UNAM Mirada a la Ciencia
La **UNAM** presenta el quehacer de los científicos al alcance de nuestros lectores
www.unamiradaalaciencia.unam.mx

ATAQUES cibernéticos

LAS VÍCTIMAS SUELEN SER USUARIOS INGENUOS

"Twitter detecta infiltración de hackers. Un total de 250 mil nombres de usuarios y contraseñas fueron robados", revelaron medios de comunicación de todo el mundo hace unos días. Un ataque similar difundió *The New York Times* recientemente. El diario estadounidense acusó a hackers chinos de haber penetrado en sus redes informáticas y robar información confidencial.

Los ciberataques están a la orden del día. La recomendación es tener cuidado con lo que uno descarga en Internet, pues algún software malicioso puede instalarse en el equipo, paralizar sus funciones e inclusive, copiar datos personales sin notificar al usuario.

VIRUS, GUSANOS Y TROYANOS

Conforme los sistemas informáticos incorporan nuevos mecanismos de seguridad, los creadores de software malicioso contraatacan con métodos cada vez más sofisticados. Los más antiguos son los virus, los cuales tienen la capacidad de pegarse a un archivo o programa. Este modo de "infectar" recuerda el mecanismo de acción de los virus biológicos, los cuales se unen a las células y se reproducen en el organismo.

"Muchos usuarios de computadoras tienen la idea de que un virus se pega a un programa y lo que hace es borrar archivos, pero no es así; este concepto de lo que puede hacer un software malicioso ha evolucionado mucho desde sus orígenes en los años 80 hasta la época actual", precisa Rubén Aquino Luna, de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM.

El subdirector de Seguridad de la Información describe la diversidad de programas maliciosos que pueden infectar una computadora. Los gusanos tienen la propiedad de propagarse sin la intervención del usuario, ya que se instalan en los componentes automáticos de los sistemas operativos. Los caballos de Troya, o troyanos, pueden robar información o controlar un equipo.

"Los zombies se instalan en varios equipos y se quedan sin ejecutar ninguna acción; simplemente se conectan a un punto central de Internet, en donde esperan instrucciones, por ejemplo, de propagarse. La sofisticación de este software reside en que muchas veces no nos damos cuenta de que nuestra computadora, el teléfono celular o la tableta puede estar infectado."

Por lo general, los programas maliciosos buscan información en el disco duro, de la forma como el usuario navega en la red, y la recolectan en alguna parte de internet. A veces están diseñados para actúar en contra de toda una infraestructura, como sistemas de plantas nucleares y de redes eléctricas.

AMENAZA LATENTE

La instalación de virus, gusanos o troyanos ocurre cuando encuentran el ambiente propicio. Puede ser una vulnerabilidad en alguna red o sistema, asociada a un error en la configuración del sistema operativo o una aplicación.

Otro escenario es el engaño. El usuario recibe la publicidad de una empresa muy conocida sobre un nuevo antivirus capaz de brindar protección al 100%. También es común el envío de correos electrónicos con mensajes sensacionalistas, como la advertencia de un próximo terremoto. La descarga de este tipo de avisos es el principio de la propagación del software malicioso.

"Estas trampas y engaños, conocidos en la jerga de seguridad de la información como ingeniería social, no tienen que ver con algo técnico sino con la participación del usuario por ignorancia o ingenuidad", aclara el ingeniero Rubén Aquino.

Los antivirus son la principal herramienta disponible contra posibles infecciones. Actúan a través de firmas o patrones, es decir, revisan si algo extraño en el equipo coincide con las amenazas registradas en una base de datos; de ser así levantan una alerta. También detectan movimientos extraños en el equipo, como la ejecución de un programa sospechoso, con la ventaja de que sugieren al usuario mantenerlo en cuarentena.

En palabras del ingeniero Aquino, los ataques informáticos nunca se van a acabar porque hay diversos motivos para hacerlo y eso incluye a quién está detrás. "A veces tenemos la idea del adolescente jugando en su computadora en un cuarto oscuro y desordenado en alguna parte del mundo. Pero también puede haber componentes económicos y políticos, gobiernos y corporaciones involucrados."

En junio de 2012, el diario *Washington Post* publicó que Estados Unidos e Israel habían colaborado para crear el virus informático *Flame*, como parte de una estrategia para robar información sobre el programa nuclear de Irán.

MALDADES VIRTUALES

I love you hizo de las suyas en el año 2000, presentándose como una carta de amor en correo electrónico. Este gusano nació en Filipinas y colapsó equipos de todo el mundo. Causó daños estimados en millones de dólares.

Nimda se propagó desde China en 2001.

El objetivo de su creador fue impedir la conexión a Internet y luego tomar control del equipo infectado.

SQL Slammer/Zafiro es el virus que invadió archivos de todo el mundo en 2003. Afectó el servicio del 911 de Seattle y causó la cancelación de vuelos de Continental Airlines.

Texto: Claudia Juárez
Diseño: Adolfo González

Escríbenos a cienciaunam@unam.mx
o llámanos en el D.F. al 5622-7303

Dirección General de Divulgación de la Ciencia UNAM

Director General: Dr. José Franco,
Coordinador de Medios: Ángel Figueroa, Edición: Juan Tonda,
Asistente: Mariana Fuentes, Investigación: Xavier Criou,
Soporte Web: Aram Pichardo