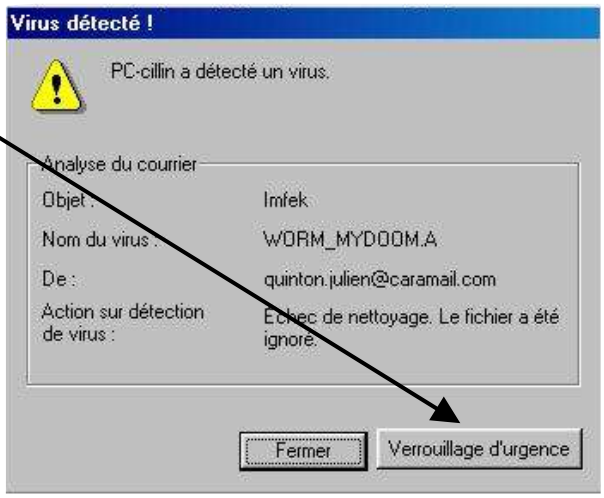
EXEMPLE DE TRAVAIL SUR UN VIRUS

Partons du principe que votre poste informatique est pourvu d'un antivirus disposant des mises à jour les plus récentes.
Prenons le virus / ver[1] MYDOOM A qui fait actuellement des ravages dans toutes les boîtes aux lettres électroniques.

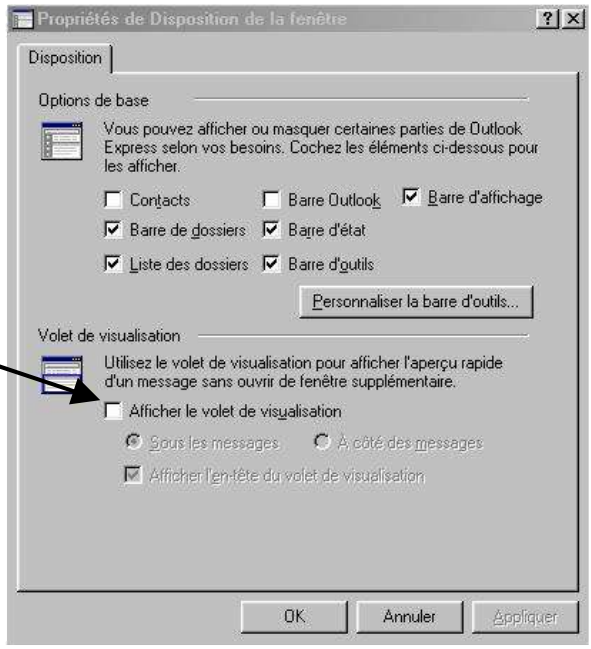
Il est détecté par l'anti-virus ; une fenêtre d'alerte s'affiche, dans laquelle le nom du virus et le mail de l'expéditeur apparaissent.
L'anti-virus ne pouvant pas agir, cliquer ici
Ou, selon le cas, mettre en quarantaine pour ensuite aller vider la quarantaine.
Supprimer ensuite le mail infecté.



Attention : selon l'affichage choisi dans Outlook Express, un mail s'ouvre automatiquement en cliquant dessus (ce qui est nécessaire pour la supprimer !). Ce n'est pas grave si le virus, comme ici (et dans la plupart des cas) est contenu dans un fichier attaché, que l'on se gardera bien d'ouvrir.

Mais certains virus peuvent se propager à la simple ouverture du mail, sans aide de pièce jointe. Dans ce cas, comment faire ?

Configurer son affichage dans Outlook afin de ne pas faire apparaître la fenêtre en bas à droite dans laquelle un mail « cliqué » dans la fenêtre supérieure s'ouvre automatiquement.
Pour cela, cliquer dans le menu Affichage puis sur Disposition. Apparaît alors cette fenêtre : décocher « Afficher le volet de visualisation », puis cliquer sur Appliquer et OK.
A partir de cette nouvelle configuration, on pourra cliquer sur l'annonce du mail et le supprimer (croix rouge) sans l'ouvrir ; en contrepartie, il faudra double-cliquer sur l'annonce d'un mail que l'on veut vraiment ouvrir. C'est le prix d'une certaine sécurité …

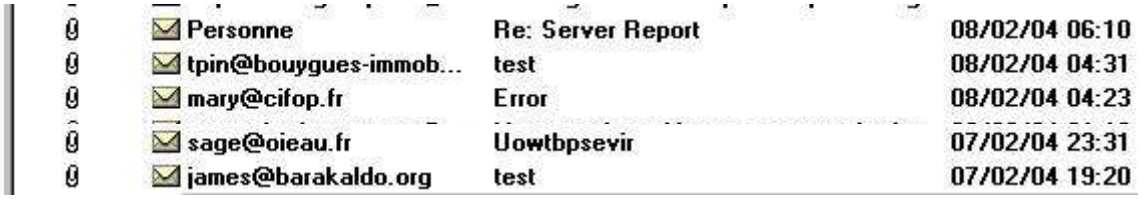


Autres remarques :

- Les mails infectés, comme dit plus haut, contiennent le virus le plus souvent dans un fichier joint ayant pour extension **.doc, .com, .exe, .pif., .lnk, .bat**

[1] Programme auto-répliquant se liant à des organismes pré-existants.

