CienciaUAT

ISSN: 2007-7521
cienciauat@uat.edu.mx
Universidad Autónoma de Tamaulipas
México

Mata Villalpando- Becerra, Isaac; Guevara-Juárez, Oscar Antonio
Virus informáticos, todo un caso, pero no perdido
CienciaUAT, vol. 4, núm. 4, abril-junio, 2010, pp. 56-61
Universidad Autónoma de Tamaulipas
Ciudad Victoria, México

ISSN 2007-7521. 4(4): 56-61 (Abr-Jun 2010)

Virus informáticos, TODO UN CASO, PERO NO PERDIDO

I.T. Isaac Mata Villalpando- Becerra*; coadministrador de correo electrónico, DGIT, UAT.
Oscar Antonio Guevara-Juárez; pasante de Ingeniería en Sistemas Computacionales, UAM Mante Centro, UAT.
*Autor responsable: it.isaac@hotmail.com

RESUMEN

El *malware* incluye *software* malicioso como los virus, gusanos y troyanos. Su gravedad va desde ser bromas hasta ataques que causan pérdida de información, daños en los equipos, denegación de servicios y cuantiosas pérdidas económicas. Tiene su origen en el comienzo de la computación a mediados del siglo XX, a lo largo de la historia el *malware* ha evolucionado aumentando en cantidad, gravedad, sofisticación, afectando a internet, a todas las plataformas y a los sistemas operativos, principalmente a Microsoft Windows debido a su gran popularidad y su carácter comercial. Para expandirse, el *malware* utiliza principalmente la ingeniería social (práctica de obtener información confidencial a través de la manipulación de las personas), la mensajería instantánea y las redes sociales. Llevando a la práctica métodos y atendiendo consejos de prevención es posible mitigar satisfactoriamente los riesgos.

PALABRAS CLAVE: *Malware,* prevención de *malware*, solución de incidentes por *Malware*.

ABSTRACT

Malware Malicious software includes viruses, worms and Trojans. Its severity ranges from jokes to be attacks that cause loss of data, equipment damage, denial of services and economic losses. It originated in the beginning of computing to mid-twentieth century, throughout history, the malware has evolved to grow in number, severity and sophistication, and affecting the Internet, to all platforms and all operating systems, mainly to Microsoft Windows because of its great popularity and commercial. To expand, the malware used primarily social engineering (practice of obtaining confidential information through the manipulation of people), instant messaging and social networks. Putting into practice methods and response prevention tips can successfully mitigate the risks.

KEY WORDS: malware, malware prevention, malware incidents solution.

INTRODUCCIÓN

En la actualidad es imposible concebir el mundo sin tecnologías de la información; éstas son necesarias para todas las actividades y para el desarrollo humano. Pero existe un riesgo que atenta contra la información, los equipos de cómputo y las telecomunicaciones: el *malware*. Éste aumenta en número, severidad, variedad y sofisticación, sin embargo, puede ser prevenible y mitigar sus efectos.

