Nos ordinateurs sans virus !

Georges Khaznadar <georgesk@ofset.org>

association DKLibre

mai 2009

Table des matières

Introduction

Un système informatique totalement sûr n'existe pas, du moins si l'on veut qu'il puisse communiquer. J'ai cependant déjà vu un ordinateur totalement sûr. Il était dans le coffre-fort d'un centre de documentation et n'était pas branché.
Le nombre de virus informatiques existants n'est pas aisé à évaluer. Chaque producteur de logiciel anti-virus a intérêt à gonfler ce nombre pour promouvoir son produit. Selon Wikipedia, le producteur d'anti-virus SOPHOS en recenserait 95 000, cependant que le nombre de virus circulant réellement est plus faible.
La base de donnée de signatures virales de ClamAV, le seul anti-virus sous licence libre et qui est construit collaborativement, contenait 549811 entrées le 9 mai 2009 à 20 heures 51 minutes.

Qu'est-ce qu'un virus ?

Répondez à ce petit questionnaire :

1. Un virus est un logiciel qui peut abîmer mon ordinateur (oui/non)
2. Un virus est un logiciel qui peut espionner mes activités (oui/non)
3. Un virus est un logiciel qui peut me faire perdre des données (oui/non)
4. Un virus est synonyme d'un cheval de Troie (oui/non)
5. Un virus est quelque chose qui est détecté par un anti-virus (oui/non)

Qu'est-ce qu'un virus ?

Analyse des réponses :

Qu'est-ce qu'un virus ?

Analyse des réponses :

1. Un virus est un logiciel qui peut abîmer mon ordinateur Faux

Qu'est-ce qu'un virus ?

Analyse des réponses :

1. Un virus est un logiciel qui peut abîmer mon ordinateur Faux
2. Un virus est un logiciel qui peut espionner mes activités Faux

Qu'est-ce qu'un virus ?

Analyse des réponses :

1. Un virus est un logiciel qui peut abîmer mon ordinateur Faux
2. Un virus est un logiciel qui peut espionner mes activités Faux
3. Un virus est un logiciel qui peut me faire perdre des données Faux

Qu'est-ce qu'un virus ?

Analyse des réponses :

1. Un virus est un logiciel qui peut abîmer mon ordinateur Faux
2. Un virus est un logiciel qui peut espionner mes activités Faux
3. Un virus est un logiciel qui peut me faire perdre des données Faux
4. Un virus est synonyme d'un cheval de Troie Faux

Qu'est-ce qu'un virus ?

Analyse des réponses :

1. Un virus est un logiciel qui peut abîmer mon ordinateur Faux
2. Un virus est un logiciel qui peut espionner mes activités Faux
3. Un virus est un logiciel qui peut me faire perdre des données Faux
4. Un virus est synonyme d'un cheval de Troie Faux
5. Un virus est quelque chose qui est détecté par un anti-virus Faux

Qu'est-ce qu'un virus ?

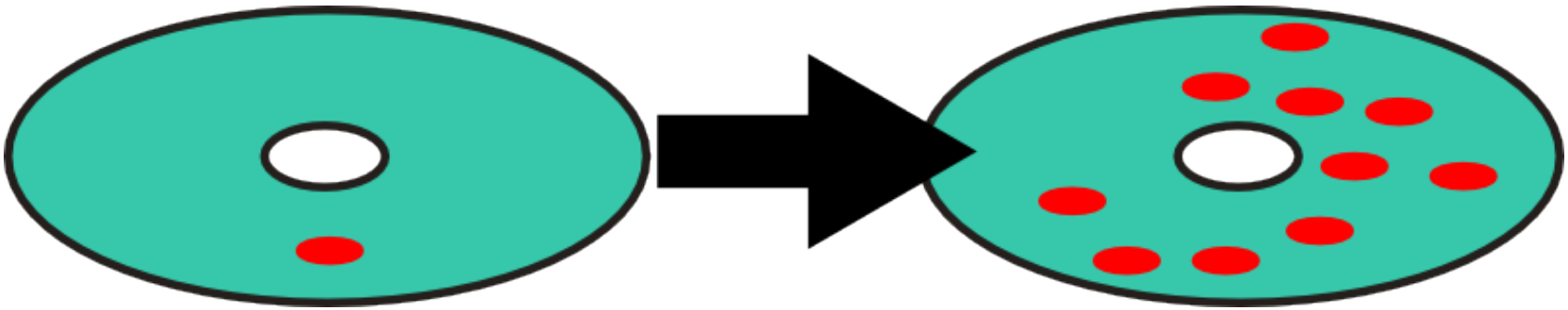
Analyse des réponses :

