Visitantes indeseables

ROBERTO PLA
Teniente coronel de Aviación
http://www.aire.org/
pla@aire.org

Hasta hace bien poco, cada viernes trece teníamos que soportar el aviso de los medios de comunicación sobre el supuesto peligro de un virus informático cuya incidencia dejó de ser preocupante hace años.

Sin embargo los virus informáticos y sus nuevos parientes los gusanos, se reproducen con mas energía que nunca. ¿Qué son y como funcionan estos visitantes indeseables?. Conocer la respuesta a esta pregunta es el primer paso para mantener nuestro ordenador a salvo de sus deletéreos efectos.

Un virus es un programa. Recibe este nombre sobre todo por su capacidad para producir copias de si mismo y extenderse de unas máquinas a otras provocando un efecto comparable al que produce una infección biológica en los seres vivos. Usualmente estos programas producen un efecto maligno, un daño en las maquinas en las cuales se reproducen y ejecutan. Estos daños pueden ser muy variados, desde la simple aparición de mensajes anunciando su presencia o el uso de tiempo de procesador y espacio en disco, hasta provocar graves daños en el equipo o la información que contiene.

Los gusanos se diferencian de los virus por su capacidad para extenderse a través de las redes informáticas, robando identidades para acceder a otras máquinas o usando el correo electrónico de la victima para extenderse.

Con la proliferación de los llamados 'lenguajes script' y la inclusión de diferentes mecanismos para ejecutar instrucciones desde páginas de hipertexto como las que se consultan en la web pero enviadas por correo, algunos virus y gusanos han alcanzado una notoriedad y difusión elevadísima en los últimos tiempos.

El caso de Melissa fue ampliamente difundido por tratarse de un virus que utilizaba las posibilidades de programación de los documentos de texto escritos con el programa Word de Microsoft, ILOVEYOU se enviaba por correo y usaba las características de automatización de Windows y más exactamente de un componente de instalación opcional el "Windows Script Host" un intérprete de lenguaje script. Aun cuando estos virus se hicieron famosos y se extendieron notablemente, otros programas malignos han conseguido en los últimos tiempos ocupar primeros puestos en la lista de principales enemigos públicos de nuestros ordenadores.

El virus del enanito es asombrosamente simple en su concepción y requiere que el usuario ejecute un programa adjunto al mensaje. A pesar de ello ha seguido extendiéndose por la red durante mas de un año.

Los usuarios ejecutan el programa adjunto porque el texto del mensaje les da a entender que se trata de una broma de carácter erótico.

El virus 'Chernobil' tiene entre sus terribles efectos destruir los primeros sectores de arranque del disco duro, con lo que no solo inutiliza la información sino que puede resultar difícil recuperar el disco así como borrar la BIOS. Este efecto es lo mas cerca que han llegado los virus de dañar el hardware. La BIOS es el programa que ejecuta el ordenador al conectarse y sin él, el PC es incapaz de arrancar. Estos programas vienen ahora en chips que son actualizables por software. El virus utiliza el mecanismo de actualización para borrar la BIOS, con el consiguiente trastorno ya que eso supone la mayor parte de las veces sustituir la placa base completa ya que no se venden BIOS sueltas.

Por último mencionar a un 'campeón del mal', el gusano 'SirCam'. Este gusano es una de las infecciones mas virulentas de los últimos tiempos. Al día siguiente de recibir el aviso del centro de alerta de virus, llegaban cuatro mensajes infectados a mi ordenador. Durante mas de una semana se mantuvo el nivel entre cuatro y seis mensajes diarios y aun hoy, cosa de un mes después siguen llegando uno o dos mensajes diarios con este virus. Los mensajes proceden muchas veces del ordenador de una persona conocida y su texto dice:

"Hola como estas?