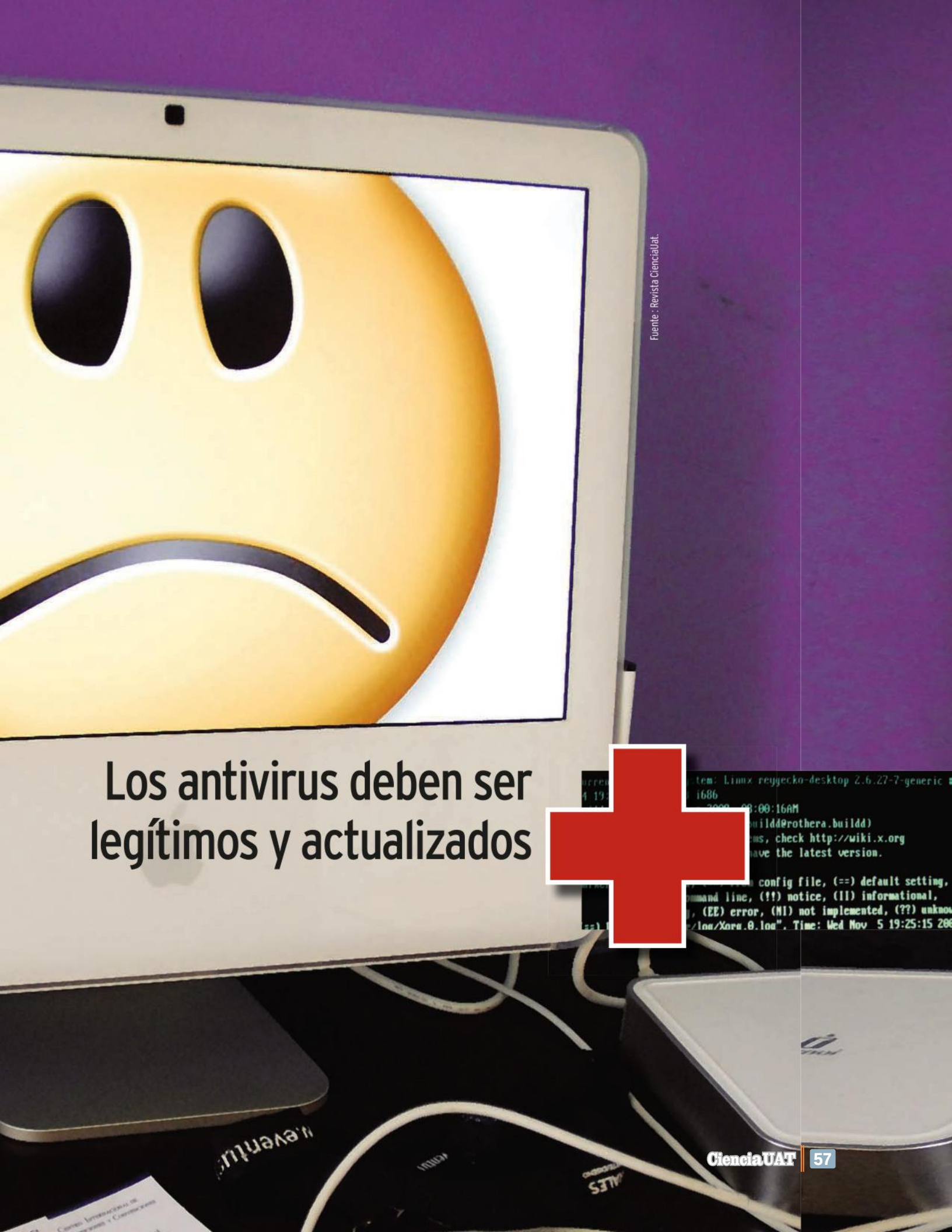
DESARROLLO

El impropio término "virus informático" es en la práctica utilizado para agrupar todos los tipos de *malware*. El *malware* incluye virus, gusanos, troyanos, *rootkits*, *spyware*, *adware*, *crimeware*, y *software* malicioso e indeseado (Wikipedia, 2009a; Microsoft, 2009a; Panda Security, 2010).

¿CUÁL ES EL DAÑO REAL?

Para comprender el daño que puede causar el *malware* analizamos los siguientes hechos.

Las hojas de cálculo con las que se lleva la contabilidad en un negocio son infectadas por un virus que cambia números al azar... ¿en realidad se cuenta con la contabilidad? Su empresa sufre un ataque de un virus de correo electrónico, recibe tantos que



Fuente : Revista CienciaUat.

Los antivirus deben ser legítimos y actualizados

Los virus no se difunden sin intervención humana

decide apagar temporalmente su servidor de *e mail* y por esto pierde un correo con un pedido urgente de su mejor cliente.

Está por terminar su tesis, el más pequeño de la casa instala un juego pirata que infecta su computadora, el virus borra el disco duro, incluida la tesis. Recibe por mensajería instantánea una supuesta fotografía que acepta, es un virus que envía documentos al azar, incluidos archivos confidenciales de su empresa a sus contactos, entre ellos a la competencia. Envía un informe infectado a varios de sus clientes... ¿seguirán confiando en usted y en su forma de hacer negocios? (Oldfield, 2001: 72).

¿QUÉ ES EL *MALWARE*? DEFINICIÓN, TIPOS Y CARACTERÍSTICAS

El *malware* es un tipo de programas malintencionados que pueden provocar daños en el equipo, en la información y en el *software*, también pueden hacer más lento el trabajo en red y utilizar el equipo para auto difundirse (Microsoft, 2009a). Desde el punto de vista de las telecomunicaciones, es el tipo de *software* cuya finalidad es interrumpir el correcto funcionamiento de la red y sus dispositivos (Cisco Systems, 2004: 1008).

