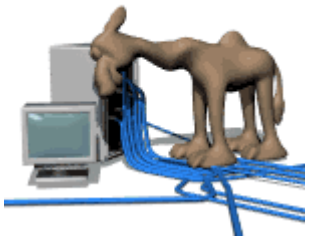


DOSSIER VIRUS

OBJECTIFS DU DOSSIER :

- Dans le dossier suivant, nous vous proposons de découvrir les virus. Vous découvrirez ce que sont les virus, comment les détecter, comment s'en prémunir et comment les détruire.

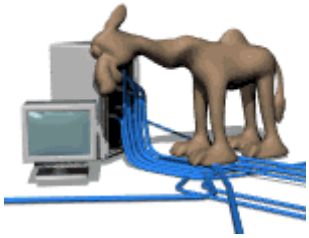
DEMARCHE DE TRAVAIL :

- Consultez rapidement le dossier avant de commencer
- Complétez le dossier en suivant les indications du document
- Réalisez les exercices correspondant au dossier multimédia

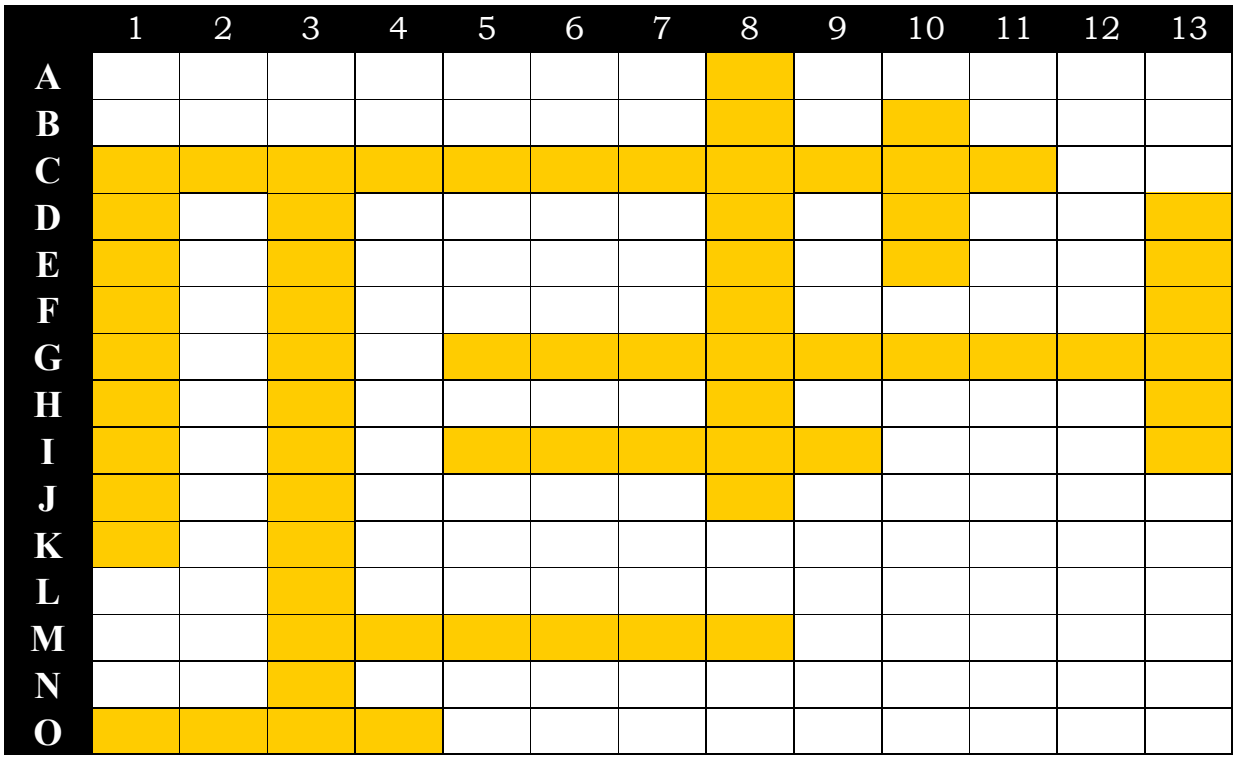
BON COURAGE !