1. Un virus est un logiciel qui peut abîmer mon ordinateur Faux
2. Un virus est un logiciel qui peut espionner mes activités Faux
3. Un virus est un logiciel qui peut me faire perdre des données Faux
4. Un virus est synonyme d'un cheval de Troie Faux
5. Un virus est quelque chose qui est détecté par un anti-virus Faux

Définition : un virus informatique est une suite de codes qui possède la propriété de s'auto-répliquer dans l'environnement d'un ordinateur.

Qu'est-ce qu'un virus ?

Les virus ont fait parler d'eux à cause de leurs « charges nuisibles » (en anglais *payload*, littéralement charge utile), mais la charge nuisible ne définit pas le caractère viral. On reconnaît ainsi un virus : à partir du moment où une copie du virus est installée dans une ordinateur, le nombre de ces copies va en augmentant.



Propagation d'un virus sur le disque dur d'un ordinateur.

Qu'est-ce qu'un cheval de Troie ?

Homère a chanté la ruse d'Ulysse, qui offrit aux habitants de Troie un monumental cheval, dont ils ne s'avisèrent pas assez tôt d'explorer les entrailles ... ce qui mit fin à la guerre de Troie, par la victoire des Grecs.

Qu'est-ce qu'un cheval de Troie ?

Homère a chanté la ruse d'Ulysse, qui offrit aux habitants de Troie un monumental cheval, dont ils ne s'avisèrent pas assez tôt d'explorer les entrailles ... ce qui mit fin à la guerre de Troie, par la victoire des Grecs.

L'équivalent informatique de la ruse d'Ulysse, c'est :

1. mettre à disposition gratuitement un logiciel d'aspect agréable ;

Qu'est-ce qu'un cheval de Troie ?

Homère a chanté la ruse d'Ulysse, qui offrit aux habitants de Troie un monumental cheval, dont ils ne s'avisèrent pas assez tôt d'explorer les entrailles ... ce qui mit fin à la guerre de Troie, par la victoire des Grecs.

L'équivalent informatique de la ruse d'Ulysse, c'est :

1. mettre à disposition gratuitement un logiciel d'aspect agréable ;
2. ne pas garantir le logiciel ;

Qu'est-ce qu'un cheval de Troie ?

Homère a chanté la ruse d'Ulysse, qui offrit aux habitants de Troie un monumental cheval, dont ils ne s'avisèrent pas assez tôt d'explorer les entrailles ... ce qui mit fin à la guerre de Troie, par la victoire des Grecs.

L'équivalent informatique de la ruse d'Ulysse, c'est :

1. mettre à disposition gratuitement un logiciel d'aspect agréable ;
2. ne pas garantir le logiciel ;
3. ne pas autoriser à voir ce qu'il y a *dans* le logiciel ;

Qu'est-ce qu'un cheval de Troie ?

