

Sécurité: Virus

Mohamed El-Had Mellany - Mouagni Anas

UM2

6 Décembre 2012

Sommaire

- 1 Introduction
- 2 Qu'est-ce qu'un virus ?
- 3 Les différentes familles
- 4 Comment lutter ?
- 5 Quelles sont les failles exploitées ?
- 6 Les virus dans le monde
- 7 Conclusion

Introduction

Un logiciel malveillant est un programme développé dans le but de nuire à un système informatique.

Sommaire

- 1 Introduction
- 2 Qu'est-ce qu'un virus ?
 - Définition
 - Origine
 - Les vecteurs de contamination
 - Comment se reproduisent-ils ?
- 3 Les différentes familles
- 4 Comment lutter ?
- 5 Quelles sont les failles exploitées ?

Définition

Un virus est un programme susceptible de s'introduire dans un système, de s'y exécuter et qui tend à se propager de machines en machines par un mécanisme de réplication.

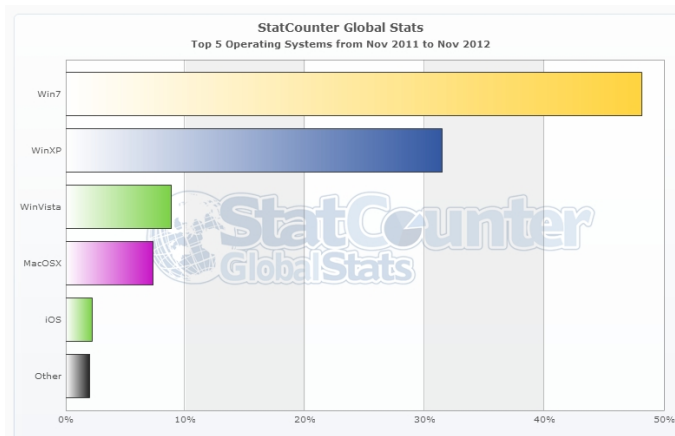
Origine

- 1949: Jhon Von Neumann présente les fondements théorique des logiciels autocopié.
- 1960: Un groupe d'ingénieur des laboratoire Bell met au point un jeu informatique du nom de Core War.
- 1983: Le premier virus fut créé par Fred Cohen.

Origine

- Dans les années 80, les virus visent un ensemble de systèmes d'exploitation de réseaux.
- Dans les années 90, ils servent surtout à dérober des informations confidentielles.
- Les années 2000, ils utilisent les failles de Windows.

Systèmes d'exploitation les plus utilisés



Comment attrape-t-on un virus ?

Un virus ne s'installe pas seul, il lui faut toujours un moyen pour arriver sur la machine et s'installer, on parle de vecteurs.

Quels sont les vecteurs possibles ?

- Le réseau (téléchargement http, pièce jointe dans un mail...)

Quels sont les vecteurs possibles ?

- Le réseau (téléchargement http, pièce jointe dans un mail...)
- Les périphériques (Disque Dur, clef USB)

Quels sont les vecteurs possibles ?

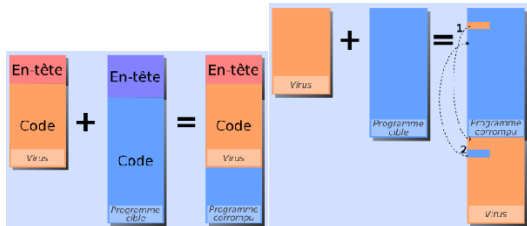
- Le réseau (téléchargement http, pièce jointe dans un mail...)
- Les périphériques (Disque Dur, clef USB)
- Autres supports (DVD, CD, BlueRay)

Comment se reproduisent-ils ?

Les virus se reproduisent en infectant un hôte: ajout d'un comportement malveillant à un programme existant.

Comment se reproduisent-ils ?

Infection par écrasement et par recouvrement de code.



Sommaire

- 1 Introduction
- 2 Qu'est-ce qu'un virus ?
- 3 Les différentes familles
 - Familles
 - Le plus dangereux
- 4 Comment lutter ?
- 5 Quelles sont les failles exploitées ?
- 6 Les virus dans le monde

Familles

1 virus de boot

Familles

- 1 virus de boot
- 2 virus polymorphique

Familles

- 1 virus de boot
- 2 virus polymorphique
- 3 virus furtif

Familles

- 1 virus de boot
- 2 virus polymorphique
- 3 virus furtif
- 4 virus chiffré

Familles

- 1 virus de boot
- 2 virus polymorphique
- 3 virus furtif
- 4 virus chiffré
- 5 virus lié à l'horloge système

Familles

- 1 virus de boot
- 2 virus polymorphique
- 3 virus furtif
- 4 virus chiffré
- 5 virus lié à l'horloge système
- 6 bombe logique

Le plus dangereux

Tchernobyl (CIH), de 1998 à 2002 a fait environ 80 millions de dollars de dégâts.

