

Virus informáticos

Georg Lehner

17 de septiembre de 2002

La amiga de una amiga tiene que contestarle a su profesor algunas preguntas sobre los "Antivirus". Ya que las preguntas son tontas pero el tema importante publico la información respectiva aquí. Para que el/la profesor/a tenga pena, también publico las preguntas.

Índice

1. Generalidades	2
2. ad 1.- ¿Que son los antivirus?	2
3. ad 2.-¿Como funcionan los antivirus?	3
4. ad 3.-¿Por que y Para que crearon los antivirus?	3
4.1. Por que:	3
4.2. Para que:	3
5. ad 4.-Tipos de antivirus.	3
5.1. Clasificación A, por acción:	3
5.2. Clasificación B, por método de detección:	4
5.3. Clasificación C, por instante de activación:	4
5.4. Clasificación D, por Objeto infectado:	4
6. ad 5.-Características de los antivirus.	4
7. Derecho de autor	4

El lun, 01-01-1990 a las 02:30, <censurado> escribió:
> Hola Jorge:
>
> Aqui van las preguntas:
> Hay que hacer tres tipos de antivirus. Y de cada uno contestar las

```
> siguientes preguntas:
>
> 1.- ¿Que son los antivirus?
> 2.-¿Como funcionan los antivirus?
> 3.-¿Por que y Para que crearon los antivirus?
> 4.-Tipos de antivirus.
> 5.-Características de los antivirus. >
>
```

Hola <censurado>!

Si en caso esto son las formulaciones literales del o de la profesor/a debe estar bastante chiflada o no saber ni jota de lo que está pidiendo.

Pero bueno:

1. Generalidades

hay varios tipos de virus. Un virus es un programa, que se anexa una copia de si mismo en uno o varios otros programa.

Al ejecutarse estos, se vuelven a "reproducir" por la misma función.

Además, la mayoría de los virus está cargado con una función dañina para el sistema en el cual se anida.

Todo "objeto" informático que puede "ejecutarse" puede ser "infectado" por un programa virus. Los objetos comunes a infectarse son:

- El sector de arranque de un floppy o disco duro - Un programa ejecutable del sistema (aplicación) - Documentos Word u Hojas de Cálculo Excel, a través de su lenguaje `_Macro_`, que en condiciones normales se utiliza para expandir las funciones de estos programas.

Estos son probablemente los tres tipos de virus a cual se refiere la pregunta. También existen virus en lenguaje Java y JavaScript, que se distribuyen a través de páginas Web o aplicaciones Java, otros habrán también...

2. ad 1.- ¿Que son los antivirus?

Son programas que tratan de detectar, si un objeto informático ejecutable es infectado por un programa Virus.

La mayoría de los antivirus pueden restaurar el archivo infectado a su estado original, aunque no siempre es posible, dado que los virus pueden haber hecho cambios no reversibles.

Los antivirus pueden también borrar los archivos infectados u hacer el virus inofensivo.

3. ad 2.-¿Como funcionan los antivirus?

Un método es la comparación del archivo infectado con una muestra de un virus conocido.

Hay métodos heurísticos que tratan de encontrar modificaciones típicas que producen los virus en los archivos encontrados,

y existen programas que graban para cada archivo encontrado en el sistema unos atributos típicos (longitud, suma cíclica). Al revisar el sistema por virus, se vuelven a determinar estos atributos y si no coinciden con los datos guardados con los actuales se considera posiblemente infectado el archivo.

4. ad 3.-¿Por que y Para que crearon los antivirus?

4.1. Por que:

Porque los virus en muchos casos causan daño a los datos y archivos. En caso contrario todavía queda la reducción del rendimiento de la computadora, causado por el aumento de tamaño de los archivos, y la actividad computacional adicional para su reproducción.

4.2. Para que:

Para detectar la infección, y para eventualmente restaurar los archivos infectados.

También se aplican preventivamente: Antes de introducir un archivo al sistema por copia de un disquete o guardar un archivo añadido a un Email, o antes de ejecutar, abrir o copiar un archivo dentro del sistema se revisa si presenta infección, y se aborta la acción intentada, o retrazada hasta que el archivo u objeto informático esté desinfectado.

5. ad 4.-Tipos de antivirus.

5.1. Clasificación A, por acción:

- solo detección
- detección y desinfección
- detección y aborto de la acción
- detección y eliminación del archivo/objeto

5.2. Clasificación B, por método de detección:

- Comparación directa
- Comparación por signatura
- Comparación de signatura de archivo (detección por comparación con atributos guardados).
- por métodos heurísticos

5.3. Clasificación C, por instante de activación:

- Invocado por el/la usuario/a
- Invocado por actividad del sistema (abrir, ejecutar, copiar, guardar archivo)

5.4. Clasificación D, por Objeto infectado:

- Sector de Arranque
- Archivo Ejecutable
- MacroVirus (Excel, Word)
- Java

6. ad 5.-Características de los antivirus.

Los antivirus solo son necesarios en sistemas y aplicaciones de la empresa Microsoft.

Ya que continuamente se desarrollan nuevos Virus, hay que actualizar las bases de datos y los programas antivirus constantemente, para obtener buena protección.

A pesar de una actualización constante no se puede garantizar una protección completa, ya que una vacuna puede ser desarrollada solo después de descubrir la enfermedad.

7. Derecho de autor

Este Documento ha sido elaborado por Georg Lehner, Jorge.Lehner@gmx.net; y solo puede ser utilizado para uso personal. La reproducción y uso para fines educativos o comerciales son permitidos bajo la condición que esta nota de derecho de autor sea incluido en la copia.

Se puede descargar este documento en formato PDF desde el sitio Web del autor: <http://www.magma.com.ni>.