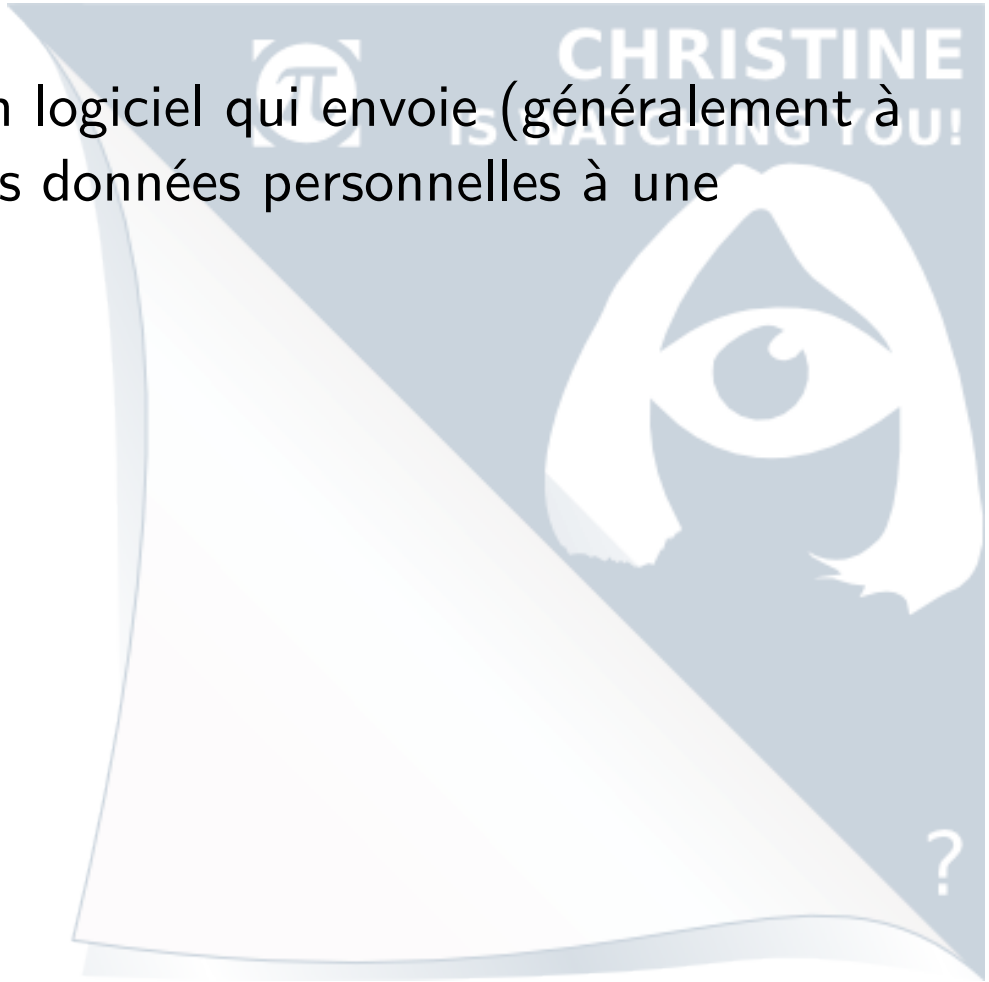
Homère a chanté la ruse d'Ulysse, qui offrit aux habitants de Troie un monumental cheval, dont ils ne s'avisèrent pas assez tôt d'explorer les entrailles ... ce qui mit fin à la guerre de Troie, par la victoire des Grecs.
L'équivalent informatique de la ruse d'Ulysse, c'est :

1. mettre à disposition gratuitement un logiciel d'aspect agréable ;
2. ne pas garantir le logiciel ;
3. ne pas autoriser à voir ce qu'il y a *dans* le logiciel ;
4. ajouter un rôle indélicat au logiciel (par exemple communiquer un carnet d'adresses).

