PETIT GUIDE ELEMENTAIRE DES VIRUS

Par CNET.COM, traduit de l'anglais par VDN.

Qu'est-ce qu'un virus ?

En 1983, le chercheur Fred Cohen définissait un virus informatique ainsi «un programme qui peut " contaminer " un autre programme en le modifiant pour inclure...une copie de lui-même.» En d'autres mots, tous les virus se reproduisent d'eux-mêmes. Pour bien jouer le jeu, la plupart des virus tentent d'échapper aux détections, soit en utilisant des méthodes d'encryptage ou en effectuant de légères mutations chaque fois qu'ils se reproduisent.

Le virus que vous devez craindre fait cependant beaucoup plus que se reproduire. Environ 5 pour-cent des virus ont une charge utile, c'est à dire un ensemble d'instructions conçu pour perturber le cours normal du traitement informatique. La charge utile peut déclencher n'importe quoi, d'un message clignotant inoffensif jusqu'à la réécriture complète de la table d'allocation des fichiers, ce qui implique que vous perdez toutes les données de votre disque dur. Les virus utilisent souvent l'horloge interne de votre ordinateur pour déclencher la charge utile à une date particulière, les vendredis 13 et les anniversaires célèbres sont populaires.

Des programmeurs malveillants cachent quelquefois des instructions destructrices dans ce qui étaient auparavant des logiciels normaux. Par exemple, la disquette «AIDS Information diskette» (disquette d'information sur le Sida) soutirait de l'argent aux utilisateurs d'ordinateurs en faisant un encryptage du disque dur et en les forçant à payer des droits d'inscription pour récupérer leurs données. Ces mauvaises blagues peuvent être extrêmement dommageables, cependant ce sont des Chevaux de Troie (Trojan Horse) plutôt que des virus, ils ne se reproduisent pas nécessairement et ne se répandent pas d'un ordinateur à l'autre. (Bien sûr, il est possible qu'un virus reproducteur fasse partie d'un Cheval de Troie).

Comment les virus se sont-ils développés ?

Au commencement, il y avait les vers.

Les premiers ordinateurs ne pouvaient exécuter qu'une procédure à la fois. Mais lorsque les ingénieurs apprirent comment exécuter des programmes simultanément, les procédures outrepassaient quelques fois leurs frontières et endommageaient les données ailleurs dans le système. Ces dommages apparaissaient à des endroits aléatoires dans la mémoire, ce qui rappelaient aux ingénieurs le bois mangé par des vers. Ce processus était connu sous le nom

«wormholes» (trous de vers) et les bogues qui les créaient, les «worms» (vers). À la longue les vers se sont répandus dans les ordinateurs d'un même réseau. Ces vers furent nommés les vers Xerox, ils ont créé un précédent dans l'industrie informatique.

Début 1960 - Les programmeurs imitent les vers dans les laboratoires de recherche, créant des assembleurs qui se battent les uns contre les autres à l'intérieur d'environnements contrôlés. (Ces «batailles de noyaux» ont encore lieu de nos jours).

1981 - Plusieurs virus de l'Apple II sont retrouvés dans la «nature» (à l'extérieur des laboratoires de recherche). Conçus au départ comme une expérience inoffensive, les virus interrompaient les programmes spontanément.

1983 - Le terme «virus informatique» est défini officiellement pour la première fois.

1986 - Le premier virus commun de l'IBM PC, «Brain», est découvert dans la nature. Il était relativement inoffensif, mais furtif et difficile à détecter.

1988 - Le 3 mars, certains utilisateurs de Macintosh voient apparaître un «message de paix» lors du démarrage de leur ordinateur. Ce message provenait d'un virus créé pour en faire un exploit publicitaire par un rédacteur du magazine MacMag. Ce fut également l'année où les logiciels antivirus sont devenus populaires, et l'année du premier canular de virus (le virus du modem 2400 baud).

1989 - Une compagnie du nom de PC Cyborg expédia 10,000 copies d'une disquette d'information sur le Sida (AIDS Information diskette). La plupart des gens n'avaient pas lu la licence d'utilisation qui portait l'avertissement «N'utilisez pas ce logiciel si vous n'avez pas l'intention de le payer. » Après 90 accès au logiciel, le disque dur des utilisateurs est bloqué par un encryptage, une facture est affichée demandant un paiement pour obtenir la clé de décryptage. Cette disquette était un Cheval de Troie, pas un virus, mais elle a servi d'exemple aux histoires d'horreur maintenant associées aux virus.

