Virus y Antivirus: Los nombres de los virus

El nombre que se da a cada nuevo virus que se descubre no se elije de forma totalmente aleatoria; de hecho el propio nombre completo proporciona bastante información acerca de la naturaleza del virus. Este documento pretende reseñar las reglas de la asignación de nombres a los virus.

Son los fabricantes de productos antivirus quienes dan nombre a los ejemplares que reciben y la mayor parte de ellos se guián (si bien de forma sólo aproximada) por la Convención de Nombres de Virus propuesta por CARO - Computer Antivirus Research Organization- en 1991 y actualizada en 1999.

Estructura de los nombres de los virus

La estructura de los nombres de los virus es la siguiente:

Prefijo + Nombre + Variante + Sufijo

La mayoría de los fabricantes separan el prefijo del nombre mediante una barra "**/**" y este de la variante con un punto "**.**"

Prefijos

Los prefijos indican la plataforma a la que afecta el virus y ocasionalmente el lenguaje en que está escrito:

W32 -> Afecta a sistemas Windows de 32 bits (Windows 95/98/ME/NT/2000/XP)
W95 -> Afecta a sistemas Windows 95/98/ME
WM -> Virus de macro de Microsoft Word
XM97 -> Virus de macro de Microsoft Excel 97
Worm -> Gusano
Troj -> Troyano
Bck -> Puerta trasera
VBS -> Escrito en Visual Basic Script
JS -> Escrito en Java Script
HTML -> Virus incrustado en código HTML para explotar alguna vulnerabilidad
Mac -> Afecta a sistemas Apple Macintosh
Linux -> Afecta a sistemas Linux

Ocasionalmente algunos fabricantes yuxtaponen más de un prefijo, así Worm.W32 señalaría a un gusano que se propaga a través de sistemas Windows de 32 bits.

Nombres

El nombre del especimen es asignado por cada fabricante de antivirus y normalmente se corresponde bien con alguna característica destacable del virus (Viernes 13), bien con algún término presente en los mensajes en los que se propaga, en el propio código del virus o en textos que este presenta tras la infección (LoveLetter, Netsky).

Aunque los fabricantes de antivirus tienden a compartir muestras y unificar nombres no siempre todos ellos utilizan la misma denominación para un especimen dado, de ahí que se hable de "alias" de los virus para identificar los diferentes nombres.

Variantes

Los autores de virus raramente se conforman con escribir una única versión de estos. Cada dia es más frecuente la aparición de decenas y aún centenares de variantes de un mismo virus original, llegando a constituir auténticas familias. Para identificar estas variantes se utilizan letras que se asignan en orden alfabético a medida que se detectan nuevos miembros de una familia.

La profusión de variantes de algunos virus genera un problema añadido de identificación ya que no hay manera de garantizar que los fabricantes de antivirus identifiquen y cataloguen de forma simultanea las

diferentes variantes.

Sufijos

Los sufijos se utilizan para reseñar alguna otra caracterítica importante del virus, tales como:

@m -> Virus que de propgación por correo electrónico
@mm -> Virus de propagación masiva por correo electrónico
gen -> Detección genérica, en este caso no se dispone de una identificación precisa de la variante.

Temas relacionados

Búsqueda de descripciones de virus
Análisis de muestras de virus

Apoyo adicional

Si ha tenido problemas al aplicar estos procedimientos o requiere de apoyo adicional, recuerde que puede solicitarlo cumplimentando el formulario ubicado en la dirección:

http://moncayo.unizar.es

a través del enlace Solicitar intervenciones al SICUZ.

Marzo de 2005
Informática Distribuida
Servicio de Informática y Comunicaciones - Centro de Cálculo
Universidad de Zaragoza

Puedes obtener este documento en formato pdf pulsando aquí