☞ ***Consultez le dossier VIRUS multimédia en n'oubliant pas de faire les exercices associés…***

☞ ***Lorsque vous vous sentirez prêt, complétez le dossier papier…***



☞ ***A l'aide du dossier multimédia et du dossier papier, complétez le mot croisé suivant…***



HORIZONTAL

C : Je suis une propriété permettant aux virus de se reproduire et de contaminer rapidement les fichiers de l'ordinateur.

G : Je suis un programme qui détecte et éradique les virus.

I : Je suis un petit programme informatique situé dans le corps d'un autre qui cherche à se reproduire.

M : Je suis le nom d'un virus ver qui se propage à l'aide du courrier électronique. Le 16 octobre de chaque année, je risque de supprimer tous les fichiers de votre disque dur.

O : Je suis omniprésent sur les réseaux. J'ai de nombreuses variantes et je me propage dans le courrier électronique en me faisant passer pour un autre. A cause de moi, votre ordinateur sera lent et réagira bizarrement.

VERTICAL

1 : Je suis un support par lequel les virus peuvent s'introduire…

3 : Je suis une caractéristique de certains virus. Je me présente sous une forme incompréhensible pour les antivirus pour passer inaperçu.

8 : Je suis un virus ayant la capacité de modifier les signatures des antivirus afin de les rendre inopérants.

10 : Je suis une rumeur.

13 : je suis apparu durant l'été 2003. Je suis le 1er virus à avoir exploiter la

faille d'appel de procédure distant.

INTRODUCTION AUX VIRUS...

Introduction aux virus

Un virus est un petit programme informatique situé dans le corps d'un autre.

La définition d'un virus pourrait être la suivante :

"tout programme d'ordinateur capable d'infecter un autre programme

d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire."

Ils se multiplient pour la plupart, c'est-à-dire qu'ils s'insèrent dans les fichiers que vous exécutez. Le véritable nom donné aux virus est *CPA* soit *Code Auto-Propageable*, mais par analogie avec le domaine médical, le nom de "virus" leur a été donné.
Les virus vont de la simple balle de ping-pong qui traverse l'écran, au virus destructeur de données. Ce dernier étant la forme de virus la plus virulente. Ainsi, étant donné qu'il existe une vaste gamme de virus ayant des actions aussi diverses que variées, les virus ne sont pas classés selon leurs dégats mais selon leur mode de propagation et d'infection.

On distingue ainsi différents types de virus :

- les vers sont des virus capables de se propager à travers un réseau
- les troyens (chevaux de Troie) sont des virus permettant de créer une faille dans un système (généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle)
- les bombes logiques sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...)

Depuis quelques années un autre phénomène est apparu, il s'agit des canulars (en anglais hoax), c'est-à-dire des annonces reçues par mail (par exemple l'annonce de l'apparition d'un nouveau virus destructeur ou bien la possibilité de gagner un téléphone portable gratuitement,...) accompagnées d'une note précisant de faire suivre la nouvelle à tous ses proches. Ce procédé a pour but l'engorgement des réseaux ainsi que la désinformation.

Introduction aux antivirus

Les antivirus sont des programmes capables de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou des virus sont trouvés. On parle ainsi d'**éradication** de virus pour désigner la procédure de nettoyage de l'ordinateur.

La détection des virus

Les virus se reproduisent en infectant des "*applications hôtes*", c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant. Or, afin de ne pas avoir un fonctionnement chaotique, les virus sont programmés pour ne pas infecter plusieurs fois un même fichier. Ils intègrent ainsi dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté : il s'agit de la **signature virale**.

Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter. Il s'agit de la méthode de **recherche de signature** (*scanning*), la plus ancienne méthode utilisée par les antivirus.
Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus. Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus. De plus, les programmeurs de virus les ont désormais doté de capacité de camouflage, de manière à rendre leur signature indétectable, il s'agit de "virus polymorphes".

