Panoramica de los Programas Malignos

XIII Asamblea General OLACEFS

(Primera parte)

Lic. José Bidot Peláez.
Director General de Segurmática. Cuba.
Email: jbidot@seg.inf.cu

Según una investigación de **ICSA**, en 1999 los programas malignos superaron en 4 veces otros tipos de ataques y agresiones a las redes por lo que desde esa fecha resulta imprescindible analizar el comportamiento de ellos en cualquier estudio sobre la seguridad de las Tecnologías de la Información. Esta ponencia pretende analizar los sucesos más significativos ocurridos durante el año 2003, y considera los programas malignos que más incidentes ocasionaron desde el año 2000 hasta la fecha y de los recursos de los cuales se valieron sus autores para engañar a los usuarios finales. Los programas malignos causaron durante el año 2001 daños ascendentes a 13 Billones de USD , según la revista especializada SC InfoSecurity News Magazine, de Mayo del 2002.

MAYORES AFECTACIONES ECONÓMICAS :

Michael Erbschloe, vicepresidente de desarrollo de Computer Economics (firma independiente de investigación especializada), realizó un análisis económico publicado a principios del 2002, titulado "Indice de Ataques Cibernéticos", donde muestra el impacto relativo de incidentes específicos.

Los causantes de las mayores epidemias con incidencias económicas, son los siguientes:

Año	Código Maligno	Impacto Económico Mundial ($U.S.)
2000	Love Letter	$ 8.750 Millones
2001	Code Red(s)	$ 2.620 Millones
2001	SirCam	$ 1.150 Millones
1999	Melissa	$ 1.100 Millones
1999	Explorer	$ 1.020 Millones
2001	Nimda	$ 635 Millones

Según las estadísticas internacionales del Computer Research Institute aparecen como promedio 10 nuevos programas malignos diarios, y en la actualidad se reportan unos 75 Mil.

CAMBIO EN LA NATURALEZA DE LOS PROGRAMAS MALIGNOS

Al analizar el desarrollo de los Sistemas Operativos para las PCs podemos apreciar un cambio en la naturaleza de los programas malignos. Inicialmente, con el MS-DOS predominaron los virus infectores de programas ejecutables, con la entrada de Windows 3.1 prevalecieron los infectores de Boot Sector; a partir de Windows' 95 (Office 95) entramos en la Era de los Virus Macros, y a partir del año 99 la mayor cantidad de incidentes la ocasionan los programas malignos que como anexos se transmiten por correo electrónico. En el 2003 son los programas malignos escritos para Windows de 32 bits los que dominan el escenario internacional.

Además de los anexos a mensajes infectados por Virus, desde mediados de 1999 la mayor cantidad de incidentes la ocasionan los Gusanos, cuyos creadores han sido capaces de desarrollar diferentes técnicas para autoenviarse desde una PC "infectada" a través del correo electrónico a todas las direcciones del Libro de Direcciones, a las primeras 100 direcciones, a las direcciones de los mensajes que estén en la bandeja de entrada, a los que tengan anexos. Al autoenviarse, el receptor recibe un mensaje desde una dirección conocida (ya que su email aparece en el Libro de Direcciones de la PC desde donde se autoenvía) que le resulta familiar o hasta confiable. El detalle es que no es el usuario de esa PC quien nos envía el mensaje, es el propio Gusano quien se autoenvía.

De esta forma, las técnicas desarrolladas para burlar o confundir a los receptores van desde escribir un texto fijo o hasta variable, incluso en diferentes idiomas, relacionado con un asunto, que puede ser variable también. El cambio de nombre del anexo (conteniendo al programa maligno), textos que hacen referencia a un falso anexo conteniendo imágenes pornográficas, y hasta mensajes que infectan sin utilizar anexos, pues el código malicioso se encuentra dentro del formato MIME modificado del texto.

Estas amenazas, a las cuales nos enfrentamos en el presente, y que de ninguna manera serán las únicas, nos motivan a analizarlas . En marzo del 99 el virus macro de Word, Melissa, infectó 1 millon 200 mil PCs en un fin de semana en mayo del 2000, el Gusano I love you, alias Love letter , infectó 3 Millones de PCs en un solo día. A partir de éste,aparecieron nuevos códigos maliciosos, fundamentalmente Gusanos que transformaron el modo de operación tradicional de los Programas Malignos.

Año 2002

Durante el año 2002 se mantuvieron en el Hit Parade Internacional de los Programas Malignos que mayor incidencias causan, muchos códigos maliciosos que aparecieron en el 2001 e incluso, en el 2000. Esta es una característica del año 2002.