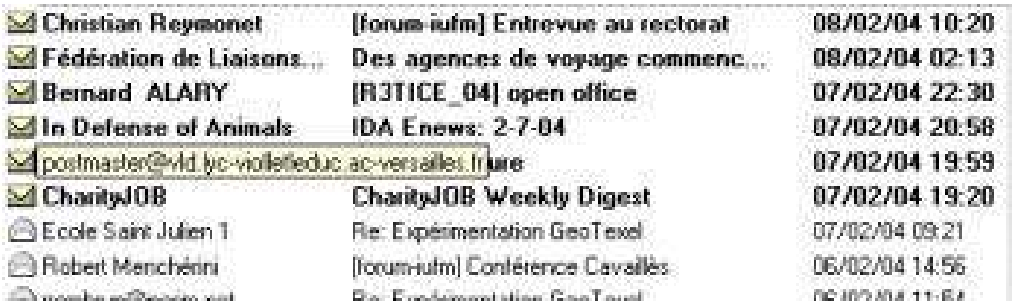
- Evitez donc d'ouvrir de tels fichiers joints sauf si vous savez expressément qu'ils vont arriver, car ils peuvent venir de gens que vous connaissez et dont le carnet d'adresses a été infecté à leur insu.
- Un fichier infecté a souvent les caractéristiques suivantes :



	Personne	Re: Server Report	08/02/04 06:10
	tpin@bouygues-immob...	test	08/02/04 04:31
	mary@cifop.fr	Error	08/02/04 04:23
	sage@oieau.fr	Uowtbpsevir	07/02/04 23:31
	james@barakaldo.org	test	07/02/04 19:20

Nom d'expéditeur bizarre, extensions également « originales » après l'arobase (pas toujours !), objet en anglais (mais avec « test », cela n'est pas évident !), et surtout fichier attaché signalé par le trombone.

- Attention aux mails surprenants, comme ici :



Christian Reymonet	[forum-iufm] Entrevue au rectorat	08/02/04 10:20
Fédération de Liaisons...	Des agences de voyage commenc...	08/02/04 02:13
Bernard ALARY	[R3TICE_04] open office	07/02/04 22:30
In Defense of Animals	IDA Enews: 2-7-04	07/02/04 20:58
postmaster@vld.lyc-viollefeduc.ac-versailles.fr	ure	07/02/04 19:59
CharityJOB	CharityJOB Weekly Digest	07/02/04 19:20
Ecole Saint Julien 1	Re: Expérimentation GeoTexel	07/02/04 09:21
Robert Menchérini	[forum-iufm] Conférence Cavaillès	06/02/04 14:56

un mail sans fichier joint, mais indiquant une « failure » (échec de réception) d'un mail que l'on aurait donc envoyé … sauf qu'aucun mail n'a été adressé au lycée Viollet le Duc dans l'académie de Versailles. Dans ce cas, supprimer le mail sans l'ouvrir.

Pour en savoir plus sur un virus

Connaissant le nom du virus, on peut aller chercher des infos à son sujet sur le site de Hoaxbuster à la page consacrée aux virus http://www.hoaxbuster.com/vraisvirus/info.php

On y repère (premier de la liste !) notre fameux ver. En cliquant sur son nom, on accède au site de Trend, fabricant d'antivirus (PC-Cillin). Paraissent alors des informations très complètes (malheureusement en anglais !) sur la dangerosité du virus et de sa propagation, et on accède aux méthodes capables de l'éradiquer.

Pour plus d'infos sur les virus, quelques autres sites :

Sur le site du CNRS : http://www.cnrs.fr/Infosecu/Virus.html
CRISI, Université de Caen : http://www.unicaen.fr/crisi/legislation/legis_virus.htm
Club de la sécurité des services Informatiques Français (CLUSIF) : https://www.clusif.asso.fr/index.asp
Infos sur les virus et les hoax : www.commentcamarche.net/virus/hoax.php3
Le site des hoax en français (rappel) : http://www.hoaxbuster.com/
Son équivalent américain : Urbanlegends : http://urbanlegends.about.com/