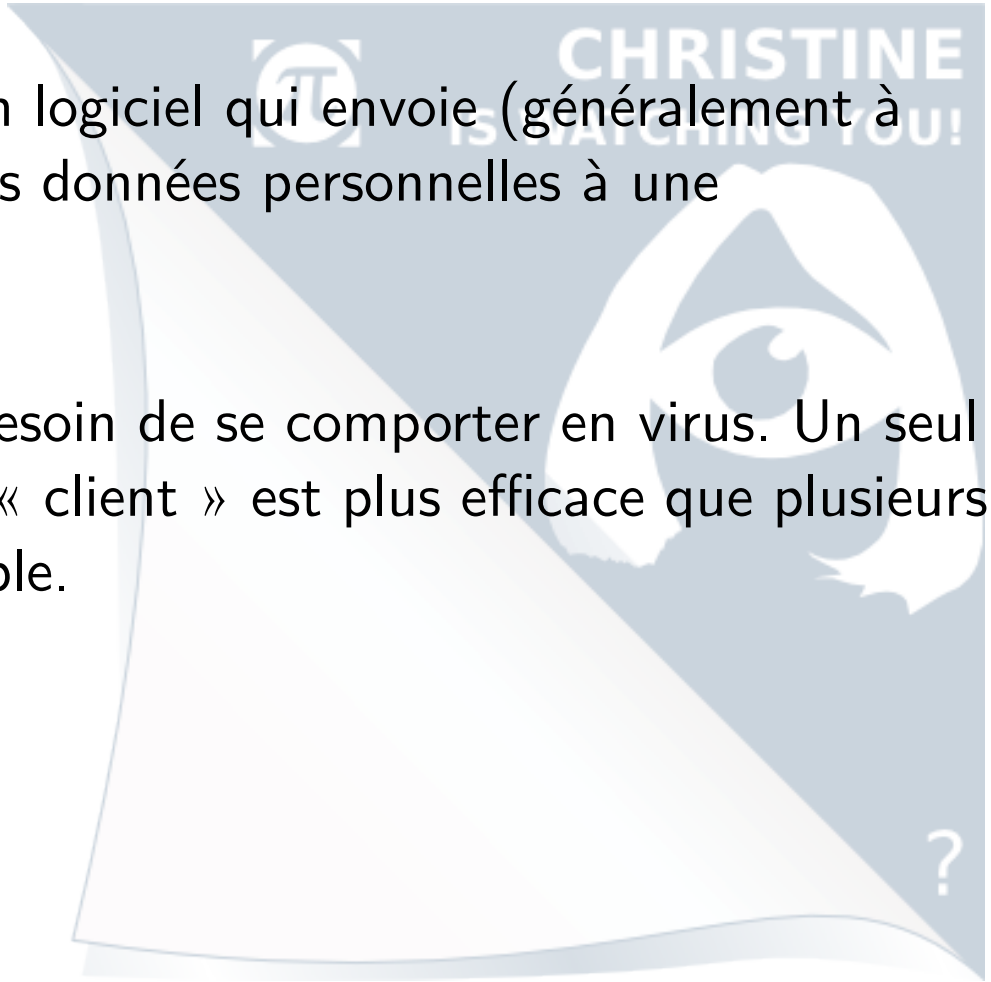
Qu'est-ce qu'un logiciel espion (spyware) ?

Qu'est-ce qu'un logiciel espion (spyware) ?

Un logiciel espion, c'est un logiciel qui envoie (généralement à l'insu de son utilisateur), des données personnelles à une destination non autorisée.



Qu'est-ce qu'un logiciel espion (spyware) ?



Un logiciel espion, c'est un logiciel qui envoie (généralement à l'insu de son utilisateur), des données personnelles à une destination non autorisée.

Un logiciel espion n'a pas besoin de se comporter en virus. Un seul exemplaire installé chez un « client » est plus efficace que plusieurs exemplaires installés ensemble.

Qu'est-ce qu'un logiciel espion (spyware) ?

Un logiciel espion, c'est un logiciel qui envoie (généralement à l'insu de son utilisateur), des données personnelles à une destination non autorisée.

Un logiciel espion n'a pas besoin de se comporter en virus. Un seul exemplaire installé chez un « client » est plus efficace que plusieurs exemplaires installés ensemble.

Certains logiciels ordinaires envoient tant de données personnelles à leurs concepteurs qu'ils ne sont pas loin de la classification de logiciel espion.