Les virus mutants

En réalité, la plupart des virus sont des clones, ou plus exactement des "**mutants**", c'est-à-dire des virus

ayant été réécrits par d'autres utilisateurs afin d'en modifier leur comportement ou bien uniquement leur signature.

Le fait qu'il existe plusieurs versions (on parle de **variantes**) d'un même virus le rend d'autant plus difficile à repérer dans la mesure où les éditeurs d'antivirus doivent ajouter ces nouvelles signatures à leurs bases de données ...

Les virus polymorphes

Etant donné que les antivirus détectent (entre autres) les virus grâce à leur signature (la succession de bits qui les identifie), certains créateurs de virus ont pensé à leur donner la possibilité de modifier automatiquement leur apparence, tel un caméléon, en dotant les virus de fonction de chiffrement et de déchiffrement de leur signature de telle manière à ce que seul le virus soit capable de reconnaître sa propre signature. Ce type de virus est appelé **virus polymorphe** (ce mot provenant du grec signifie *qui peut prendre plusieurs formes*).

Les rétrovirus

On appelle "rétrovirus" ou "virus flibustier" (en anglais *bounty hunters*) un virus ayant la capacité de modifier les signatures des antivirus afin de les rendre inopérants.

Les virus de boot

On appelle *virus de boot*, un virus capable d'infecter le secteur de démarrage d'un disque (*MBR*, soit *master boot record*), c'est-à-dire un secteur du disque copié dans la mémoire au démarrage de l'ordinateur, puis exécuté afin d'amorcer le démarrage du système d'exploitation.

Les chevaux de Troie

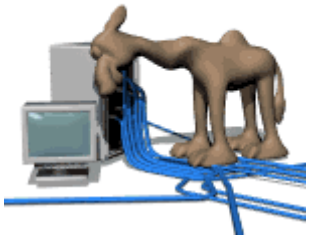
De plus, le virus peut représenter une faille dans la sécurité d'un réseau en créant des vulnérabilités dissimulées qu'un utilisateur extérieur pourra utiliser pour s'introduire dans le système, ou pour lui fournir des informations. Le but de ces virus est de se propager, vulnérabiliser des systèmes, et "marquer" les systèmes de telle façon à ce qu'ils puissent être repérés par leurs créateurs. De tels virus dévoilent l'ensemble des systèmes d'informations d'une machine et brisent ainsi la confidentialité des documents qu'elle renferme, on appelle ce type de virus un cheval de Troie...

Les virus trans-applicatifs (virus macros)

Avec la multiplication des programmes utilisant des macros, Microsoft a mis au point un langage de script commun pouvant être inséré dans la plupart des documents pouvant contenir des macros, il s'agit de VBScript, un sous-ensemble de Visual Basic. Ces virus arrivent actuellement à infecter les macros des documents Microsoft Office, c'est-à-dire qu'un tel virus peut être situé à l'intérieur d'un banal document Word ou Excel, et exécuter une portion de code à l'ouverture de celui-ci lui permettant d'une part de se propager dans les fichiers, mais aussi d'accèder au système d'exploitation (généralement Windows).

Or, de plus en plus d'applications supportent Visual Basic, ces virus peuvent donc être imaginables sur de nombreuses autres applications supportant le VBScript.
Le début du troisième millénaire a été marqué par l'apparition à grande fréquences de scripts Visual Basic diffusés par mail en fichier attaché (repérables grâce à leur extension *.VBS*) avec un titre de mail poussant à ouvrir le cadeau empoisonné.

Celui-ci a la possibilité, lorsqu'il est ouvert sur un client de messagerie Microsoft, d'accèder à l'ensemble du carnet d'adresse et de s'auto-diffuser par le réseau. Ce type de virus est appelé ver (ou worm en anglais).



DOSSIER VIRUS
QUELQUES EXEMPLES…

VIRUS SIRCAM

Présentation du virus Sircam

Le virus Sircam (nom de code *W32.Sircam.Worm@mm*, *Backdoor.SirCam* ou *Troj_Sircam.a*) est un ver se propageant à l'aide du courrier électronique. Il affecte particulièrement les utilisateurs de Microsoft Outlook sous les systèmes d'exploitation Windows 95, 98, Millenium et 2000.