1992 - Les chercheurs découvrent un nouveau virus programmé pour être déclenché le jour de la naissance de Michel-Ange, le 6 mars. Les média ont fait courir des histoires sur cette menace et les ventes de logiciels antivirus sont montées en flèche. Cependant, moins de vingt milles ordinateurs furent affectés (certains spécialistes en virologie croient que ce nombre est encore plus bas).

1995 - Les macros virus font leur apparition. Quoique la majorité ne soient pas mortels, les macros virus contaminent les applications populaires de Bureautique et peuvent voyager d'une plate-forme à l'autre, se répandant ainsi très rapidement.

1996 - Des millions de cinéphiles ont regardé Jeff Goldblum sauver la Terre en téléchargeant un virus informatique dans le vaisseau mère extraterrestre du film «Independance Day». Plus tard cet été là, la peur du virus Hare rappela celle du virus Michel-Ange, mais avec moins de fracas et encore moins de dommages.

Comment les virus se répandent-ils ?

La majorité des virus se classent dans trois catégories, selon la manière dont ils se répandent :

Les virus du secteur d'amorçage - ces virus s'attachent aux disquettes, puis se copie eux-mêmes sur le secteur d'amorçage (Boot Sector) de votre disque dur lorsque vous démarrez ou redémarrez votre ordinateur. (Le secteur d'amorçage renferme les instructions que votre ordinateur exécute au démarrage). Vous ne pouvez obtenir un virus de secteur d'amorçage qu'à partir d'une disquette contaminée, vous ne pouvez pas l'obtenir par le partage de fichiers ou en exécutant des programmes. Puisque la plupart des ordinateurs d'aujourd'hui n'ont pas besoin d'une disquette d'amorçage pour démarrer, ces virus sont devenus de moins en moins habituels.

Les virus d'applications - aussi connus sous le nom de virus traditionnels de fichiers, ces démons s'attachent aux fichiers exécutables. Alors que la plupart s'accrochent aux fichiers EXE et COM, ils peuvent contaminer également tous les fichiers que votre ordinateur exécute lorsqu'il lance une application (incluant les fichiers SYS, DLL, BIN et plusieurs autres). Lorsque vous lancez une application contenant un virus, celui-ci se loge dans la mémoire de votre ordinateur. Dès lors, le virus peut contaminer tous les autres programmes qui sont exécutés. Les macros virus sont, techniquement parlant, une variation des virus d'applications.

Les macros virus - ces virus affectent les fichiers modèles utilisés pour créer des documents. Une fois le modèle contaminé, chaque document ouvert par l'application est altéré. Par ce qu'ils contaminent les applications de Bureautique couramment utilisées et qu'ils peuvent voyager d'une plate-forme à l'autre, les macros virus sont devenus récemment très répandus.

Voici ce qui est important à retenir : les virus n'entrent en fonction que si vous les exécutez, soit en exécutant une application qu'ils ont contaminées, ou en démarrant votre ordinateur en utilisant une disquette contaminée. Cela peut paraître évident, mais la plupart des canulars de virus effraient les gens qui n'ont pas compris ce principe de base.

Canulars communs

Vous venez tout juste de recevoir un message urgent d'un ami: il y a un nouveau virus dans les parages, et il est vraiment vilain. Si vous lisez du courrier électronique ou cliquez sur un lien, le virus effacera automatiquement votre disque dur, videra votre compte en banque, et expédiera des messages obscènes à votre patron. Étant un internaute consciencieux, vous passez le mot à vos amis et au département d'informatique de votre travail.

Quelques minutes plus tard, vos amis sont sans pitié: «Je ne peux pas croire que tu es tombé dans le panneau, ce canular existe depuis 1988!» Les gens du département d'informatique, s'ils se donnent la peine, vous enverront un message laconique pointant sur une FAQ (Frequently Asked Question, Foire Aux Questions) de virus sur le net.

Alors, une fois pour toutes, les avertissements de virus suivants sont tous faux:

Good Times (Bon temps) - La père de tous les canulars de virus, celui-là a été dans les parages depuis tellement longtemps (depuis 1984) et s'est répandu tellement loin, qu'il a même inspiré une parodie hilarante. Un des messages Good Times revendique que c'est le FCC (Federal Communications Commission) qui a émis l'avertissement original. Devinez quoi ? Le FCC n'a rien à voir avec les virus, et n'a jamais émis d'avertissement au sujet d'un virus.

Penpal Greetings (Salutations d'un correspondant) - Probablement dérivé du canular Good Times, ce «message d'avertissement» prétend qu'un courrier électronique ayant comme sujet Penpal Greetings est un virus. Le virus est censé, pendant que vous lisez le message, contaminer votre secteur d'amorçage, effacer votre disque dur, se copier lui-même, et s'expédier à toutes les adresses qu'il trouve dans votre boîte aux lettres. Ce message est un canular: aucun virus ne peut s'exécuter uniquement par ce que vous lisez un message; et pour fonctionner, le virus devrait connaître le fonctionnement interne de tous les logiciels de courrier électronique sur le marché. Impossible.

Make Money Fast (Faites de l'argent rapidement) - Tous ceux qui ont visité les «newsgroups» ont probablement rencontré des messages hors de propos avec l'entête «Make Money Fast». Quelqu'un a cru qu'en inventant un avertissement au sujet d'un virus «Make Money Fast», que cela laverait les newsgroups de ces messages agaçants. L'avertissement a semé la confusion chez les internautes qui n'étaient pas familiers avec les newsgroups, et ces messages frauduleux sont toujours omniprésents.

Deeyenda - Ils existent plusieurs versions de cet avertissement. La plupart mentionnent le FCC, et la plupart prétendent que le virus inspectera votre disque dur à la recherche d'information sur des cartes de crédits (jusqu'à maintenant, aucun virus connu ne peut faire cela).

Irina - Cet avertissement à propos du virus Irina fut émis dans le but de créer un exploit publicitaire pour un livre interactif dont le titre est Irina. Le message est censé avoir été créé par un certain professeur Edward Prideaux. Prideaux est un personnage du livre.

NaughtyRobot (Méchant robot) - Conformément à l'avertissement, ce robot peut récupérer les informations personnelles d'un concepteur de sites Web en passant par une brèche dans la sécurité du protocole HTTP. Cette brèche n'existe pas, le message est embrouillé et utilise une terminologie insensée. NaughtyRobot est un élégant canular pour cette unique raison: il modifie l'entête «From» (De) du courrier électronique pour que le message paraisse provenir de l'ordinateur du concepteur.

death69 - Cet avertissement prétend avoir été écrit par des techniciens de la compagnie Symantec. Symantec nie complètement être l'auteur d'un tel message.

Trois moyens par lesquels vous ne pouvez pas attraper un virus.

Les ingénieurs sont infiniment créatifs et fabriquent constamment de nouveaux virus. Cependant, les canulars, les avertissements, et les histoires d'horreur sont presque aussi habituels que les vrais virus. Alors la prochaine fois que vous entendrez une histoire de virus, faites preuve de retenue avant de céder à la panique. Vous ne pouvez pas obtenir de virus par les méthodes suivantes:

Lire un courrier électronique - Le simple fait de lire le texte d'un courrier électronique est totalement inoffensif. Mais si le message possède des documents annexés («attachments» en anglais), vous devriez jouer de prudence avant de les ouvrir. En fait, une rumeur veut qu'un tout nouveau virus tire avantage du logiciel Microsoft Mail pour se copier et s'expédier lui-même à toutes les adresse de votre boîte aux lettres. Si vous êtes familiers avec les canulars de virus, celui-ci est étrangement soupçonneux. Voilà pourquoi il n'en est rien: le virus est logé dans un document annexé plutôt que dans le message lui-même. N'exécutez pas les documents annexés inconnus avant de les avoir inspectés, et ne configurez pas votre logiciel de courrier électronique pour lancer automatiquement Microsoft Word lorsque vous recevez un document annexé.

Lire une page Web - Oui, il y a une brèche dans la sécurité du navigateur Internet Explorer: si vous désactivez les fonctions de sécurité du navigateur, des contrôles ActiveX malveillants peuvent réarranger les fichiers de votre disque dur, chercher des informations secrètes et ainsi de suite. Des problèmes similaires sont théoriquement possibles avec Java. Mais ces brèches ne sont pas des virus. Pour être contaminé par un virus logé dans une page Web, vous devez télécharger un programme et l'exécuter, et les navigateurs Netscape et Internet Explorer vous donnent amplement d'avertissements avant de vous laisser faire. Si vous êtes paranoïaque, assurez-vous d'inspecter tous les fichiers que vous téléchargez.

Télécharger un fichier - Répétons-le, vous devez exécuter un programme pour contracter un virus. Alors, si vous téléchargez un document, vous pouvez attraper un virus en ouvrant votre traitement de texte pour le lire (techniquement parlant, les documents sont des données et ne peuvent être contaminés, c'est une macro ou un modèle de document qui sont contaminés). Ou si vous téléchargez un logiciel soupçonneux, vous pouvez contracter un virus en essayant de l'installer. Par exemple, il existe un programme appelé AOL4Free qui vous permettra d'utiliser les services d'America Online sans payer (l'étudiant qui a créé ce programme a récemment plaidé coupable d'escroquerie envers AOL). Il existe également un Cheval de Troie appelé AOL4Free qui, si exécuté, détruit tous les fichiers de votre disque dur. Le téléchargement du fichier est en soi inoffensif, aussi longtemps que vous ne l'exécutez pas! Pour être en sécurité, inspectez chaque fichier que vous téléchargez avant d'en faire quoi que ce soit.

Erreurs, mauvais fonctionnement et bogues.

Le seul fait que votre ordinateur se comporte bizarrement ne signifie pas que vous ayez attrapé un virus. Lorsque ça ne tourne pas rond, vous devez diagnostiquer le problème et le réparer; autrement, la même chose pourrait se reproduire indéfiniment.

Bogues - L'informatique moderne est très compliquée, et les logiciels n'interagissent pas toujours correctement avec votre système d'exploitation. Cela est encore plus vrai si vous utilisez beaucoup de versions bêta de logiciels. Si votre version bêta de logiciel ne fonctionne pas correctement, les chances sont grandes qu'il est été mal conçu ou mis sur le marché trop rapidement. Ou peut être le logiciel est trop avancé pour votre ordinateur. Avant de jeter le blâme sur le malheureux vendeur de logiciels, assurez-vous d'avoir suffisamment de mémoire, que vous utilisez la bonne carte de son, le bon système d'exploitation (et oui, ça peut arriver), et ainsi de suite.

Mauvais fonctionnement - La quincaillerie et les pilotes de dispositifs ne sont pas parfaits. Si votre souris refuse soudainement d'opérer, que votre système plante, ou que des messages d'erreurs étranges apparaissent sur votre écran, ne signifient pas que vous ayez attrapé un virus. Probablement que votre quincaillerie se fait vieille, que les pilotes de dispositifs ne fonctionnent pas correctement, ou que vous n'ayez pas suffisamment de mémoire pour tout ce que voulez faire en même temps.

Fausses alarmes - Horribles mais vraies : les logiciels antivirus peuvent générer de fausses alarmes. Le plus efficace des détecteurs de virus inspecte les fichiers exécutables et les autres fichiers du système pour y détecter des comportements ou motifs anormaux, tels que les changements de taille de fichiers. Certains de ces comportements se produisent pour des raisons valables. Alors si votre logiciel vous indique qu'il n'y a qu'un seul fichier contaminé ou qu'il ne nomme pas le virus, il s'agit probablement d'une fausse alarme. Alors que plusieurs milliers de virus existent, seulement 500 d'entre eux se retrouvent dans la nature. La liste du CIAC n'est pas très exhaustive et n'est pas mise à jour assez fréquemment, mais elle couvre la plupart des virus communs. Si votre logiciel détecte un virus qui n'est pas sur cette liste, les chances sont grandes pour que votre logiciel se trompe.

La prévention en 6 étapes simples.

Même si plusieurs milliers de virus informatiques sont connus des chercheurs, la vaste majorité sont enfermés bien loin dans des laboratoires informatiques. Des 500 virus qui existent «dans la nature», la plupart sont relativement inoffensifs, ils peuvent soutirer une petite quantité de mémoire, mais ils ne détruiront probablement pas tous les fichiers de votre disque dur.

Cependant, vous ne devez prendre aucune chance. Suivez ces étapes simples et vous serez sur la bonne voie de l'informatique sans souci:

1. Procurez-vous un logiciel antivirus - Le logiciel antivirus parfait n'existe pas, et les

fausses alarmes peuvent être aussi dérangeantes que les virus eux-mêmes. Dans un monde informatique aujourd'hui hyper branché, aucun ordinateur ne devrait être sans logiciel antivirus. Assurez-vous de le mettre à jour fréquemment, des nouveaux virus apparaissent tous les jours.

2. Inspectez tous les disques - En général, vous devriez être très prudent avant d'insérer une disquette provenant de sources inconnues dans votre ordinateur, surtout si la disquette a été partagée entre plusieurs personnes. Quelques fois vous n'aurez pas le choix. Dans ces situations, la seconde chose que vous devriez faire (après avoir inséré la disquette dans votre lecteur) c'est de l'inspecter avec votre logiciel antivirus. Inspectez tous les fichiers de la disquette, pas seulement les fichiers d'application. Faites cela également pour les logiciels achetés et emballés. Lorsque vous remettez une disquette à quelqu'un d'autre, protégez-la en écriture. De cette manière, le virus situé sur l'ordinateur de l'autre personne ne contaminera pas votre disquette (à moins que cette personne retire la protection en écriture pour effectuer des changements, ce sera alors la responsabilité de cette personne). Les CD-ROM sont moins à risques, mais inspectez-les la première fois que vous les utilisez. Le virus «Concept» fut trouvé sur les CD-ROM du test de la compatibilité pour Windows 95 et dans celui sur les outils de support Windows 95 pour Windows NT.

3. Téléchargez prudemment - Plusieurs utilisateurs d'ordinateur croient que la meilleure source de contamination est le téléchargement de fichiers. Rien n'est plus loin de la vérité: la vaste majorité des virus voyagent par l'entremise des disquettes partagées ou les fichiers d'un réseau. Vous ne pourrez jamais être assez prudent, surtout si vous utilisez des logiciels «clandestins» comme AOL4Free (qui est véritablement un Cheval de Troie). Par prudence, téléchargez tous les fichiers dans un répertoire spécial sur votre disque dur, puis assurez-vous de tous les inspecter avant de les utiliser.

4. Inspectez les documents annexés aux courriers électroniques avant de les lire - Alors qu'il est impossible de contracter un virus simplement en lisant un message, c'est possible par l'entremise d'un document annexé au message. Certains logiciels de courrier électronique vont ouvrir automatiquement certains documents annexés en utilisant l'application appropriée. C'est bien et cela rend la lecture des documents annexés plus efficace, mais peut devenir une source potentielle de cauchemars si des virus s'y cachent. Désactivez cette fonction de votre logiciel de courrier électronique, et inspectez chaque document annexé que vous recevez avant de les consulter.

5. Sauvegardez les fichiers partagés en formats RTF ou ASCII - Si vous désirez partager des données sur un serveur réseau, et que vous désirez conserver votre environnement à l'abri des virus, sauvegardez tous vos fichiers en formats RTF et ASCII. Aucun de ces formats ne conserve des macros ou des informations de styles, cela vous protégera des macros virus.

6. Faites une copie de sécurité complète - Faites des copies de sécurités de vos documents de travail et des fichiers de configuration du système régulièrement. Conservez ces copies de sécurité dans un endroit sécuritaire, ailleurs que sur votre disque dur. Ainsi, si votre

système est contaminé par un virus, vous pourrez compter sur vos copies de sécurité.

Comment se débarrasser d'un virus ?

La plupart des logiciels antivirus d'aujourd'hui inspectent la mémoire de votre ordinateur aussitôt le démarrage amorcé, et le logiciel devrait vous prévenir aussitôt que vous tentez d'ouvrir un document contaminé. A ce stade, laissez le logiciel nettoyer le fichier contaminé, ou détruisez le fichier si nécessaire (heureusement, vous avez une copie de sécurité).

Néanmoins, certains virus réussissent parfois à percer vos défenses. Peut-être quelqu'un a-t-il utilisé votre ordinateur à l'heure du lunch ou peut-être que votre logiciel antivirus est désuet ? Alors que faire ?

1. Restez calme - Vous pouvez pleurer, crier, supplier votre patron d'allonger la date limite de remise de votre travail, mais quoi que vous fassiez, ne paniquez pas. Le virus n'a probablement pas détruit votre ordinateur, le jeter par la fenêtre le fera sûrement.

2. Redémarrez votre ordinateur proprement - Fermez votre ordinateur et redémarrez-le à partir d'une disquette d'amorçage protégée en écriture.

3. Cherchez et réparez les fichiers contaminés - Utilisez votre logiciel antivirus pour trouver et réparer les fichiers contaminés. Si les dommages sont trop grands pour que le logiciel puisse les réparer, remplacez les fichiers contaminés par ceux de votre copie de sécurité.

4. Vérifiez de nouveau - Inspectez tout votre système avec votre logiciel antivirus une ou plusieurs fois. Normalement le logiciel antivirus devrait avoir supprimé le virus.

5. Si rien n'y fait - Contactez votre manufacturier de PC pour obtenir de l'aide.