Sommaire

- 1 Introduction
- 2 Qu'est-ce qu'un virus ?
- 3 Les différentes familles
- 4 Comment lutter ?**
 - Antivirus
- 5 Quelles sont les failles exploitées ?
- 6 Les virus dans le monde
- 7 Conclusion

Antivirus ?

- Qu'est ce qu'un antivirus ?

Les techniques de détections

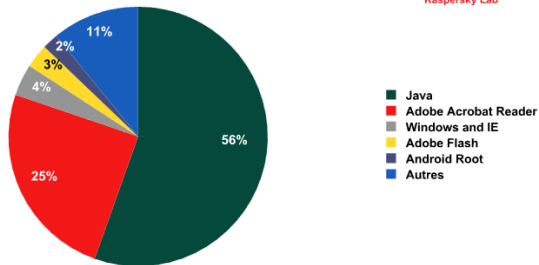
- Signature
- Contrôleur d'intégrité
- Analyse spectrale
- Comportement

Sommaire

- 1 Introduction
- 2 Qu'est-ce qu'un virus ?
- 3 Les différentes familles
- 4 Comment lutter ?
- 5 Quelles sont les failles exploitées ?**
- 6 Les virus dans le monde
- 7 Conclusion

Quelles sont les failles exploitées

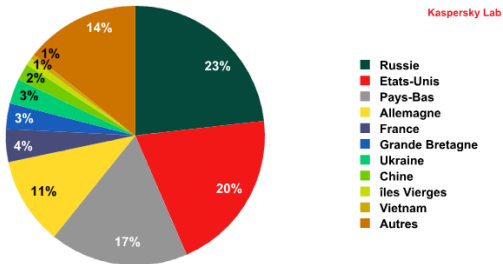
Graphique des vulnérabilités exploitées par les codes malveillants



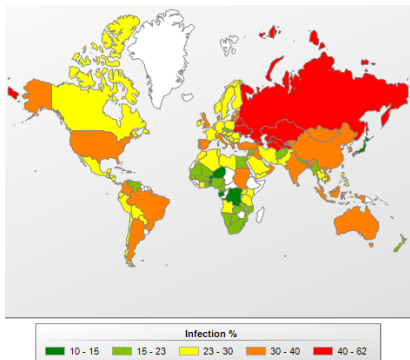
Sommaire

- 1 Introduction
- 2 Qu'est-ce qu'un virus ?
- 3 Les différentes familles
- 4 Comment lutter ?
- 5 Quelles sont les failles exploitées ?
- 6 Les virus dans le monde**
 - Les pays hébergeurs de programmes malveillants
 - Pays dont les internautes ont été les plus exposés

Les pays hébergeurs de programmes malveillants



Pays dont les internautes ont été les plus exposés



Sommaire

- 1 Introduction
- 2 Qu'est-ce qu'un virus ?
- 3 Les différentes familles
- 4 Comment lutter ?
- 5 Quelles sont les failles exploitées ?
- 6 Les virus dans le monde
- 7 Conclusion

Conclusion

Les virus ont été créés dans un but expérimental, puis l'idée a été reprise pour en faire des programmes malveillants.

Le principal vecteur se trouve généralement entre la chaise et le clavier.

De nos jours, les virus sont devenus des armes employées dans des cyber-guerres menées par certains états.

Ne pas se soucier de la sécurité de ses machines fait potentiellement de l'utilisateur un participant passif de la cyber-criminalité.

Sources

Les réseaux - G. Pujolle - Edition 2011

<http://vaccin.sourceforge.net/docs/definition2.html>

<http://fr.wikipedia.org/>

<http://www.infos-du-net.com/actualite/dossiers/112-2-histoire-virus.html>

<http://www.commentcamarche.net/news/5856869-le-systeme-d-exploitation-windows-7-devient-le-plus-utilise-dans-le-monde>

<http://vaccin.sourceforge.net/docs/definition2.html>

<http://securite.topnet.tn/>

<http://www.viruslist.com/fr/viruses/analysis>