans des hôtels ou des cybercafés, s'expose à un triple risque. Il ne peut savoir si l'appareil mis à sa disposition et les applications qu'il comporte sont conformes aux exigences minimales en matière de sécurité. Il ne sait pas non plus dans quelle mesure une éventuelle utilisation insouciante par l'utilisateur précédent a pu ou non infecter la machine par un spyware. De plus, des cybercriminels peuvent très bien avoir directement préparé l'ordinateur public en question : les pirates ont peut-être installé un spyware de façon ciblée sur le PC afin de collecter les données des utilisateurs, telles que mots de passe et numéros de cartes de crédit. Ce genre de pratique est, hélas, devenu courant.

Pour les vacanciers, il est donc fortement conseillé de ne pas utiliser d'ordinateurs publics à des fins d'e-commerce ou d'e-banking. Il convient également d'être prudent lors de la consultation d'e-mails contenant des données commerciales : pour bien faire il faudrait tout bonnement l'éviter. L'utilisateur devrait également être conscient que tout mot de passe utilisé afin d'obtenir l'accès à des services, tels que les messageries instantanées, peut être intercepté.

Les spywares en faits et chiffres

Selon les indications de la société anti-spyware Lavasoft, 90 % des ordinateurs sont touchés par des spywares – pour ainsi dire toutes les machines reliées à internet. 88 % des ordinateurs stockent des données personnelles, telles que numéros de sécurité sociale, informations bancaires, informations de santé et curriculum vitæ. Sur ces ordinateurs sont effectuées des opérations sensibles, comme par exemple de l'e-commerce et de l'e-banking. 78 % des ordinateurs ne disposent pas des équipements élémentaires de sécurité et ne peuvent donc pas protéger efficacement l'utilisateur et sa famille contre la cybercriminalité.

Si l'utilisation d'un ordinateur public ne peut être évitée, celui-ci devrait être analysé grâce à un logiciel anti-spyware avant toute opération. Ces logiciels anti-spyware sont proposés gratuitement (pour les utilisateurs privés) au téléchargement sur Internet.

Les spywares ne sont pas les seules mauvaises surprises pouvant guetter les voyageurs.

Titre intermédiaire : **Virus, supports de données et photos de vacances**

Presque tous les vacanciers sont aujourd'hui équipés d'appareils photo numériques. Ces précieux assistants permettent d'immortaliser les plus beaux souvenirs de vacances, mais qu'en est-il en cas de perte de la memory card contenant ces photos, ou lorsque l'on attrape des virus sur les bornes des studios de développement de photos ?

De nombreux voyageurs utilisent des supports de données afin de mettre en ligne des photos, les stocker ou les porter au développement dans un magasin spécialisé. Un support de données de faibles dimensions, comme une clé USB par exemple, est toutefois

facile à égarer dans un cybercafé. Si les photos n'ont pas été sauvegardées ailleurs, les souvenirs de vacances numériques sont définitivement perdus. Si, outre les photos, d'autres informations importantes sont stockées sur ce support de données, il ne peut être exclu que celles-ci soient utilisées par un tiers. Les informations privées ou commerciales se trouvant sur un support de données devraient être effacées avant toute utilisation de ce dernier en vacances. Ces supports étant de très faibles dimensions, les voyageurs devraient particulièrement veiller à ne pas les perdre.

Les supports de données et autres cartes mémoire pour appareils photo sont souvent infectés par des malwares pendant les vacances. Cela peut se faire par le biais d'un magasin photos utilisant des ordinateurs infectés. Une mauvaise surprise attend ensuite le voyageur lors de sa prochaine connexion sur son propre ordinateur. Ces supports devraient donc subir une analyse de virus. avant toute utilisation.

Conseils de sécurité :

Des liens utiles et des logiciels anti-spyware gratuits pour les utilisateurs privés sont disponibles sur :

<http://www.spychecker.com>

<http://www.safer-networking.org> (Spybot – anti-spyware)

Avant toute publication de photos de vacances, les voyageurs devraient porter une attention particulière au choix des photos qu'ils vont rendre accessibles par le biais d'applications Internet et à qui elles seront accessibles. La publication de photos de tiers est légalement soumise à autorisation de ceux-ci. Lorsqu'il s'agit de mineurs, l'autorisation des parents doit, de plus, être demandée. De plus amples informations sont disponibles sur www.cases.lu, sous la rubrique « Publications », fiche thématique « Droit à l'image ».

Les spywares sont illégaux

La directive 95/46 de la Communauté européenne prévoit que ni la collecte de données personnelles, ni le traitement de ces données ne sont autorisés sans l'accord formel de la personne concernée. La directive 2002/58 définit le statut des spywares et des technologies équivalentes. Elle précise que ces programmes peuvent s'introduire dans les appareils des utilisateurs à l'insu de ces derniers. Ces programmes peuvent ensuite accéder à des informations ou tracer les activités de l'utilisateur. Les spywares et technologies équivalentes peuvent ainsi constituer une grave atteinte à la sphère privée de l'utilisateur.

Définition : messagerie instantanée

Les messageries instantanées permettent l'échange d'informations sous forme écrite entre deux ou plusieurs personnes par le biais d'Internet. Ces personnes sont alors en ligne et les échanges se font en temps réel.

Définition : peer-to-peer

Le peer-to-peer (ou pair à pair) désigne l'échange de données entre pairs. Cela signifie que tous les utilisateurs sont égaux et qu'ils peuvent aussi bien solliciter que mettre à disposition des données.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu