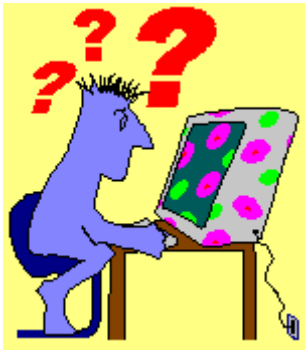
Le viroax, véritable virus du pauvre

Par Emmanuel JUD (15/05/02)



L'année 2002 a vu se confirmer l'existence d'une nouvelle cybermenace : le viroax. Comme un virus, il peut supprimer des fichiers et se transmettre à tous vos contacts. Comme un hoax, il ne nécessite aucune connaissance en programmation et utilise la crédulité de l'internaute pour arriver à ses fins. Les canulars du Net étaient jusqu'à présent appelés "virus du pauvre" quelque peu abusivement. Avec les viroax, cette expression prend désormais tout son sens.

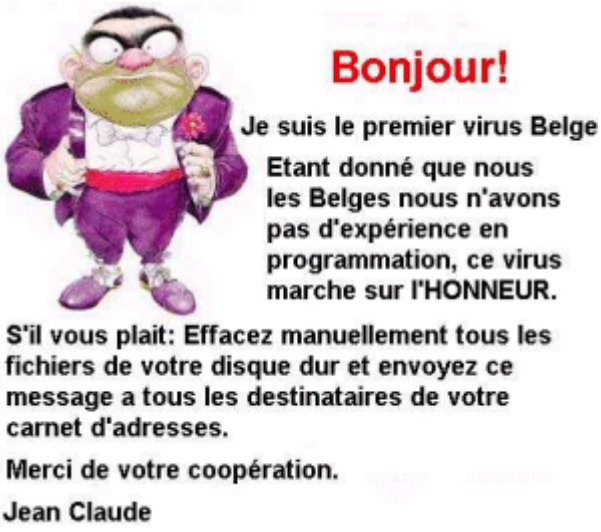
Qu'est-ce qu'un viroax?

Un viroax - contraction de "virus et "hoax" - est un simple courrier électronique qui sous un faux prétexte tente de persuader l'internaute d'exécuter une action dangereuse pour l'intégrité ou la sécurité de son système, puis de l'inciter à avertir tous ses contacts pour leur recommander de faire de même.

Généralement, il s'agit de supprimer un fichier sain (utilitaire du système d'exploitation, composant d'une application connue, etc.) au motif qu'il serait en réalité un virus. Les internautes convaincus de la menace exécutent alors à la lettre la procédure préconisée, puis font suivre une copie du message à leurs correspondants en pensant leur rendre service.

Un peu d'histoire

L'histoire du viroax commence comme un gag : celui du virus belge, encore appelé virus sur l'honneur. Ce message humoristique circule toujours aujourd'hui, sous forme de texte ou d'image :



Le véritable premier viroax est apparu en avril 2001 au Brésil et visait le fichier Sulfnbk.exe. Traduit dans des langues aussi variées que l'anglais, le danois, le français, le chinois ou l'indonésien, il a connu depuis une propagation mondiale. Voici la première version intégrale française que nous ayons reçue, datée du 31 mai 2001 :

> Salut tout le monde, on m'a forwardé ce message aujourd'hui, alors ATTENTION
>
> Certains clients et amis de l'entreprise ont trouvé par hasard un fichier du nom de

> SULFNBK.EXE : c'est un fichier qui est programmé pour s'activer le el 1° Juin 2001. Les systèmes antivirus ne le détectent pas parce qu'il n'est pas encore activé. Mais c'est un parasite, c'est à dire qu'il entre dans votre machine sans être détecté, comme s'il faisait partie d'un courrier.
>
> Faites un clic sur le bouton DEMARRER, choisissez RECHERCHER, puis FICHIERS OU DOSSIER et écrivez le nom du fichier, recherchez-le dans toutes les mémoires. Si vous le trouvez NE L'OUVREZ PAS ! (l'icône est fait de lettres noires peu lisibles qui disent SULF NBK).
>
> Cliquez sur l'icône avec le bouton droit et faites SUPPRIMER. Vous aurez droit aux avertissements habituels de Windows comme quoi effacer un programme risque d'affecter Windows. Ignorez cet avertissement et effacez ce truc. Ensuite, VIDEZ LA CORBEILLE, car il peut aussi s'activer depuis là.
>
> CE N'EST PAS UN GAG !!!
>
> Avertissez les gens à qui vous avez forwardé des messages venant d'on ne sait pas trop où, et qui pourrait les recevoir sur leur PC, le plus vite possible, afin qu'ils puissent éviter que le virus ne s'active le 1er juin. Rappelez-vous, il s'appelle SULFNBK.EXE

Les circonstances de l'apparition du message originel ne sont pas clairement établies, aussi n'est-il pas certain qu'il ait été diffusé avec l'intention de nuire. En effet, à cette même époque le virus Magistr.A se propageait déjà sous divers noms de fichiers joints dont Sulfnbk.exe, donc une personne de bonne foi mais mal informée aurait pu faire un amalgame.

Fonctionnement d'un viroax

Le viroax est un message bien construit, en apparence solidement argumenté mais qui mélange en fait mensonges et vérités dans un langage pseudo-technique. Sa crédibilité ne fait ainsi aucun doute aux yeux d'un internaute non averti ou pressé, d'autant que ce message est transmis par un ami, un collègue ou un client, donc a priori une personne de confiance.

Les viroax exploitent un levier psychologique simple et bien connu : créer une peur, puis apporter immédiatement le remède, afin de favoriser le passage à l'acte. Sauf que la peur n'a aucune raison d'être, et que le remède consiste à exécuter une action hostile à l'intégrité du système.

Afin de mieux comprendre les mécanismes de fonctionnement d'un viroax, voici ci-dessous le découpage commenté d'une autre version du viroax Sulfnbk.exe, conçue cette fois délibérément dans l'intention de nuire :

> J'ai reçu un émail et j'ai appris qu'il contenait un virus. Je l'ai trouvé et l'ai éliminé de mon système.

Envoyé par un proche, sans fichier joint et semblant rédigé spécialement à son attention, le message a tout pour mettre en confiance le destinataire.

En fait, il s'agit simplement de la copie d'un message que son ami ou collègue a lui-même reçu d'un autre de ses correspondants. Tout juste peut-il contenir une mention amicale ajoutée avant de transférer le message, ce qui renforcera néanmoins encore un peu plus sa crédibilité.

> Le programme de détection de virus McAffee & Norton est à jour et pourtant il ne l'a pas détecté.

L'auteur du viroax veut évidemment toucher un maximum de monde. Le concept du "virus indétectable", un classique chez les canulars, permet d'inquiéter et d'impliquer y compris les possesseurs d'antivirus.

La présence des noms d'éditeurs d'antivirus renommés participe indirectement à crédibiliser l'existence du faux virus, et leur prétendue impuissance face à cette menace n'en rend la situation que plus dramatique.

Dans la réalité, les éditeurs d'antivirus sont le plus souvent capables de mettre au point un antidote en quelques minutes à quelques heures après la découverte d'un nouveau virus. Le danger pour l'utilisateur est donc plutôt de ne pas mettre à jour régulièrement son antivirus.

> LA MAUVAISE NOUVELLE: Comme vous vous trouvez dans mon carnet d'adresses, votre ordinateur à probablement le virus car le virus attaque les carnets d'adresse.

La propagation des virus de mail via le carnet d'adresses est un phénomène réel et maintenant bien connu. Il sert ici d'argument pour justifier que le destinataire doit avoir été contaminé, mais le point principal est passé sous silence : le fichier présent sur le disque est-il réellement contaminé ou non?

Seul un antivirus permettrait de le savoir, et probablement de réparer le fichier si vraiment il était infecté. Supprimer un fichier sans vérification est donc la dernière des choses à faire, d'autant qu'en cas de nécessité il existe des antivirus gratuits.

> LA BONNE NOUVELLE: Le virus est facile a éliminer.

Après avoir eu peur, l'internaute a besoin d'être rassuré. Voilà qu'on lui propose une solution, en plus facile à appliquer : de quoi capter toute son attention, même si certains auront encore quelques doutes.

> Apparemment le virus "sommeille" pendant 14 jours, puis il détruit le disque dur.

Afin de mettre encore un peu plus la pression et emporter définitivement la décision de l'internaute, rien de tel que la technique de la date limite rapprochée associée à un péril extrême. Cependant, pour maximiser le caractère incitatif tout en s'assurant que le viroax puisse continuer à circuler indéfiniment, il n'est pas spécifié une date précise mais une durée en jours.

Cet argument devrait faire douter l'internaute, car si le fichier incriminé est réellement un virus et qu'il est présent sur le disque depuis plus de 14 jours, l'ordinateur aurait déjà dû cesser de fonctionner. Par ailleurs, il n'est pas rare de recevoir plusieurs viroax ciblant le même fichier mais comportant une durée de sommeil différente. Cependant, conditionnés par les propos précédents, beaucoup ne prêteront pas attention à ces "détails".

> Voilà ce qu'il faut faire : suivez les instructions, puis si vous avez effectivement le virus, vous devrez envoyer ce e-mail à toutes les personnes se trouvant dans votre carnet d'adresses.
> 1. Allez sur démarrage puis rechercher
> 2. Dans chercher dossier taper: sulfnbk.exe c'est le nom du virus
> 3. Soyez sûr de chercher dans le disque dur (C)
> 4. Taper chercher
> 5. Si votre rechercher trouve le virus, c'est une icône de forme bizarre noire avec le nom sulfnbl.exe ATTENTION : NE PAS OUVRIR!!!
> 6. Supprimer l'icône
> 7. L'envoyer dans la corbeille l'éliminer encore une fois

Pour s'assurer une nouvelle fois de toucher un maximum de monde, la procédure permettant de supprimer le fichier est largement détaillée, et l'internaute est incité à transférer le message à tous ses correspondants.

Cette incitation à faire suivre devrait elle aussi faire douter l'internaute, car elle est la signature de tous les hoax circulant sur Internet. Tout message se terminant ainsi doit être considéré comme hautement suspect.

Autre contradiction notable : la mention "ATTENTION : NE PAS OUVRIR!!!". L'internaute pensera que c'est pour le préserver du virus, alors que pourtant quelques lignes au-dessous il lui est indiqué que le virus n'est pas actif.

Reste que l'effacement du fichier conservé dans la corbeille prive l'utilisateur du moyen de restaurer facilement le fichier inopportunément supprimé. Le message n'a dès lors plus rien d'un canular.

> 8. SI VOUS AVEZ TROUVEZ LE VIRUS DANS VOTRE SYSTÈME. S.V.P. ENVOYER CET ÉMAIL A TOUTES LES PERSONNES QUI SE TROUVENT DANS VOTRE CARNET D'ADRESSES.

La redondance avec le début du paragraphe précédent laisse penser que l'une des deux phrases a probablement été copiée/collée depuis un autre hoax, dans le but d'inciter encore une fois l'internaute à propager le viroax à tous ses contacts. Convaincus d'avoir supprimé un vrai virus, beaucoup le feront, d'où une réaction en chaîne.

Une menace grandissante mais facilement évitable

Si l'on peut avoir des doutes quant au but réel du tout premier message concernant Sulfnbk.exe, celui-ci a été suivi de multiples variantes sans ambiguïté quant à leur intention malveillante. Par ailleurs, d'autres fichiers ont été la cible de viroax : Cleanmgr.exe, immédiatement après Sulfnbk.exe, puis plus récemment Setdebug.exe et Jdbgmgr.exe.

Le viroax est en effet une menace facile à mettre en oeuvre : un copier/coller et quelques secondes suffisent à en créer un nouveau. Ci-dessous ont été mises en gras les parties du viroax ciblant Jdbgmgr.exe identiques ou très semblables à celles des viroax visant Sulfnbk.exe :

> **UN DE MES CORRESPONDANTS A ETE INFECTE PAR UN VIRUS** QUI CIRCULE SUR LE MSN Messenger. **LE NOM DU VIRUS EST** jdbgmgr.exe **L'ICONE EST** UN PETIT OURSON. **IL EST TRANSMIS** AUTOMATIQUEMENT PAR MESSENGER AINSI QUE **PAR LE CARNET D'ADRESSES. LE VIRUS N'EST PAS DETECTE PAR McAFEE OU NORTON ET RESTE EN SOMMEIL PENDANT 14 JOURS AVANT DE S'ATTAQUER AU DISQUE DUR. IL PEUT DETRUIRE TOUT LE SYSTEME. JE VIENS DE LE TROUVER SUR MON DISQUE DUR! !! AGISSEZ DONC TRES VITE POUR L'ELIMINER COMME SUIT:**
>
> **Très simple à faire !**
> **1; Aller à DEMARRER, faire "RECHERCHER"**
> **2. dans la fênetre FICHIERS-DOSSIERS taper le nom du virus: jdbgmgr.exe**
> **3. Assurez vous de faire la recherche sur votre disque dur "C"**
> **4. Appuyer sur "RECHERCHER MAINTENANT"**
> **5. Si vous trouvez le virus L'ICONE EST UN** PETIT OURSON **son nom "**jdbgmgr.exe**" NE L'OUVREZ SURTOUT PAS !!!!!**
> **6.Appuyer sur le bouton droi de la souris pour l'eliminer (aller à la CORBEILLE) vous pouvez aussi l'effacer en appuyant sur SHIFT DELETE afin qu'il ne reste pas dans la corbeille.**
> **7. aller à la CORBEILLE et l'effacer definitivement ou bien vider la corbeille.**
>
> **SI VOUS TROUVEZ LE VIRUS SUR VOTRE DISQUE DUR ENVOYEZ CE MESSAGE A TOUS VOS CORRESPONDANTS FIGURANT SUR VOTRE CARNET D'ADRESSE** CAR JE NE SAIS PAS DEPUIS QUAND IL EST PASSE.

Cette facilité de fabrication, le "succès" de ce genre de messages auprès d'une grande partie des internautes et la nature même du viroax qui rend difficile toute sanction, devraient conduire au développement de cette menace, d'autant qu'elle prend à contre-pied les règles établies.

En effet, de la même manière que la recommandation qui voulait avant 1999 que pour se protéger des virus "il suffisait de ne pas ouvrir les messages envoyés par des inconnus" a eu un effet pervers lors de l'apparition des virus de mail s'envoyant automatiquement à tout le carnet d'adresses, le fait que les hoax aient jusque-là été considérés comme de gentils canulars permet aux plus destructeurs d'entre eux de se répandre d'autant plus facilement.

Comment se protéger des viroax?

En entreprise, les administrateurs peuvent bloquer les messages contenant le nom du fichier visé par un viroax via un firewall ou tout dispositif de filtrage par mots-clés. Cette procédure à l'avantage d'être

simple et radicale, mais elle peut être contournée et conduit au blocage de courriers utiles, comme par exemple nos newsletters Secuser News ou Secuser Alerte.

Dans la mesure du possible, le mieux reste l'information des utilisateurs, d'autant qu'une fois que les mécanismes d'un viroax ont été démontés il devient évident de les identifier et donc de ne plus se laisser piéger. Quatre conseils simples permettent ainsi d'en finir avec les viroax :

- **ne pas faire confiance a priori à l'expéditeur d'un message**. N'importe qui peut être abusé par une fausse alerte, qu'il soit chef d'entreprise, secrétaire ou ministre. Le nom, la fonction ou l'entreprise de l'expéditeur n'est pas une garantie en soit. Le cas s'est même déjà produit d'un commercial chez un célèbre éditeur d'antivirus ayant transféré à ses revendeurs une alerte qui était en réalité un canular ;
- **ne jamais transférer un message douteux**. La quasi totalité des alertes qui circulent sur le Net sont des canulars : le doute profitera donc toujours à l'auteur du viroax, mais c'est votre responsabilité (morale) et votre crédibilité qui seront engagées si vous poussez un ami ou un client à effacer des fichiers sains ou si vous diffusez de fausses informations. Il faut systématiquement valider une alerte auprès d'une source sûre avant de la faire suivre à ses connaissances ;
- **supprimer un fichier infecté est le plus souvent inutile**. En cas de doute sur un fichier, analysez-le avec un antivirus à jour. S'il est infecté, l'antivirus pourra probablement le réparer. Dans le cas contraire, il vous suggérera de le supprimer, mais cette suppression ne doit intervenir qu'en dernier recours. Le fichier concerné est probablement nécessaire au bon fonctionnement de votre ordinateur ou d'une application ;
- **rester informé de l'apparition des nouveaux virus et viroax**. Secuser.com propose ce service gratuitement sur son site, par abonnement gratuit à la lettre hebdomadaire Secuser News ou encore en temps réel via la liste Secuser Alerte. Etre prévenu de l'apparition des principaux nouveaux virus et viroax permet de savoir au plus tôt comment bien réagir.

Cette prévention anti-viroax est d'ailleurs une excellente occasion pour sensibiliser les utilisateurs à l'existence des hoax, ces messages concernant de faux virus, de fausses disparitions d'enfants, de fausses bonnes astuces, etc. qui polluent régulièrement les boîtes aux lettres