Como se acaba de mencionar, el *malware* es *software*, por lo cual, son desarrollos intelectuales realizados por personas con amplios conocimientos en informática, computación y telecomunicaciones, con intenciones ya sean de bromas, de causar daño, ganar poder, obtener beneficio económico, y se les conoce como criminales informáticos o criminales electrónicos (Wikipedia, 2009a; Oldfield, 2001: 72; Microsoft, 2009a; Cisco Systems, 2004: 1008; Wikipedia, 2009b; Wikipedia, 2009c; Borghello, 2008b: 7; Wikipedia, 2010).

Un virus es un *software* que puede copiarse a sí mismo e infectar una computadora sin el permiso o conocimiento del usuario. Sólo puede expandirse de una computadora a otra, en forma de código ejecutable adjunto a un archivo, cuando su huésped entra en contacto con el programa objetivo, ya sea porque lo ejecutó mientras se utilizaban otros programas, lo envió por red o internet, o lo transportó en algún medio removible comúnmente un dispositivo portátil de almacenamiento (USB, por sus siglas en inglés). Su función es básicamente propagarse. Los virus de hoy en día aprovechan los servicios de red como el *world wide web* (www), el correo electrónico, la mensajería instantánea y la compartición de archivos para expandirse. Los virus infectan a medida que se transmiten y pueden dañar el *software*, el equipo y la información. Son de gravedad variable, pueden ser simples bromas o ser verdaderamente destructivos, dañando los sistemas o generando tráfico inútil que bloquea las redes. Un virus no se difunde sin intervención humana (Wikipedia, 2009a; Oldfield, 2001: 72; Microsoft, 2009a; Cisco Systems, 2004: 1008; Wikipedia, 2009b).

Un gusano (*worm*) es un programa que se propaga automáticamente de computadora a computadora, crean copias de sí mismos en la memoria, permitiéndole tomar el control para transferir información. Pueden aprovechar las vulnerabilidades del sistema para expandirse a otras computadoras sin necesidad de ser transferidos y no necesitan un portador, pueden crear túneles en los sistemas permitiendo que usuarios maliciosos tomen el control de los equipos de forma remota. Son muy peligrosos debido a su habilidad para replicarse exponencialmente con tal frecuencia que la máquina colapse o pueden enviarse por red o internet a infinidad de destinos provocando tráfico intenso, ocasionando retrasos, bloqueos o hasta colapsarlas (Wikipedia, 2009a; Oldfield, 2001: 72; Microsoft, 2009a; Cisco Systems, 2004: 1008).

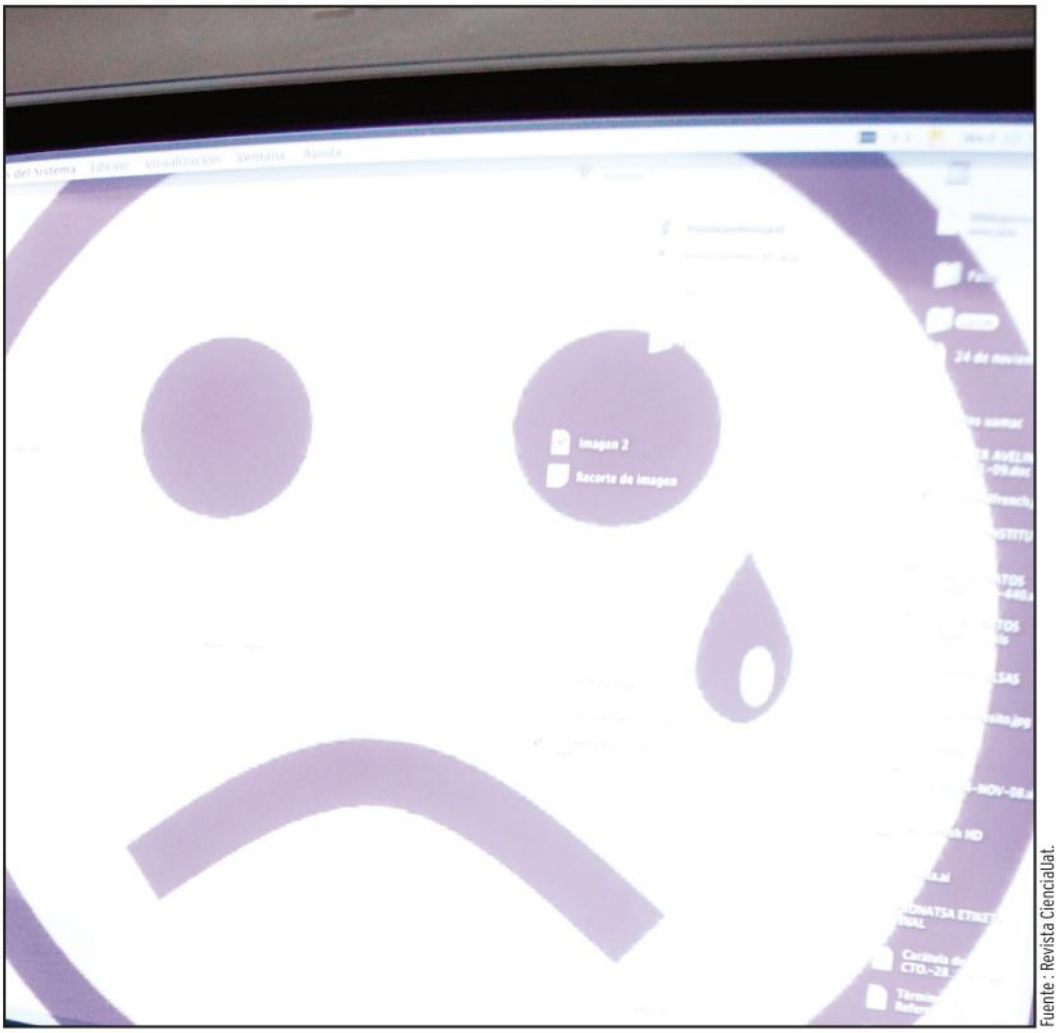
Un troyano (*trojan hourse*) es un programa que provoca daños y vulnera la seguridad. Se difunden engañando a los usuarios aparentando ser programas útiles y legítimos con la finalidad de recabar información o permitir el control remoto de la computadora para fines malintencionados (Wikipedia, 2009a; Oldfield, 2001: 72; Microsoft, 2009a; Wikipedia, 2009b; Wikipedia, 2009c).