Qu'est-ce qu'un ver informatique ?

Un ver est similaire à un virus en ce qu'il tend à s'auto-répliquer. La différence est qu'il utilise les protocoles des réseaux pour se propager d'un ordinateur à l'autre.

Logiciels installés d'origine

Quand on achète un ordinateur, il comporte des logiciels déjà installés la plupart du temps.

La seule garantie que ces logiciels soient inoffensifs vient de leurs fabricants... Mais avez-vous lu la garantie ?

8. LIMITATION DE RESPONSABILITÉ. SAUF DANS LE CADRE DU RECOURS EXCLUSIF EXPOSE CI-DESSUS ET SAUF DISPOSITION CONTRAIRE DE L'ARTICLE 14, EN AUCUN CAS ADOBE, SES SOCIETES AFFILIEES OU SES FOURNISSEURS NE SERONT RESPONSABLES ENVERS VOUS POUR TOUTES PERTES, DOMMAGES, RÉCLAMATIONS OU QUELQUES FRAIS QUE CE SOIT, Y COMPRIS TOUS DOMMAGES CONSECUTIFS, INDIRECTS OU INCIDENTS, TOUT MANQUE À GAGNER, PERTES D'ECONOMIE, DOMMAGES RESULTANT DE

Logiciels installés volontairement plus tard

Quand on achète un ordinateur avec un système Windows(^{TM}), il contient peu de logiciels spécialisés. On y ajoute couramment des logiciels pour écrire du texte, pour traiter des photographies, etc.

Que ces logiciels supplémentaires soient vendus ou distribués gratuitement, sont-ils garantis, et qui garantit qu'ils ne font que ce qu'ils annoncent ?

Plusieurs logiciels libres sont diffusés gratuitement, sans garantie. Quand on les récupère depuis le site web officiel, on peut aussi y trouver leur source, la faire expertiser et recompiler... Cependant on trouve aussi ces logiciels, téléchargeables depuis d'autres sites, ... qui dit que ce sont exactement les mêmes ?

Logiciels installés involontairement

Par commodité, un grand nombre d'ordinateurs sont réglés pour télécharger et exécuter immédiatement de nombreux contenus actifs (programmes), quand ceux-ci sont référencés par un courriel ou une page web.

Depuis 2004 environ, le réglage préconisé par le fabricant fait que l'exécution d'un programme non certifié est précédée par un avertissement, et l'utilisateur peut décider de ne pas lancer le programme.

Prise de contrôle à distance

Il est facile de prendre le contrôle d'un ordinateur à travers Internet, pour peu que celui-ci ait lancé un logiciel permettant ce contrôle distant. Par exemple le programme très pratique VNC est idéal pour cela.

Encore faut-il s'assurer que la personne qui prend le contrôle soit autorisée à le faire !

Vulnérabilités

Par construction, la mémoire des ordinateurs les plus répandus sert indifféremment pour contenir des programmes (instruments de contrôle) et des données. On découvre souvent que tel ou tel programme possède une faille, c'est à dire qu'il est possible de luis communiquer des données d'une telle façon que celles-ci soient mélangées aux zones de programmes.

La personne qui réussit cela réalise un *exploit* (mot anglais signifiant exploitation), et peut aller jusqu'à lancer une opération arbitraire sur l'ordinateur-cible. Il dispose des droits et privilèges du programme qu'il a réussi à modifier. Si les privilèges sont mal séparés, ça peut aller jusqu'à un contrôle total de l'ordinateur.

Vulnérabilités

Par construction, la mémoire des ordinateurs les plus répandus sert indifféremment pour contenir des programmes (instruments de contrôle) et des données. On découvre souvent que tel ou tel programme possède une faille, c'est à dire qu'il est possible de luis communiquer des données d'une telle façon que celles-ci soient mélangées aux zones de programmes.