Les actions du virus

Le ver Sircam choisit aléatoirement un document (d'extension *.gif, .jpg, .mpg, .jpeg, .mpeg, .mov, .pdf, .png, .ps ou .zip*)se trouvant dans le répertoire *c:\Mes Documents*\ de l'ordinateur infecté, puis envoie automatiquement un courrier électronique dont le sujet est le nom de ce document, dont le corps du message est un des deux messages suivants :

- En anglais

```
"Hi! How are you?

I send you this file in order to have your advice

See you later. Thanks"
"Hi! How are you?

I hope you can help me with this file that I send

See you later. Thanks"
"Hi! How are you?

I hope you like the file that I send to you

See you later. Thanks"
```

- Ou en espagnol

```
"Hola como estas ?

Te mando este archivo para que me des tu punto de vista

Nos vemos pronto, gracias."
```

Le virus Sircam adjoint au message une copie de lui-même dont le nom est celui du fichier récupéré sur le disque de l'utilisateur avec la double extension *.vbs*.

Le ver Sircam risque en outre de supprimer l'intégralité des fichiers de votre disque dur le **16 octobre** de chaque année si votre ordinateur utilise un format de date à l'européenne (jour/mois/année).

Sircam ajoute également du texte au fichier *c:\recycled\sircam.sys* lors de chaque redémarrage de la machine, ce qui risque potentiellement de saturer l'espace disponible sur le lecteur *C:*\.

Symptomes de l'infection

Les machines infectées possèdent sur leur disque les fichiers :

- Sirc32.exe
- Sircam.sys
- Run32.exe

Pour vérifier si vous êtes infectés, procédez à une recherche des fichiers cités ci-dessus sur l'ensemble de vos disques durs (*Démarrer / Rechercher / Fichiers ou Dossiers*).

Eradiquer le virus

Pour éradiquer le ver Sircam, la meilleure méthode consiste à utiliser un antivirus récent ou bien le kit de désinfection proposé par Symantec :
Télécharger le kit de désinfection

Il vous est également possible de procéder à une désinfection manuelle en suivant la procédure suivante :

- Supprimer les fichiers *Sirc32.exe* et *Sircam.sys*
- Supprimer le fichier *c:\windows\Runddl32.exe*
- Renommer le fichier *c:\windows\Run32.exe* en *c:\windows\Rundll32.exe*
- Editer le fichier *c:\autoexec.bat* et supprimer la séquence suivante : @win \recycled\sirc32.exe
- Dans la base de registre (à éditer en exécutant *c:\windows\regedit.exe*)
    - Dans *HKEY_CLASSES_ROOT/exefile/shell/open/command*, modifier la chaîne de données (en double-cliquant

sur *Défaut*) et entrer la chaîne suivante :

```
"%1" %*
```

- Dans *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/RunServices*, supprimer la clé *Driver32=C:\WINDOWS\SYSTEM\SCam32.exe*
- Dans *HKEY_LOCAL_MACHINE/Software*, supprimer le dossier *Sircam*

- Redémarrer votre ordinateur

VIRUS NIMDA

Présentation du virus Nimda

Le virus Nimda (nom de code *W32/Nimda* est un ver se propageant à l'aide du courrier électronique, mais il exploite également 4 autres modes de propagation :

- Le web
- Les répertoires partagés
- Les failles de serveur Microsoft IIS
- Les échanges de fichiers

Il affecte particulièrement les utilisateurs de Microsoft Outlook sous les systèmes d'exploitation Windows 95, 98, Millenium, NT4 et 2000.

Les actions du virus

Le ver Nimda récupère la liste des adresses présentes dans les carnets d'adresses de Microsoft Outlook et Eudora, ainsi que les adresses e-mails contenues dans les fichiers HTML présents sur le disque de la machine infectée.

Puis le virus Nimda envoie à tous les destinataires un courrier dont le corps est vide, dont le sujet est aléatoire et souvent très long et attache au courrier une pièce jointe nommée *Readme.exe* ou *Readme.eml* (fichier encapsulant un fichier exécutable). Les virus utilisant une extension du type *.eml* exploitent une faille de Microsoft Internet Explorer 5.

D'autre part le virus Nimda est capable de se propager à travers les répertoires partagés des réseaux Microsoft Windows en infectant les fichiers exécutables s'y trouvant.

La consultation de pages Web sur des serveurs infectés par le virus Nimda peut entraîner une infection lorsqu'un utilisateur consulte ces pages avec un navigateur Microsoft Internet Explorer 5 vulnérable.

En effet, le virus Nimda est également capable de prendre la main sur un serveur Web Microsoft IIS (Internet Information Server) en exploitant certaines failles de sécurité.

Enfin, le virus infecte les fichiers exécutables présents sur la machine infectée, ce qui signifie qu'il est également capable de se propager par échange de fichiers.

Symptomes de l'infection

Les postes de travail infectés par le ver Nimda possèdent sur leur disque les fichiers suivants :

- README.EXE
- README.EML
- fichiers comportant l'extension .NWS
- fichiers dont le nom est du type *mep*.tmp*, *mep*.tmp.exe* (par exemple *mepE002.tmp.exe*)

Pour vérifier si vous êtes infectés, procédez à une recherche des fichiers cités ci-dessus sur l'ensemble de vos disques durs (*Démarrer / Rechercher / Fichiers ou Dossiers*).

Eradiquer le virus

Pour éradiquer le ver Nimda, la meilleure méthode consiste tout d'abord à déconnecter la machine infectée du réseau, puis à utiliser un antivirus récent ou bien le kit de désinfection proposé par Symantec

:
Télécharger le kit de désinfection

D'autre part, le virus se propage par l'intermédiaire d'une faille de sécurité de Microsoft Internet Explorer, ce qui signifie que vous pouvez être contaminé par le virus en naviguant sur un site infecté. Pour y remédier il est nécessaire de télécharger le patch (correctif logiciel) pour Microsoft Internet Explorer 5.01 et 5.5. Ainsi, veuillez vérifier la version de votre navigateur et télécharger le correctif si nécessaire :
http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

VIRUS MAGISTR

Présentation du virus Magistr

Le virus Magistr (nom de code *W32/Magistr.b@MM*, *I-Worm.Magistr.b.poly* ou *PE_MAGISTR.B*) est un ver polymorphe (c'est-à-dire un ver dont la forme, ou plus exactement la signature, se modifie continuellement) se propageant à l'aide du courrier électronique. Il s'agit d'une variante du ver *Disemboweler* (*Magistr.A*) affectant particulièrement les utilisateurs de client de messagerie Microsoft Outlook, Eudora ou Netscape sous les systèmes d'exploitation Windows 95, 98, Millenium et 2000.

Les actions du virus

Le virus Magistr.B recherche les fichiers de carnet d'adresses présents sur le système (respectivement d'extensions .WAB et .DBX/.MBX pour les clients Outlook et Eudora), afin de sélectionner les destinataires du message.

Le sujet et le corps du message envoyé par le ver Magistr sont choisis aléatoirement en prenant un extrait de fichier trouvé sur le disque de l'ordinateur infecté.

Le virus Magistr adjoint au message une copie de lui-même dont le nom contient une extension (ou une double extension) du type *.com, .bat, .pif, .exe ou .vbs*.

Le ver Magistr risque en outre de supprimer l'intégralité des informations contenues dans :

- Le CMOS
- le BIOS
- Le disque dur

Le virus Magistr.B peut ainsi gravement endommager votre système et les informations s'y trouvant.

De plus, le virus Magistr.B est capable de désactiver le Firewal personnel *ZoneAlarm* à l'aide de la commande *WM_QUIT*.

Symptomes de l'infection

Les machines infectées possèdent la particularité suivante :
Un déplacement du pointeur de la souris sur le bureau provoque un déplacement des icones.

Eradiquer le virus

Pour éradiquer le ver Magistr, la meilleure méthode consiste à utiliser un antivirus récent ou bien le kit de désinfection suivant :
Télécharger l'utilitaire de désinfection.