BREVE HISTORIA Y CRONOLOGÍA DEL *MALWARE*

El origen del *malware* es precisamente el origen de la computación moderna y los inventos que han revolucionado la vida desde el siglo pasado. John Louis Von Neumann, de origen húngaro, en 1951 sienta los precedentes de la auto reproducción, con miles de aplicaciones en la ciencia, en el modelado y simulado de sistemas, tiene también una aplicación negativa: el *malware* (Oldfield, 2001: 72; Borghello, 2008a: 42). El físico y escritor de ciencia ficción Dr. Gregory Benford describió en mayo de 1970 el término "*computer virus*", y "*vaccine*" al programa para eliminarlo (Borghello, 2008a: 42).

El primer virus fue creado en 1972 por Robert Thomas Morris, capaz de infectar a computadoras IBM 360 difundiéndose a través de Arpanet (actual internet); fue llamado *Creeper*, mostraba el mensaje: "*I´m a creeper... catch me if you can!*". Para eliminarlo se creó el programa Reaper el cual se convirtió en el origen de los antivirus actuales (Wikipedia, 2009a; Borghello, 2008a: 42). El primer troyano fue desarrollado inadvertidamente en enero de 1975 por John Walker mientras buscaba cómo distribuir un juego, le llamó Animal/Pervade. A finales de los setenta en el Centro de Investigación Xerox en California, John Shoch y Jon Hupp, crearon un programa que se encargaría de tareas de mantenimiento y gestión automáticamente durante las noches al que llamaron *Worm*, se convirtió en un grave problema siendo el primer gusano de la historia (Borghello, 2008a: 42).

Elk Cloner, desarrollado en 1981 por Richard Skreta es el primer virus para computadoras *Apple* (Wikipedia, 2009a; Borghello, 2008a: 42). Como demostración, Leonard Adleman hace un virus que afecta a UNIX terminado el 10 de noviembre de 1983 (Borghello, 2008a: 42). El virus *Brain*, primero para PC y la primer epidemia detectada, desarrollado en 1986 por los hermanos Basit, Shahid y Amjad Farrq Alvi (Wikipedia, 2009a; Oldfield, 2001: 72; Borghello, 2008a: 42). El mismo año Ralf Burger creó Virdem, primer virus dañino; Bernt Fix lo desensambla y desarrolla un programa para neutralizarlo, convirtiéndose en el precursor de los actuales antivirus (Borghello, 2008a: 42). Creado por Artemus Barnoz y Boris Wanowitch, MacMag se convierte en el primer virus para computadoras Macintosh a finales de 1987. El 2 de noviembre de 1988 Robert Tappan Morris hace el primer gusano de reproducción masiva llamado *Gusano de Morris*. Infectó y colapsó a la Administración Nacional Aeronáutica y del Espacio (NASA, por sus siglas en inglés), al Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés) y el 10% de Arpanet durante 72 horas, convirtiéndose en el primer enjuiciado por desarrollar *malware*; explotaba una vulnerabilidad de UNIX en computadoras VAX y Sun Microsystems, siendo el primero en hacerlo. En octubre de 1989 aparece el peligroso *Datacrime*, lo que originó la venta de un programa anti *Datacrime* que se convirtió en el antecesor de los antivirus comer-



