Virus

Aujourd'hui, les virus informatiques se propagent le plus souvent par le courrier électronique (en pièces jointes ou fichiers attachés) et par le téléchargement en P2P (*peer-to-peer* : eDonkey, Gnutella, BitTorrent...). Attention, cela est plus rare, mais un virus peut aussi s'attraper en visitant un site web malin.

Lorsque vous recevez un e-mail, ne vous fiez pas seulement à l'expéditeur pour ouvrir une pièce jointe, car un message porteur de virus peut avoir été envoyé depuis l'ordinateur infecté d'un de vos contacts (amis, collègues, clients...) à son insu, ou par un usurpateur.

Conseil n° 1 : Protégez-vous !

Procurez-vous un anti-virus (gratuit ou payant) et vérifiez quotidiennement la disponibilité de mises à jour (un bon anti-virus fait cela automatiquement).

Conseil n°2 : Utilisateurs d'Outlook, placez Outlook en zone de sécurité "sensible"

Allez dans le menu "Outils", ligne "Options", onglet "Sécurité" et cochez la ligne "Zone de sites sensibles". Cette procédure peut varier légèrement suivant votre version d'Outlook.

Conseil n°3 : Etudiez les caractéristiques de vos messages avant de les ouvrir

Les e-mails avec pièces jointes inférieures à 70 ko, envoyés par des inconnus et rédigés en anglais sont très probablement porteurs de virus. Attention aux fichiers à **doubles extensions**, par exemple, "ma-photo.jpg.pif" ou "lettre.doc.vbs", *etc.* Seule la dernière extension compte. Les fichiers .pif, .vbs, .exe, .com et .cpl sont généralement des virus.

Conseil n°4 : Ne prenez pas ce qui est écrit pour argent comptant...

Afin de tromper votre vigilance, certains virus ajoutent, à la fin des e-mails infectés qu'ils envoient, une note selon laquelle l'e-mail que vous lisez a été scanné et déclaré "sans virus" par un logiciel anti-virus, par exemple :

```
*-*-* Mail_Scanner: No Virus
*-*-* SYMANTEC- Anti_Virus Service
*-*-* http://www.symantec.com
```

Prenez donc le temps d'étudier les caractéristiques de votre message (expéditeur, langue, taille et type du fichier attaché) avant d'ouvrir une pièce jointe.

Conseil n°5 : Si vous utilisez une vieille version d'Outlook ou Outlook Express...

Si vous utilisez encore une vieille version (antérieure à 2000) non corrigée d'Outlook ou Outlook Express, il est possible que certains virus se trouvant en pièces jointes soient activés automatiquement à la lecture des messages qui les contiennent. Pour éviter cela :

1) Désactivez la visualisation automatique de vos messages : Dans Outlook Express 4 par exemple, allez dans "Affichage", puis "Disposition" et décochez la ligne "Utiliser le volet de visualisation". La manœuvre est similaire dans les autres versions d'Outlook Express (allez voir dans les Options si vous ne trouvez pas).

2) Activez la lecture des messages en format brut : Allez dans le menu "Outils", ligne "Options", onglet "Lecture" et cochez la ligne "Lire tous les messages en texte clair". Cela désactivera toutes les mises en formes, fioritures, images et les éventuels partie du message visant à vous inoculer le virus. Attention, si un fichier joint est contaminé par un virus, cela reste un danger potentiel, mais tant que vous ne touchez

pas à ce fichier attaché, vous ne craignez quasiment rien. Si vous avez un doute, contactez l'expéditeur, **si vous le connaissez**, pour qu'il vous explique le contenu de son message, ou supprimez le message.

Spam (publicité non sollicitée, publicité sauvage, pourriel, pollupostage)

Le *spam* est une appellation qui englobe tous les messages commerciaux, souvent en anglais, que vous recevez sans avoir donné votre accord.

Le *spam* promeut généralement le Viagra, le Xanax, le Valium, le Cialis, les recettes miracles pour maigrir, les diplômes universitaires sans cours ni examen, les méthodes pour accroître les performances sexuelles, les sites pornographiques, les crédits américains à faible taux, etc.

Attention aux offres trop attrayantes. Selon la loi française, toute sollicitation commerciale par e-mail devrait recevoir votre accord préalable. Selon la loi américaine, c'est à vous de vous inscrire sur une sorte de liste rouge des personnes refusant le démarchage commercial par e-mail. Devant la complexité des diverses réglementations nationales et de la quasi impunité des contrevenants hors de l'Union Européenne, mieux vaut respecter quelques règles simples.