VIRUS KLEZ

Présentation du virus Klez

Apparu au début de l'année 2002, le virus Klez est désormais omniprésent sur les réseaux et le risque qu'il représente est d'autant plus important que des nouvelles variantes du virus ne cessent d'apparaître (Klez.e, Klez.g, Klez.h, Klez.i, Klez.k, ...). Les nouvelles versions du virus intègrent des mécanismes de diffusion de plus en plus innovants rendant sa propagation de plus en plus aisée. Le virus KLEZ (nom de code *W32.Klez.Worm@mm*) est un ver se propageant à l'aide du courrier électronique. Il exploite également 4 autres modes de propagation :

- Le web
- Les répertoires partagés

- Les failles de serveur Microsoft IIS
- Les échanges de fichiers

Il affecte particulièrement les utilisateurs de Microsoft Outlook sous les systèmes d'exploitation Windows 95, 98, Millenium, NT4, 2000 et XP ainsi que les utilisateurs de Microsoft Internet Explorer.

Les actions du virus

Le ver Klez récupère la liste des adresses présentes dans les carnets d'adresses de Microsoft Outlook, Eudora ainsi que des logiciels de messagerie instantanée (ICQ), .

Puis le virus Klez envoie à tous les destinataires un courrier à l'aide de son propre serveur SMTP.

Ainsi le virus Klez est capable de générer des courriers dont le corps est vide, dont le sujet est choisi aléatoirement parmi une gamme d'une centaine de thèmes prédéfinis et attache au courrier une pièce jointe exécutable contenant une variante du virus. Les virus utilisant une extension du type *.eml* exploitent une faille de Microsoft Internet Explorer 5.

ATTENTION ! Le virus Klez a comme particularité d'être capable d'envoyer des mails en se faisant passer pour un expéditeur dont l'adresse a été trouvée sur la machine de la victime (le virus trafique le champ *from* du mail envoyé).

Les variantes les plus récentes du virus embarquent même des outils leur permettant de rendre obsolète les principaux anti-virus.

Comble du cynisme : les auteurs du virus l'ont programmé pour envoyer aux victimes un pseudo-correctif contre lui-même dans un courrier intitulé *Worm Klez.E immunity*. Le mail envoi également des faux messages d'erreur indiquant qu'un message n'a pas pû être délivré et contenant une fois de plus une copie du virus en fichier attaché !

D'autre part le virus Klez est capable de se propager à travers les répertoires partagés des réseaux Microsoft Windows en infectant les fichiers exécutables s'y trouvant.

La consultation de pages Web sur des serveurs infectés par le virus Klez peut entraîner une infection lorsqu'un utilisateur consulte ces pages avec un navigateur Microsoft Internet Explorer 5 vulnérable.

En effet, le virus Nimda est également capable de prendre la main sur un serveur Web Microsoft IIS (Internet Information Server) en exploitant certaines failles de sécurité.

Enfin, comme ses confrères, le virus infecte les fichiers exécutables présents sur la machine infectée, ce qui signifie qu'il est également capable de se propager par échange de fichiers.

ATTENTION ! Pour compléter le tableau, le virus Klez est prévu pour supprimer des fichiers choisis aléatoirement tous les sixièmes jours (donc le 6 du mois) des mois impairs. Petite cerise sur le gâteau : le 6 janvier et le 6 juillet le virus efface la totalité des fichiers présents sur le disque !!

Symptomes de l'infection

Le virus Klez utilise le plus de ressources possibles sur la machine infectée. Si votre ordinateur réagit lentement et bizarrement, la première chose à faire est donc de passer l'ensemble de vos disques au crible avec votre antivirus, sachant que le virus est capable d'avoir modifié l'antivirus pour ne pas se faire repérer...