Fuente : Revista CienciaUat.

ciales (Borghello, 2008a: 42).

En 1994 Christopher Pile fue condenado en Inglaterra a 18 meses de prisión por haber fabricado los virus *Pathogen*, *Queeg* y *SMEG*; por primera vez en la historia un creador de *malware* es sentenciado (Borghello, 2008a: 42). En febrero de 1997 aparecen los virus *Staog* y Bliss para el sistema operativo Linux; Bliss también afectaba SunOS, Solaris y OpenBSD. En el 2001 aparecen los gusanos, *Ramen* y *Lion* que aprovechan múltiples vulnerabilidades en RPC, wuftpd y BIND de Linux (Borghello, 2008a: 42).

Malware para celulares y dispositivos móviles; Liberty, un troyano para el sistema operativo PalmOS aparece en el 2000; en el 2003 el gusano *Cabir* y el troyano *Brador* para Symbian y Windows CE, respectivamente. En 2005 CommWarrior para Symbian utiliza los mensajes multimedia para propagarse (Borghello, 2008a: 42).

El 43% del *phishing* intenta obtener información bancaria y está directamente ligado al 3.75% de los fraudes bancarios efectivos

Entre el *malware* más memorable está el gusano *CodeRed* (julio 2001), el troyano *Nimda* (septiembre 2001), los gusanos *Slammer* y *Blaster* (2003), el gusano *Sasser* (mayo 2004), el gusano *Conficher* (noviembre 2008). Entre los hechos más destacables recientes del *malware* está la utilización desde 2003 de *Botnets* (conjunto de computadoras conectadas a internet que han sido infectadas con un *malware* específico, permitiendo que una persona tenga control sobre ellas), el uso de la mensajería instantánea como medio de propagación desde 2007 y desde 2008, la explotación de las redes sociales (Borghello, 2008a: 42).

EL *MALWARE* Y LOS SISTEMAS OPERATIVOS

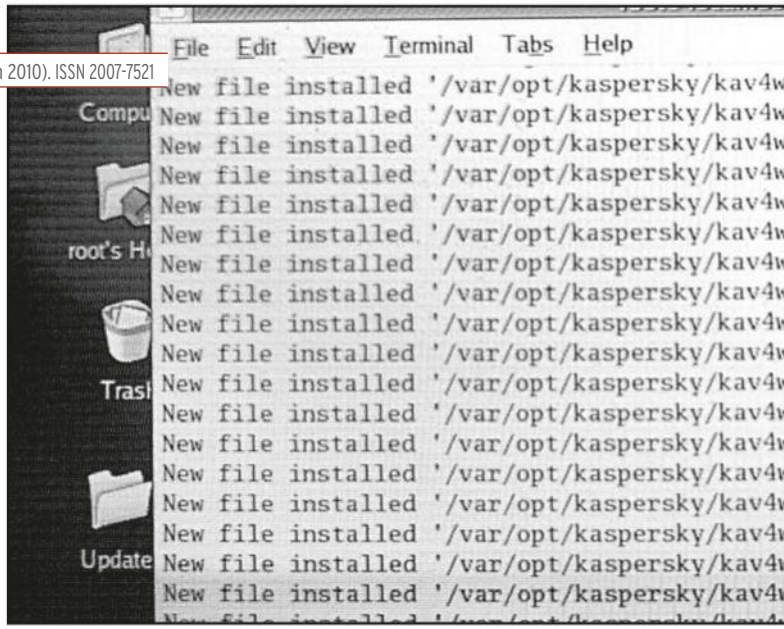
Como se puede apreciar, ninguna plataforma de *hardware* ni los sistemas operativos Windows, MacOS, Solaris, Linux, UNIX están exentos de estas amenazas (Wikipedia, 2009a; Wikipedia, 2009b; Borghello, 2008a: 42). Es sumamente fácil predecir que las plataformas que hoy en día no son tan populares serán blancos de mayores, graves y más complejos ataques al hacerse más populares y accesibles para el usuario final (Borghello, 2008a: 42).

