Como se nombran los virus informáticos

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 guíen (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 espécimen 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 espécimen 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 característica importante del virus, tales como:

@m -> Virus que de propagación 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.

prefijos

* A2M: Macrovirus de Microsoft Access 2.0

* A97M: Macrovirus de Microsoft Access 97

* BAS: En lenguaje BASIC.

* BAT: Script de procesamiento por lotes de comandos. Existen gusanos y troyanos que utilizan estos ficheros Batch (.bat en MS-DOS/Windows)

* CHM: HTML compilado. Utilizado en los archivos de ayuda de Windows.

* CSC: Virus que utilizan el Corel Script.

* DOS32: Virus para la versión de 32 bits de DOS.

* FreeBSD: Virus para el sistema operativo FreeBSD.

* INF: Infecta archivos .INF de Windows.

* IRC: Gusanos que utilizan el Internet Relay Chat para reproducirse.

* JAVA: Programado en Java.

* JS: Programado en Java Script o JScript.

* Linux: Virus para el sistema operativo Linux.

* LOGO: Programado en el lenguaje de programación Logo.

* MAC: Virus para el sistema operativo de Macintosh.

* Novell: Gusanos que aprovechan los sistemas Novell para propagarse.

* O97M: Macrovirus de Microsoft Office 97 en general; puede ser tanto de Word, Excel y PowerPoint.

* OS2: Virus para el sistema operativo OS2.

* Palm: Virus para el sistema operativo PalmOS.

* PERL: Scripts en Perl.

* PIF: Infecta archivos .PIF de Windows.

* PHP: Scripts en PHP.

* PP97M: Macrovirus de Microsoft PowerPoint 97.

* REG: Infecta archivos .REG de Windows.

* SQL: Gusano que utiliza una base de datos SQL para propagarse.

* SunOS: Virus para el sistema operativo SunOS.

* Unix: Virus para el sistema operativo Unix.

* V5M: Macrovirus de Microsoft Visio 5.

* VBS: Programado en Visual Basic Script

* VirTools: Malware utilizado para la creación de virus/gusanos/troyanos o agregado de funcionalidades básicas.

* WBS: Programado en Windows Batch Script.

* W1M: Macrovirus de Microsoft Word 1.0.

* W2M: Macrovirus de Microsoft Word 2.0.

* W97M: Macrovirus de Microsoft Word 97.

* Win16: Se ejecuta sobre plataformas Windows de 16 bits (por ejemplo, Windows 3.11)

* Win32: Se ejecuta sobre plataformas Windows de 32 bits

* Win95: Sólo puede ejecutarse correctamente sobre Windows 95, o puede tener problemas en hacerlo sobre otras versiones del sistema operativo.

* WinNT: Sólo puede ejecutarse sobre Windows NT.

* Win2k: Sólo puede ejecutarse sobre Windows 2000.

* WM: Macrovirus de versiones anteriores de Microsoft Word.

* X97M: Macrovirus de Microsoft Excel 97.

* XF: Macro de fórmula de Microsoft Excel.

* XM: Macrovirus de versiones anteriores de Microsoft Excel.

Otro tipo de prefijos que se utilizan en nuestras denominaciones de nombre son para especificar si un virus fue programado en un lenguaje de alto nivel (HLL: High Level Language):

* HLL: para denominar todos los virus programados en lenguajes de alto nivel (Pascal, Delhpi, Visual Basic, C++, etc).

* HLLC: virus del tipo de compañía, programado en un lenguaje de alto nivel.

* HLLO: virus, programado en un lenguaje de alto nivel, que sobrescribe el archivo infectado.

* HLLP: virus que se agrega al comienzo del archivo infectado.

* HLLW: gusano programado en un lenguaje de alto nivel

También se utilizan otros modificadores para remarcar si un virus tiene funcionalidades de robo de contraseñas. Estos son prefijos al nombre del virus, por ejemplo Win32/PSW.Virus, donde PSW detalla que el Virus obtiene claves de acceso del equipo infectado. Los prefijos utilizados son:

* PSW: es la denominación genérica a cualquier virus que roba contraseñas (PSW = Password Stealer)

* PSW.AIM: virus que especificamente obtiene claves de acceso del AOL Instant Messenger.

* PSW.ICQ: especializado en robar contraseñas del mensajero instantáneo ICQ.

* PSW.MSN: es capaz de acceder a las contraseñas del MSN Messenger y enviarlas al autor del virus.

Asimismo, es posible encontrar modificadores especiales para especificar que el virus en cuestión es un componente de un troyano, como en los siguientes casos:

* Dialer: es un troyano con características para discar números telefonicos de pago.

* Flooder: tipo de malware que tiene capacidad para sobrecargar algún tipo de servicio, como por ejemplo, el IRC.

* TrojanDownloader: significa que es un componente encargado de descargar un virus del tipo troyano (por ejemplo, VBS/TrojanDownloader.Trident).

* TrojanDropper: similar al sufijo Dropper que se explica más abajo, pero específico para los componentes de un troyano que lo liberan en el sistema infectado (por ejemplo, VBS/TrojanDropper.Kagra.A)

Los sufijos que pueden ser utilizados en las denominaciones de los virus corresponden al tamaño del archivo, si son números, o a la versión del virus, si son letras.

Algunos otros sufijos utilizados son:

* Dropper: es un componente de un virus o troyano encargado de liberar el verdadero virus en el sistema infectado (p.e. BAT/Delwin.AP.dropper)

* UPX: significa que es una versión del virus que está comprimida por la utilidad UPX (p.e. Win32/Mirchack.UPX)

Fuente: enciclopedia del virus