Eradiquer le virus

Pour éradiquer le ver Klez, la meilleure méthode consiste tout d'abord à déconnecter la machine infectée du réseau, puis à utiliser un antivirus récent ou bien le kit de désinfection proposé par Symantec (en redémarrant de préférence l'ordinateur en mode sans échec) :
Télécharger le kit de désinfection

D'autre part, le virus se propage par l'intermédiaire d'une faille de sécurité de Microsoft Internet Explorer, ce qui signifie que vous pouvez être contaminé par le virus en naviguant sur un site infecté. Pour y remédier il est nécessaire de télécharger le patch (correctif logiciel) pour Microsoft Internet Explorer 5.01 et 5.5. Ainsi, veuillez vérifier la version de votre navigateur et télécharger le correctif si nécessaire :
http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

ATTENTION ! Etant donné que le virus falsifie l'adresse email de l'expéditeur (champ *from*), il est conseillé de ne pas répondre à l'expéditeur du virus mais de regarder le champ *Return-Path* du mail et d'écrire un message à ce dernier !

VIRUS BLASTER/LOVSAN

Présentation du virus LovSan

Apparu durant l'été 2003, le virus **LovSan** (connu également sous les noms *W32/Lovsan.worm*, *W32/Lovsan.worm.b*, *W32.Blaster.Worm*, *W32/Blaster-B*, *WORM_MSBLAST.A*, *MSBLASTER*, *Win32.Poza*, *Win32.Posa.Worm*, *Win32.Poza.B*) est le premier virus a exploiter la faille RPC/DCOM (*Remote Procedure Call*, soit en français *appel de procédure distante*) des systèmes Microsoft Windows permettant à des processus distants de communiquer. En exploitant la faille grâce à un débordement de tampon, un programme malveillant (tel que le virus LovSan) peut prendre le contrôle de la machine vulnérable. Les systèmes affectés sont les systèmes Windows NT 4.0, 2000, XP et Windows Server 2003.

Les actions du virus

Le ver **LovSan / Blaster** est programmé de telle façon à scanner une plage d'adresses IP aléatoire à la recherche de systèmes vulnérables à la faille RPC sur le port 135.

Lorsqu'une machine vulnérable est trouvée, le ver ouvre un shell distant sur le port TCP 4444, et force la machine distante à télécharger une copie du ver dans le répertoire *%WinDir%\system32* en lançant une commande *TFTP* (port 69 UDP) pour transférer le fichier à partir de la machine infectée.

Une fois le fichier téléchargé, il est exécuté, puis il crée des entrées dans la base de registre afin de se relancer automatiquement à chaque redémarrage :

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\`
- `Run "windows auto update" = msblast.exe I just want to say LOVE YOU SAN!! bill`
-
-

ATTENTION ! Pour compléter le tableau, le virus LovSan/Blaster est prévu pour effectuer une attaque sur le service *WindowsUpdate* de Microsoft afin de perturber la mise à jour des machines vulnérables !!

Symptomes de l'infection

L'exploitation de la vulnérabilité RPC provoque un certain nombre de dysfonctionnements sur les systèmes affectés, liés à la désactivation du service RPC (processus *svchost.exe* / *rpcss.exe*). Les systèmes vulnérables présentent les symptomes suivants :

- Copier/Coller défectueux ou impossible
- Ouverture d'un lien hypertexte dans une nouvelle fenêtre impossible
- Déplacement d'icones impossibles
- fonction recherche de fichier de windows erratique
- fermeture du port 135/TCP
- Redémarrage de Windows XP : le système est sans cesse relancé par *AUTORITE NT/system* avec le(s) message(s) suivant(s) :
- ```
  Windows doit maintenant redémarrer car le service appel
  de procédure distante (RPC) s'est terminé de façon inattendue
  arrêt du système dans 60 secondes veuillez enregistrer
  tous les travaux en cours cet arrêt a été initié par AUTORITE NT\SYSTEM
  Windows doit maintenant demarrer
  ```

Eradiquer le virus

Pour éradiquer le ver LovSan, la meilleure méthode consiste tout d'abord à désinfecter le système à l'aide du kit de désinfection suivant :
Télécharger le kit de désinfection

ATTENTION !