Seguramente se cuestiona por qué el *malware* afecta principalmente a las PC y al sistema operativo Microsoft Windows; posee una gran popularidad, se estima que mayor al 90%, por lo que es codiciado para los creadores de *malware* por su alcance sumamente masivo y la retribución económica que esto significa. Es un sistema operativo comercial por lo cual busca siempre ser el primero, fácil de utilizar, y altamente compatible; llevándolo desde sus orígenes a tener múltiples puntos débiles, falta de seguridad, ser muy permisivo con la instalación de *software*, la fuertemente integración con el sistema operativo de *software* adicional como Internet Explorer y Outlook Express que adolecen de los mismos inconvenientes (Wikipedia, 2009a; Wikipedia, 2009b; Borghello, 2008a: 42).

Posiblemente el principal obstáculo para los creadores de *malware* para Macintosh, Linux, Solaris, UNIX es la capacitación de sus usuarios, ya que mantienen correctamente sus sistemas, por lo que la Ingeniería Social (práctica de obtener información personal confidencial a través de la manipulación de las personas, consta de *phishing* [correos y sitios fraudulentos], apear *phishing* [suplantar identidad para enviar correos en nombre de otros, más común en ambientes empresariales] y *email heoxes* [solicitudes de ayuda humanitaria, rescates y ofertas]), actualmente principal método de propagación, pudiera no tener efecto en ellos (Borghello, 2008a: 42; Microsoft, 2010b).

FORMAS DE INFECCIÓN

En la práctica, a excepción de los gusanos, casi todo el *malware* no le puede infectar a menos que usted abra o ejecute un programa infectado. El *malware* principalmente se difunde en archivos adjuntos de correo electrónico, en información



Poco más del 80% de correo electrónico es correo no deseado, cuyo objetivo es publicitario o intento de infección con *malware*

y programas descargados desde internet o a través de medios de almacenamiento como las memorias USB. Dentro de las técnicas usadas por el *malware* para lograr que un usuario ejecute su código se encuentran la ingeniería social (mensajes como ¡Ganó un premio! Ejecute este programa para..., etc.), la instalación de *software* ilegítimo, programas y contenidos autoejecutables, transferencia de archivos por mensajería instantánea y correo electrónico (Wikipedia, 2009a; Oldfield, 2001: 72; Microsoft, 2009a; Wikipedia, 2009b).

Las redes sociales se caracterizan por tener usuarios y relaciones entre ellos a través de internet. Existen infinidad de redes sociales como; *FaceBook, Twitter, MetroFlog, Fotolog, Flickr, MySpace, Live Spaces, Hi5, LinkedIn, Second Life, etc.* Por tratarse de usuarios que interactúan entre sí, a las amenazas ya conocidas en internet debe sumársele el gravísimo riesgo de comprometer la confidencialidad, privacidad, anonimato y la intimidad de los usuarios. Las redes sociales significan millones de usuarios con gran cantidad de información y dinero circulando en ellas; los perfiles de los usuarios y sus relaciones son información útil muy codiciada por los delincuentes para ser comercializada y explotarla con cualquier fin (Borghello, 2008b: 7).

Los peligros comprobados de las redes sociales incluyen códigos maliciosos, ataques a los perfiles de usuarios para robar su información, *malware* propagado a través de ellas, engaño a los usuarios, la utilización de reproductores vulnerables, *phishing* (conjunto de técnicas para obtener o "pescar" información personal sensible) en especial de cuentas bancarias, utilización de *scripts* para descargar archivos dañinos en las computadoras de los usuarios, hasta robo de dinero y objetos (Borghello, 2008b: 7). Todo lo anterior es especialmente grave debido a que la mayoría de los usuarios de las redes sociales son niños, adolescentes y jóvenes.

Existe *malware*, los gusanos, que actúan replicándose a través de las redes y las computadoras, se infectan sin la intervención de los usuarios aprovechando vulnerabilidades de los sistemas operativos, por lo que es muy importante descargar las actualizaciones y parches de seguridad (Wikipedia, 2009a; Wikipedia, 2009b; Oldfield, 2001: 72; Microsoft, 2009a; Cisco Systems, 2004: 1008).