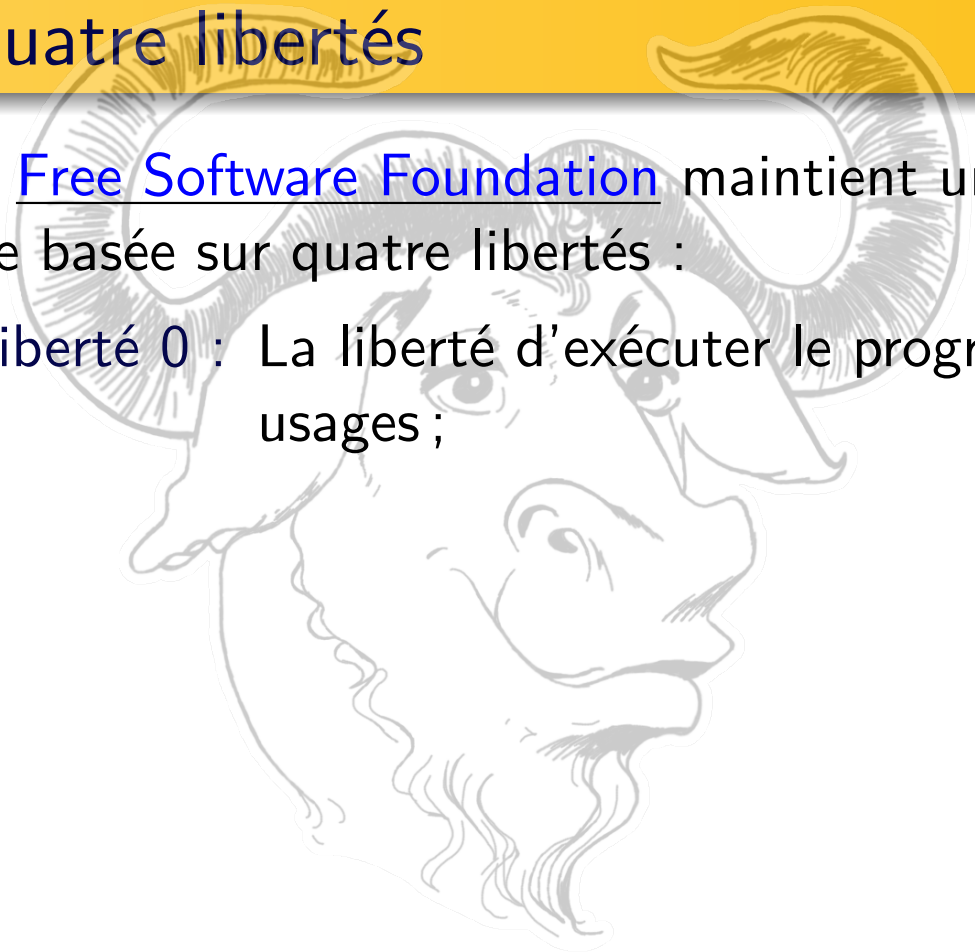
La personne qui réussit cela réalise un *exploit* (mot anglais signifiant exploitation), et peut aller jusqu'à lancer une opération arbitraire sur l'ordinateur-cible. Il dispose des droits et privilèges du programme qu'il a réussi à modifier. Si les privilèges sont mal séparés, ça peut aller jusqu'à un contrôle total de l'ordinateur.

Ne négligez jamais l'installation de correctifs pour les logiciels dont des vulnérabilités ont été signalées.

Depuis plus de dix ans, on n'a pas constaté de prolifération de virus sur certains systèmes informatiques libres.

Pourquoi ne pas en profiter ? En 2009, on peut disposer d'un environnement complet permettant de traiter des documents textes, images et multimédia, d'accéder à Internet et aux diverses communications (courriel, messagerie instantanée, téléphonie IP), avec une interface simple, le tout tenant sur quelques giga-octets.

