

Forum Télécom

Virus informatique: Comment vacciner mon PC ?

Stany Wyrzykowski

C2D System House S.A.

Introduction

- Définition du virus
- Les familles de virus
- Les cousins des virus
- Fonctionnement d'un virus
- Règles générales de protection
- Que faire en cas de contamination ?

Définition du virus

- Programme caché
- Auto-multiplicateur
- Déclenchement d'une action

Les familles de virus

- Virus d'amorce
- Virus d'applications
- Virus macros
- Virus mail

Virus d'amorce

- infecte le boot sector
- remplace l'amorce du système

Virus d'application

- infecte les fichiers exécutables
- remplace l'amorce du fichier avec extension
.exe .com .sys

Virus macros

- infecte les fichiers documents de Word et Excel
- utilise principalement Microsoft Visual Basic pour Application

Virus mails

- appelé également vers
- Sur base des programmes de messagerie (Notamment Microsoft Outlook)
- Visualisation d'une page Web à partir de l'Explorer

Les cousins des virus

- Les hoax
- Les troyens
- Les bombes emails.
- Les espions

Les Hoax

- Rumeur dont le but est de faire croire à la présence d'un virus.
- Si vous transmettez le message, vous êtes vous-même acteur de la propagation.

Les Troyens

- Egalement nommés Chevaux de Troie, Trojans
- Ne se reproduit pas comme les virus
- Permet de prendre le contrôle de votre ordinateur

Les bombes emails

- Utilise ' discrètement ' votre ordinateur pour envoyer des milliers de messages ' électroniques ' (paquets IP) ou ' humains ' (email) à un destinataire également ciblé par d'autres utilisateurs.

Les espions

- Envoie régulièrement de l'information contenue sur votre ordinateur
- Bannières publicitaires
- Logiciels utilitaires gratuits

Fonctionnement d'un virus

- Analogie au virus biologique
- Dissimulation
- Infection maximale
- Interception des parties de programmes: Commandes, Bios,...

Règles générales de protection (Première partie).

- Faites des copies de sécurité (sauvegardes, backup)
- Ne pas télécharger des programmes d'origine douteuse
- Méfiez-vous des fichiers joints dans les emails
- Fuyez les disquettes et CD d'origine douteuse

Règles générales de protection (Deuxième partie).

- Analysez avec un anti-virus tout fichier avant de l'ouvrir
- Créez une disquette ' Safe boot '
- Tenez-vous au courant des apparitions de nouveaux virus.
- Installez et mettez à jour un anti-virus

Que faire en cas de contamination ?

- Installer un logiciel antivirus
- Mettre à jour le logiciel antivirus
- Vérifier le bien fondé (hoax)
- Télécharger le remède
- Récupérer les données à partir de la sauvegarde

Conclusion

et questions-réponses