ANTIVIRUS E INFECCIONES

En la actualidad es necesario utilizar *software* antivirus, son programas que intentan detectar y eliminar el *malware*, lo hacen comparando los archivos que examinan con las definiciones de las firmas de virus o mediante la utilización de técnicas heurísticas. Los usuarios deben tener actualizado su *software* (Wikipedia, 2009a; Oldfield, 2001: 72).

Como usuarios, al elegir un antivirus debemos fijarnos en el consumo de recursos, la velocidad de escaneo, veloz pero con escaneo de todos los archivos; la actualización entre más frecuente mejor, la detección de virus y las utilerías adicionales pudieran ayudarle en caso de una infección (Oldfield, 2001: 72; Ospino, 2007).

Para saber si su sistema operativo está infectado, observe si comienza a sufrir una serie de comportamientos anómalos o imprevistos. Si su equipo funciona con lentitud, se bloquea o reinicia lo más probable es que esté infectado por algún *malware*. A no ser que cuente con un *software* antivirus actualizado no existe un método infalible para saber si está infectado (Wikipedia, 2009b; Microsoft, 2009a; UNAM, 2010). Y si así fuera infectado, dependiendo de la severidad del *malware* existen formas de removerlo y métodos de recuperación, pero la única manera de seguir utilizando el equipo con toda seguridad y certeza es volviéndolo a instalar por completo (Wikipedia, 2009a; UNAM, 2010; Microsoft, 2010a). Recurra siempre con personal capacitado.

MÉTODOS Y CONSEJOS DE PREVENCIÓN

Nada ni nadie puede garantizar de manera absoluta la seguridad de su equipo; sin embargo, se pueden minimizar riesgos manteniendo el *software* actualizado (Microsoft, 2009a) y contando con un antivirus legítimo y actualizado; utilice también un *firewall* (Oldfield, 2001: 72; Microsoft, 2009a; Cisco Systems, 2004: 1008; Wikipedia, 2009b). Use el sentido común. Evite la instalación de *software* ilegítimo y evite descargarlo de internet (Cisco Systems, 2004: 1008; Wikipedia, 2009b). Evite utilizar medios de almacenamiento removibles, como las memorias USB, hasta que sean verificados (Cisco Systems, 2004: 1008; Cnice, 2008). No abra correos electrónicos que procedan de remitentes desconocidos, ni descargue el contenido adjunto aún de remitentes conocidos sino lo espera o no sabe exactamente qué es (Oldfield, 2001: 72; Cnice, 2008). Evite la publicidad invasiva que contenga mensajes llamativos, puede violar su privacidad e infectar con *malware* (Cnice, 2008). No descargue archivos transferidos vía mensajería instantánea sino lo espera o no sabe exactamente lo que es.

Actualice su sistema operativo utilizando el servicio de Windows Updates (Microsoft, 2009a; Microsoft, 2009b) o el respectivo a su sistema operativo. Escanee periódicamente el ordenador, utilice la herramienta de eliminación de *software* malintencionado de Microsoft Windows más reciente y su herramienta antivirus actualizada, cada quince días analice su computadora con un antivirus en línea (Cnice, 2008).

En la empresa, informe sobre los riesgos y haga conciencia sobre ellos. Mantenga además copias de seguridad tanto de la información como de los sistemas. También utilice servidores de seguridad, filtrado de contenido y *firewall* (Oldfield, 2001: 72; Microsoft, 2009a; Wikipedia, 2009b).

ESTADÍSTICAS, CURIOSIDADES Y ACTUALIDAD

Para ayudar a mostrar la magnitud del problema, de acuerdo a la Asociación Internacional de Seguridad

Fuente: Revista CienciaUat.

Informática (ICSA, por sus siglas en inglés) durante el año 2000, el 99% de las empresas en el mundo habían sufrido alguna infección y más de la mitad un desastre grave a causa del *malware*, lo que no ha tenido una tendencia a disminuir (Zipfel, 2002: 16). Hasta el 2001 el costo estimado de los ataques mediante *malware* era de 13.2 billones de dólares a nivel mundial (Zipfel, 2002: 16). De los cuales, los virus más costosos fueron LoveBug 8.75 billones de dólares, codeRed 2.62 billones, SirCam 1.15 billones, Nimda 635 millones (Zipfel, 2002: 16).