Conseil n° 1 : Gardez votre adresse e-mail la plus confidentielle possible

Evitez autant que possible d'indiquer votre adresse sur un site web, à moins qu'il ne soit édité en France et que vous soyez sûrs de sa politique de respect de la vie privée.

Conseil n° 2 : Protégez les adresses de vos contacts

a. Appliquer le conseil précédent aux adresses de vos contacts (proches, collègues, clients...) : n'indiquez jamais leur adresse dans le formulaire d'une page web. De même, évitez les fonctions du genre "*Envoyer cette information à un ami*" ou "*Recommandez ce site à un ami*" sur les sites web.
b. Certains virus (Beagle, MyDoom, par exemple) scannent le disque dur de vos proches ou collègues à la recherche d'adresses e-mail. Envoyer un message à plusieurs personnes en entrant leurs adresses dans la case "A :" (destinataires visibles) revient à faciliter le travail de ces virus. En effet, ces messages à multiples destinataires visibles sont une source très appréciée d'adresses. Aussi est-il recommandé d'utiliser la **case "Cci :" ou "Bcc :"**, c'est-à-dire "copie carbone invisible", qui permet de cacher les adresses des destinataires d'un message lorsque vous écrivez à plusieurs personnes simultanément (lettres d'information, compte-rendu de réunion, etc.). Cela est d'autant plus utile et logique si les personnes ne se connaissent pas. Si vous respectez vos correspondants, appliquez cette consigne le plus souvent possible..

Conseils n° 3 : Ne publiez pas votre adresse e-mail en clair sur votre site web ou votre *blog*

Si vous gérez un site web (un *blog* par exemple), n'indiquez aucune adresse e-mail en clair, ni ne faites de lien "*mailto*:", sous peine de voir toute adresse tôt ou tard envahie de publicité. En effet, des web-robots parcours le web en permanence à la recherche de nouvelles adresses à polluer. Codez votre adresse (ex : jean.dupont AROBASE orange POINT fr) et évitez de créer un lien mailto. Vos visiteurs devront recopier l'adresse pour vous écrire ou utiliser votre formulaire de contact.

Phishing (usurpation de l'identité d'un site web)

Un usurpateur vous envoie un mail aux couleurs d'une banque bien connue par exemple, c'est-à-dire que ce message utilisera frauduleusement le logo de la banque, sa charte graphique, etc., pour vous faire croire qu'il s'agit d'un vrai message issu de la banque imitée. Ce message est envoyé à l'aveuglette à des

milliers de personnes avec l'espoir qu'il attendra des clients de la banque imitée. Dans ce message, vous serez invité(e), pour une raison quelconque, à vous rendre sur une page web pour y saisir vos identifiant et mot de passe, qui d'habitude vous servent à consulter vos comptes dans cette banque, si vous êtes client. C'est là que le piège se referme. Car la page en question, elle aussi, prend l'apparence d'une page web de la banque imitée (logo, couleurs, etc.) mais les informations que vous transmettez *via* cette page web ne vont pas à la banque mais à l'escroc qui pourra ensuite utiliser vos codes pour accéder à votre compte dans la banque imitée !

Conseils :

- Prenez l'habitude de visiter le site de votre banque en tapant vous-même l'adresse qui figure sur le papier à entête de vos relevés de compte par exemple.
- Si vous avez un doute sur un e-mail aux couleurs de votre banque, le plus simple est de ne pas suivre le lien contenu dans le message, mais d'aller dans votre espace client selon la méthode indiquée. (Généralement, les banques étant conscientes de l'existence du *phishing*, elles n'écrivent jamais à leurs clients en leur donnant un lien à suivre pour se connecter à leur site.)

Spywares (logiciels espions)

Beaucoup de logiciels dits gratuits trouvent une contrepartie en envoyant à des sociétés de marketing des informations décrivant votre comportement sur l'Internet (les sites que vous visitez, vos centres d'intérêts, etc.). Ces logiciels qui ne sont donc pas complètement gratuits, puisqu'en échange vous êtes censés participer à des études marketing, sont appelés *spywares* ou logiciels espions. Ces études marketing sont généralement mentionnées dans le contrat d'utilisation du logiciel, mais comme presque personne ne le lit, beaucoup d'utilisateurs voient un peu de leur vie privée dévoilée à des inconnus sans en être conscients...

La partie "espion" de ces logiciels "gratuits" porte un nom différent du logiciel que vous avez téléchargé, on peut citer par exemple : GAIN, Gator, CyDoor, Alexa, Comet Cursor... [liste plus complète]

Parmi les logiciels espions que vous pouvez télécharger, citons : Date Manager, PrecisionTime, VCatch Basic...