Les quatre libertés



La Free Software Foundation maintient une définition du logiciel libre basée sur quatre libertés :

Liberté 0 : La liberté d'exécuter le programme – pour tous les usages ;

Les quatre libertés

La Free Software Foundation maintient une définition du logiciel libre basée sur quatre libertés :

Liberté 0 : La liberté d'exécuter le programme – pour tous les usages ;

Liberté 1 : La liberté d'étudier le fonctionnement du programme – ce qui suppose l'accès au code source ;

Les quatre libertés

La Free Software Foundation maintient une définition du logiciel libre basée sur quatre libertés :

- **Liberté 0 :** La liberté d'exécuter le programme – pour tous les usages ;
- **Liberté 1 :** La liberté d'étudier le fonctionnement du programme – ce qui suppose l'accès au code source ;
- **Liberté 2 :** La liberté de redistribuer des copies – ce qui comprend la liberté de vendre des copies ;

Les quatre libertés

La Free Software Foundation maintient une définition du logiciel libre basée sur quatre libertés :

- **Liberté 0 :** La liberté d'exécuter le programme – pour tous les usages ;
- **Liberté 1 :** La liberté d'étudier le fonctionnement du programme – ce qui suppose l'accès au code source ;
- **Liberté 2 :** La liberté de redistribuer des copies – ce qui comprend la liberté de vendre des copies ;
- **Liberté 3 :** La liberté d'améliorer le programme et de publier ces améliorations – ce qui suppose, là encore, l'accès au code source.

Les quatre libertés

La Free Software Foundation maintient une définition du logiciel libre basée sur quatre libertés :

- Liberté 0 : La liberté d'exécuter le programme – pour tous les usages ;
- Liberté 1 : La liberté d'étudier le fonctionnement du programme – ce qui suppose l'accès au code source ;
- Liberté 2 : La liberté de redistribuer des copies – ce qui comprend la liberté de vendre des copies ;
- Liberté 3 : La liberté d'améliorer le programme et de publier ces améliorations – ce qui suppose, là encore, l'accès au code source.

Concrètement, ceci permet de copier légalement les média vifs quand ceux-ci sont basés sur des logiciels libres.

Présentation d'une clé USB vive

La clé USB que je vous présente concentre dans une place minime un système complet, adapté à de nombreux usages :

Bureautique : la suite OpenOffice.org complète est là.

Dessin, retouche photo : logiciel GIMP, leader dans ce domaine.

Internet : Firefox, totalement conforme aux normes du W3C, Gftp pour les téléchargements.

Messagerie instantanée : Pidgin, un client muti-protocoles.

Téléphonie IP : Ekiga, conforme au standard SIP.

Multimédia : le lecteur multimédia de Gnome.

Littérature : un lecteur de livres électronique, et une partie de la bibliothèque libre Project Gutenberg.

...

Le démarrage

Depuis 2004, tous les ordinateurs vendus sont capables de démarrer à partir d'un disque ou d'une clé USB. On peut paramétrer une machine précise pour le faire par défaut, sans poser de question. Cependant, même quand une machine n'est pas paramétrée spécialement, il y a une touche du clavier qui permet de choisir le mode de démarrage.

Mode d'emploi : sur la plupart des ordinateurs testés, il faut appuyer un moment sur la touche **F8** pendant que celui-ci est dans les étapes préliminaires à son démarrage (juste après l'allumage ou le redémarrage), pour pouvoir choisir un périphérique USB. Le choix se fait dans un menu semi-graphique, où on trouve le nom de la clé USB branchée.

Durée du démarrage. Quand le choix de la clé USB est fait, le démarrage lui-même dure une minute environ.

Comment est-ce possible ?

C'est possible, la preuve est là.

Une meilleure question serait : comment se fait-il que les leaders des ventes de logiciel, qui gèrent des budgets de recherche – développement énormes, ne proposent pas ce genre de combinaison ?

Comment est-ce possible ?

C'est possible, la preuve est là.

Une meilleure question serait : comment se fait-il que les leaders des ventes de logiciel, qui gèrent des budgets de recherche – développement énormes, ne proposent pas ce genre de combinaison ?

