Propios del año 2002 podemos mencionar al Gusano My Party, de origen ruso, que sigue confundiendo a muchos, y creó una rápida epidemia.
El Gusano envía el anexo WWW.MYPARTY.YAHOO.COM confundiendo a la mayoría de los usuarios finales, que lo reciben desde una PC infectada pensando que es un enlace a una dirección Web y no detallan que están dando un doble click a un ejecutable con extensión .COM que contiene el código del Gusano.

También aparecieron otros como Frethem (You password !) y BugBear, pero sin lograr grandes aportes.

El Gusano del 2002

Sin dudas el Gusano del 2002 fue el Klez.

Apareció en los reportes del 2002 desde el mes de enero (6to lugar), febrero (3er lugar), marzo (2do lugar) y desde abril hasta septiembre ¡1er lugar¡, en octubre fue desplazado al segundo lugar por el Bugbear, en noviembre retomó el 1ro y en diciembre fue al 2do. lugar desplazado por el Opaserv.

El autor del Klez se caracterizó por desarrollar sistemáticamente diferentes variantes (A hasta H o I) que comenzaron enviándose ellos mismos en un anexo infectado hasta llegar a la variante de no mostrar ningún anexo y ser altamente destructivo, llegando a afectar la disponibilidad del Sistema Windows. La variante actual: W32/Klez H (Virus Elkern B) cómo otras variantes anteriores del Klez, utiliza la vulnerabilidad llamada «Incorrect MIME Header» (MS01-020, MS01-027) que permite la ejecución automática de código mientras el mensaje simplemente es leído, o visto en el panel de vista previa.
En la actualidad el deshabilitar las opciones Panel de vista Previa y Vista Previa Automática del cliente Outlook o del cliente de correo que utilicemos así como deshabilitar la ejecución automatica de Scripts y Actives X del Navegador, son medidas de seguridad práctica que debemos aplicar para evitar ataques de este tipo.

La versión «H» de Klez apareció a mediados de mayo, y ha sido la que más incidentes ya causó durante el año 2000. Este gusano infecta ejecutables al crear una copia oculta del archivo host original y después reemplaza el archivo original consigo mismo. La copia oculta se encripta, pero no contiene datos virulentos. El nombre del archivo oculto es el mismo que el del archivo original, pero con una extensión aleatoria. Este gusano busca en la libreta de direcciones de Windows, la base de datos ICQ, y archivos locales y direcciones de correo electrónico y envía un mensaje a estas direcciones consigo mismo, con lo que garantiza las epidemias. Klez.H contiene su propio motor SMTP y trata de adivinar los servidores SMTP disponibles.

Para engañar a quienes lo reciben, la línea del asunto y el cuerpo del mensaje son aleatorios, lo que además dificultan las recetas para prevenirlo. La dirección de origen se elige aleatoriamente de las direcciones de correo que el gusano encuentra en la computadora infectada con lo cual crea falsas acusaciones y dificulta las investigaciones para detectar las PCs infectadas desde donde se autoenvía el Gusano.

También trata de deshabilitar los Software Antivirus que se encuentren activos en la PC infectada.

SITUACIÓN INTERNACIONAL DE LOS PROGRAMAS MALIGNOS , NOVIEMBRE DEL 2003

Según la información publicada por la revista especializada Virus Bulletin de Octubre del 2003, los incidentes causados por los Programas Malignos según su tipo, tienen el siguiente comportamiento:

TIPO	INCIDENTES
File	99.66 %
Macros	0.03 %
Script	0.30 %
Boot y Otros	0.01 %

Como podemos apreciar, los Virus, Gusanos y Troyanos para Windows 32 bits son los principales responsables de los incidentes internacionales. Su vía de trasmisión es el correo electrónico y utilizan la técnica del autoenvío desde una PC atacada. Escriben el código maligno dentro del cuerpo del mensaje o infectan anexos (attachments) a mensajes en los cuales utilizan la ingeniería social para que asuntos o textos sugestivos traten de confundir a los incrédulos o poco preparados usuarios finales. La otra técnica utilizada es la de ejecutar un comando enviado desde una PC remota para explotar alguna vulnerabilidad del Sistema Operativo (Ej: Windows) o de sus aplicaciones (Ej: IE, IIS)

Los **Virus Macros** de Office han cedido terreno, pues llegaron a ser los causantes de más del 80 % de los incidentes reportados, pero a mi juicio la aplicación de las protecciones standard de Office ha minimizado esta amenaza. Los Script tienen un bajo % y los Virus de Boot Sector, prácticamente no se reportan, pues las mismas pastillas Flash Bios comparan los Boot Sectors antes de dar la carga del Sistema.

(Continúa en el próximo número).