Conseils :

- Renseignez-vous bien sur la nature du logiciel que vous vous apprêtez à installer (lisez le contrat d'utilisation, notamment les sections au sujet de la collecte et du traitement des informations personnelles, et faites une recherche sur un moteur de recherche avec comme mots-clés le nom du logiciel et "*spyware*").
- Scannez régulièrement votre PC avec un détecteur de spywares tel que Ad-Aware ou SpyBot .
- Pour les maniaques de la sécurité, installez un pare-feu ou *firewall*. Windows XP, Vista,7 et 8 en intègrent un de série. Il y a ZoneAlarm par exemple. Une des fonctions d'un pare-feu est d'interdire aux programmes qui n'y sont pas autorisés à accéder à l'Internet (pour divulguer vos informations personnelles par exemple).

Canulars (*hoaxes*)

Les messages annonçant des portables gratuits et autres bonnes affaires de ce genre sont des canulars ou "*hoaxes*" en anglais (*hoax* au singulier).

Les appels à solidarité pour des enfants malades sont dans la majorité des cas, soit des bonnes intentions maladroites, soit des canulars. Ces appels ont souvent un effet pervers. Par exemple, un appel à solidarité par e-mail pour une recherche de greffon ou de sang peut conduire à une saturation et une paralysie temporaire des centres médicaux, au détriment des malades.

Certains canulars sont de fausses alertes au virus qui vous conseillent d'effacer un fichier sain de Windows au risque de rendre votre ordinateur instable (***cf.*** **canular au sujet du fichier "jdbgm.exe" de Windows**).

Evitez de faire circuler un message qu'on vous demande de transmettre à tous vos amis. Vous ne ferez qu'encombrer le réseau Internet et les boîtes e-mail, et risquez une augmentation du lot quotidien de ***spam*** que vos amis et vous-même recevez. A force d'être transmis, les messages renferment parfois des dizaines d'adresses e-mail de personnes qui voudraient probablement les garder confidentielles ! Certains virus adorent ce genre de messages remplis d'adresses à exploiter...

Les vers

Un ver (ou worm) est un type de virus particulier. Concrètement, il s'agit de programmes capables de se répliquer à travers les terminaux connectés à un réseau, puis d'exécuter certaines actions pouvant porter atteinte à l'intégrité des systèmes d'exploitation.

Les chevaux de Troie

Un cheval de Troie (ou trojan) est un programme qui, introduit dans une séquence d'instructions normales, prend l'apparence d'un programme valide. Mais il contient en réalité une fonction illicite cachée, grâce à laquelle les mécanismes de sécurité du système informatique sont contournés, ce qui permet la pénétration par effraction dans des fichiers pour les consulter, les modifier ou les détruire. A la différence d'un ver, le cheval de Troie ne se réplique pas : il peut demeurer inoffensif, à l'intérieur d'un jeu ou d'un utilitaire, jusqu'à la date programmée de son entrée en action.

Les Keyloggers:

Un keylogger est un logiciel qui enregistre les frappes au clavier pour voler, par exemple, un mot de passe.

Les Dialers (peu usité car très bas débit avec emploi d'un modem)

Les dialers sont des programmes qui composent un numéro pour connecter votre ordinateur à Internet. Il peut être sans danger et légitime si c'est celui de votre fournisseur d'accès par exemple. Toutefois, certains dialers sont malveillants et peuvent parfois s'installer à votre insu sur votre machine et composer un numéro très coûteux.

Les Rootkits

Un rootkit est un « *kit* » pour devenir "*root*"(administrateur) d'une machine.C'est un code malicieux vraiment complexe qui se greffe sur une machine, et parfois le noyau même du système d'exploitation. Il est ainsi capable de prendre le contrôle total d'un PC sans laisser de trace. Sa détection est difficile, parfois même impossible tant que le système fonctionne. Autrement dit, c'est une série de programmes qui permettent au pirate de s'installer sur une machine (déjà infecté ou exploitant une faille de sécurité) et d'empêcher sa détection. Une fois en place, le rootkit est véritablement le maître du système. À ce titre tous les programmes, y compris les antivirus et anti-spywares, doivent passer par lui avant de faire quoi que ce soit. Ils ne peuvent donc se fier à aucune information collectée sur le système. La croissance des rootkit est favorisée par le fait que la majorité des utilisateurs de système d'exploitation Windows travaille sous les droits d'un administrateur, ce qui facilite grandement l'installation de rootkit dans les ordinateurs.

Infos utiles sur le site d'Orange:

http://assistance.orange.fr/virus-ver-cheval-de-troie-les-differencier-878.php