Si votre système reboote continuellement, il faut désactiver le redémarrage automatique :

- Cliquez sur *Poste de travail* avec le bouton droit
- Cliquez sur Propriétés / Avancé / Démarrage et récupération / Paramètres
- Décochez la case "redémarrer automatiquement" !

Vous pourrez rétablir cette option lorsque votre système fonctionnera à nouveau normalement.
  ```

Il est ensuite indispensable de mettre à jour le système à l'aide du service Windows Update ou bien en mettant à jour votre système avec le patch suivant correspondant à votre système d'exploitation :

- Patch pour Windows 2000
- Patch pour Windows XP

D'autre part, dans la mesure où le virus se propage par l'intermédiaire du réseau Microsoft Windows, il est fortement conseillé d'installer un pare-feu personnel sur vos machines connectées à internet et de filtrer les ports tcp/69, tcp/135 à tcp/139 et tcp/4444.

VIRUS BADTRANS

Présentation du virus BadTrans

Le virus BadTrans (nom de code *W32.BadTrans.B* ou *W32/Badtrans-B*) est un ver se propageant à l'aide du courrier électronique. Il exploite également un autre mode de propagation :

- Les failles de Microsoft Internet Explorer

ATTENTION ! Le virus BadTrans.B affecte particulièrement les utilisateurs de Microsoft Outlook sous les systèmes d'exploitation Windows 95, 98, Millenium, NT4 et 2000, dans la mesure où le virus s'active par simple consultation du message (c'est-à-dire même si l'utilisateur ne clique pas sur la pièce jointe).
http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

Les actions du virus

Le ver BadTrans récupère la liste des adresses présentes dans les carnets d'adresses de l'utilisateur infecté, ainsi que dans les pages web contenues dans les dossiers de cache Internet et dans le répertoire *Mes Documents*.

Puis le virus BadTrans envoie à tous les destinataires un courrier :

- dont le corps est vide, ou comportant la phrase *Take a look to the attachment.*
- dont le sujet est *Re: <Sujet du mail trouvé>*
- dont la pièce jointe possède un nom composé de trois parties
    - Première partie: un des textes suivants :
        - CARD
        - DOCS
        - FUN
        - HAMSTER NEWS_DOC
        - HUMOR
        - IMAGES
        - ME_NUDE
        - New_Napster_Site
        - News_doc
        - PICS
        - README
        - S3MSONG
        - SEARCHURL
        - SETUP
        - Sorry_about_yesterday
        - YOU_ARE_FAT!
    - Seconde partie: une des extensions suivantes :
        - .DOC

        - .MP3
        - .ZIP
    - Troisième et dernière partie : une des extensions suivantes :
        - .pif
        - .scr

Ainsi, le message contiendra une pièce jointe du type :

- Me_Nude.MP3.scr
- News_doc.DOC.scr
- HAMSTER.DOC.pif
- PICS.doc.scr
- HUMOR.MP3.scr
- README.MP3.scr
- FUN.MP3.pif
- YOU_are_FAT!.MP3.scr
- ...

Symptomes de l'infection

Les postes de travail infectés par le ver BadTrans possèdent sur leur disque le fichier suivant :

- kdll.dll, ce dernier est un cheval de Troie capable d'enregistrer les frappes sur le clavier afin de récupérer vos mots de passe

Pour vérifier si vous êtes infectés, procédez à une recherche des fichiers cités ci-dessus sur l'ensemble de vos disques durs (*Démarrer / Rechercher / Fichiers ou Dossiers*).

Eradiquer le virus

Pour éradiquer le ver BadTrans, la meilleure méthode consiste tout d'abord à déconnecter la machine infectée du réseau, puis à utiliser un antivirus récent.

D'autre part, le virus se propage par l'intermédiaire d'une faille de sécurité de Microsoft Outlook, ce qui signifie que vous pouvez être contaminé par le virus sans cliquer sur la pièce jointe. Pour y remédier il est nécessaire de télécharger le patch (correctif logiciel) pour Microsoft Outlook. Ainsi, veuillez vérifier votre client de messagerie et télécharger le correctif si nécessaire :

http://www.microsoft.com/technet/security/bulletin/MS01-020.asp