Il y a plusieurs réponses à cette question. Une d'entre elles est qu'il est difficile de réaliser des logiciels propriétaires (dont le fonctionnement doit rester caché) et en même temps de permettre à tous les autres concepteurs de logiciels de réutiliser de façon optimale les briques de logiciel déjà présentes.

Comment est-ce possible ?

C'est possible, la preuve est là.

Une meilleure question serait : comment se fait-il que les leaders des ventes de logiciel, qui gèrent des budgets de recherche – développement énormes, ne proposent pas ce genre de combinaison ?

Il y a plusieurs réponses à cette question. Une d'entre elles est qu'il est difficile de réaliser des logiciels propriétaires (dont le fonctionnement doit rester caché) et en même temps de permettre à tous les autres concepteurs de logiciels de réutiliser de façon optimale les briques de logiciel déjà présentes. Avez-vous remarqué que quand on installe un nouveau logiciel propriétaire, on doit à chaque fois mettre en place des centaines de méga-octets de bibliothèques logicielles non-partagées ?

Mes données

La clé USB est structurée en plusieurs partitions.

Les « Documents Communs » : Une des partitions, ainsi dénommée, reste accessible dans tous les cas, que l'ordinateur ait été démarré par la clé USB ou non, et quel que soit son type.

Les partitions spécifiques : Les autres partitions de la clé ne sont accessibles que quand la clé a été démarrée et contrôle l'ordinateur. En particulier, les données sur le **bureau** de l'interface graphique ne sont accessibles que quand la clé contrôle l'ordinateur. C'est aussi automatiquement le cas des courriers électroniques et du cache d'accès à Internet.

Par défaut, les logiciels enregistrent les données dans les partitions spécifiques.

Ma vie privée

On n'est pas à l'abri d'une perte de clé USB. Les logiciels de la clé permettent de crypter/décrypter les données que l'on souhaite garder privées, à l'aide de méthodes de *cryptographie forte*.

Le simple fait de déposer ses documents sur le *bureau* plutôt que dans le dossier *Documents Communs* protège partiellement la privauté, face à des personnes qui ignorent le mode de démarrage de la clé.

Nomadisme

Quand la même clé vive est utilisée sur plusieurs ordinateurs différents, on retrouve à chaque fois son environnement personnalisé, ses documents personnels, etc.

Il est possible d'installer le contenu de la clé sur une partie du disque dur d'un ordinateur.

Les licences libres utilisées permettent de copier légalement le contenu de la clé USB autant de fois qu'on le souhaite.

Personnalisation, nouveaux logiciels

Il est possible de personnaliser de nombreux aspects du fonctionnement de la clé USB, bien au-delà des simples fonds d'écran et thème de style du gestionnaire de fenêtres. Les personnalisations sont conservées de la même façon que sur un ordinateur ordinaire.

Pour les nouveaux logiciels, un système de gestion intégré permet d'installer/désinstaller les paquets logiciels Debian : en fait il s'agit de la plus grande logithèque libre mondiale, **27611 paquets logiciels distincts** à la date de rédaction.

Les paquets issus de dépôts Debian sont authentifiés par une signature numérique, et font l'objet de suivis de qualité très réactifs. Votre gestionnaire sait reconnaître les signatures électroniques et authentifier les paquets logiciels.

Crédits


© 2009 G. Khaznadar, licence :
Creative Commons Attribution ShareAlike

d'après AlbanEye, © 2009, François Revol, licence MIT


ressource de Wikipedia, © 2004 Ross Burgess, il s'agit du cheval de Troie fait pour le film « Troie » conservé sur le littoral à Çanakkale, en Turquie, licence : GFDL

© 2007 Chartmann, utilisateur de Wikipedia, licence : GFDL


, licence :
Creative Commons Attribution ShareAlike

Crédits

- un court extrait de la licence d'Adobe Acrobat Reader. Standard version 7.0, nous utilisons le droit de courte citation.

© Etienne Suvasa, Peter Gerwinski, licence : Art Libre