Te mando este archivo para que me des tu punto de vista

Nos vemos pronto, gracias."

http://www.pandasoftware.es/ Panda Software. Fabricante de Platinum, el ganador absoluto de la comparativa 2001 de PC World USA

http://www.alerta-antivirus.es/ Ministerio de Ciencia y Tecnologia. Centro de Alerta Temprana sobre Virus Informáticos.

http://www.mcafeeb2b.com/international/spain/
Network Associates

http://www.hispasec.com/
Hispasec, portal Español de Seguridad con numerosos servicios

http://pp.terra.com.mx/~hugalde/virus.html
El Lado Obscuro del cUCHitril: Virus, Hackers y Crackers...

http://www.disa.mil/info/fs121999.html
Equipo de Respuesta a Emergencias Informáticas del Departamento de Defensa USA.

Eso puede hacernos creer que el archivo adjunto ha sido enviado realmente por nuestro conocido, e intentar abrirlo. Estos archivos llevan a veces una doble extensión. Si no hemos modificado la configuración de Windows la segunda extensión permanece oculta y se trata de una extensión de ejecutable: .exe, .com.pif o .bat. mientras la primera es una inocente .jpg . .doc. ... Una vez intentamos abrir el archivo, la infección se ha producido y el gusano continua su propagación hacia los ordenadores de nuestros amigos.

Como medidas de seguridad para protegernos, debemos seguir escrupulosamente las siguientes:

- Usar un antivirus de reconocido prestigio y actualizarlo frecuentemente.
- No ejecutar ningún archivo que nos llegue por correo electrónico ni aun los procedentes de personas de confianza sin haber confirmado su seguridad.
- Desinstalar el Windows Script Host de nuestro ordenador y el intérprete de VBScript, ya que seguramente podremos seguir viviendo , incluso mas tranquilos, sin esas utilidades dudosamente útiles.
- Controlar la ejecución de Macros en los documentos de Microsoft Office.
- Suscribirse a alguna lista o sistema de información sobre nuevos virus para tener conocimiento de las nuevas amenazas y desechar los falsos avisos de virus.

Siguiendo estas pequeñas reglas de seguridad nuestros problemas a causa de los virus decrecerán rápidamente al tiempo que nuestro entorno de trabajo se convertirá en un lugar mas seguro. ■

OTROS ENLACES

http://www.securityfocus.com/frames/index.html?focus=virus
SecurityFocus.com Portal de seguridad en inglés
http://www.svetlian.com/Seguridad/
Servidor con consejos, trucos y avisos de seguridad.
http://www.bysupport.cl/
Bysupport . Vendedor de Viruscan en Chile
http://ftp.azc.uam.mx/automcafee.html
Actualizaciones Automáticas para McAfee Viruscan versión 4.x
http://dsic.ucv.cl/Antivirus/pagproce/pagproce.htm
Instalacion de Mcafee Viruscan
http://www.itasa.com.mx/prods/fprot/soporte/temas/gustroy.html
Virus, Gusanos, Troyanos Y Puertas Traseras. Que son y que hacen.
http://www.ctsecurity.com/
C&T, Seguridad Informatica
http://www.terra.es/internet/articulo/html/int1653.htm
Articulo en Terra:Redes Vulnerables: Virus, Troyanos Y Gusanos
http://www.antivirus.com.mx/
Trend Micro
http://www.perantivirus.com/
Software peruano desarrollado por PER SYSTEMS
http://www.avp-es.com/
Antiviral Toolkit Pro
http://www.deepzone.org/editions/virgsm/virus&gsm.htm
Los Virus y la telefonía móvil: relación, mito y realidad
http://redtamaulipas.hypermart.net/antivirus/vacunas_contra_virus_irc.h tmSeguridad y vacunas en IRC
http://www.gfi.com/index_es.html
GFI, suministrador de software de seguridad de correo electrónico y redes
http://ortopedia.rediris.es/docus/dummies1.htm
Respuestas para Torpes sobre Seguridad Informática.