De acuerdo al *Computer Emergency Response Team* (CERT, por sus siglas en inglés) la cantidad de *malware* aumentó algo más del 50% del 2000 al 2001 (Zipfel, 2002: 16). Según un estudio realizado por la casa antivirus *Kaspersky Labs*. en septiembre de 2007 con una muestra de 5.9 millones de archivos infectados seleccionados al azar, al analizarlos por tipo 3.2% eran troyanos, 1.18% *backdoor,* 1% *downloaders*; al analizarlos por familias, el 9.15% fueron *agents* (SEI, 2009: 104). Otro estudio realizado por Enisa en noviembre de 2007, indica que el 65% del *malware* era *browser exploits,* mientras que el 13% eran adjuntos de correo electrónico (Lastein y Lin, 2009a: 18). De acuerdo a IBM el *malware* tipo *browser exploits* representaba poco más del 25% en 2005 y aumentó hasta representar casi el 60% para junio de 2008, en esta fecha el 47% afectaba a Mozzilla FireFox y el 33% a Microsoft Internet Explorer (Lanstein y Lin, 2009a: 18).

Se estima que al día se envían algo más de 100 millones de correos electrónicos (Borghello, 2009c). Poco más del 80% del correo electrónico es spam (correo no deseado cuyo objetivo es publicitario o tratar de infectar con *malware*) (SEI, 2009: 104; Borghello, 2009c). Aproximadamente un 80% del *spam* es enviado desde las máquinas de los usuarios (Borghello, 2009c). Conocer y hacer conciencia de estos números es importante para estar más protegidos a la hora de utilizar el sistema de mensajería, ya sea público o privado.

Como ya se explicó, desde el año 2003 se utilizan *botnets* (Borghello, 2008a: 42). Para tener una idea del poder que estas pueden llegar a representar, se estima que sólo con el tiempo ocioso del procesador de todos los usuarios de internet un controlador de esa utópica *botnet* podría enviar todo el *spam* y tomar el control del 25% de internet con un solo clic (Borghello, 2009c). Para crear un *botnet* es necesario infectar las computadoras objetivo con troyanos y gusanos, los puertos más utilizados en el funcionamiento de los *botnets* son el 6667 con el 35.1% y el 1863 con un 3.5% (Borghello, 2009c). *Srizbi* fue una de las mayores *botnets*; fue decodificada y controlada durante dos semanas por la empresa de seguridad *FireEye* y suprimida en noviembre de 2008 (Lanstein y Lin, 2009b: 12). Los *botnets* son un problema global que depende directamente de la buena educación de los usuarios de internet; lo más importante es contar con mecanismos de protección y usar internet y las redes con responsabilidad (Borghello, 2009c).

Otra de las amenazas relativamente reciente es el *phishing,* el cual es producido principalmente por medio de *malware*, *spam* y *botnets*. Es importante hacer conciencia pues 43% del *phishing* intenta información bancaria y está directamente ligado al 3.75% de los fraudes bancarios efectivos (SEI, 2008: 82).

Dos tercios de los usuarios de internet frecuentan redes sociales y *blogs*, y utilizan el 10% del tiempo para navegar en estos. Para darnos una idea del crecimiento que dichos sitios han tenido de abril de 2008 a abril de 2009 los usuarios de *Facebook* aumentaron un 700% y los de *Twitter* un 3,700% (SI, 2009). Esto es realmente importante considerando que las redes sociales si bien son buenas herramientas, también son demasiado peligrosas debido a la inconciencia sobre su uso y a que cada vez son más pretendidas por los delincuentes digitales.

CONCLUSIONES

El *malware* es muy diverso, aumenta con mucha rapidez, cada vez es más sofisticado y los daños que causa pueden llegar a ser muy graves, afectando a todas las plataformas físicas y a todos los sistemas operativos sin excepción; la prevención es lo más adecuado. Los antivirus son necesarios pero deben ser legítimos y estar actualizados. La mejor arma contra el *malware* es la información y concientización de los usuarios. Estos deben atender los consejos de prevención y acatar las políticas de seguridad de su empresa. En caso de infectarse con *malware* lo mejor es acudir con personal capacitado.

REFERENCIAS BIBLIOGRÁFICAS

Borghello, C. (2008a). *Cronología de los virus informáticos: La historia del malware*. Estados Unidos: ESET.

Borghello, C. (2008b). *Redes sociales utilizadas para propagar malware*. Estados Unidos: ESET.

Borghello, C. (2008c). *Botnets, redes organizadas para el crimen*. [En línea]. Estados Unidos: ESET. Disponible en: http://www.eset-la.com/threat-center/1573-botnets-redes-organizadas-crimen. Fecha de consulta: 23 de mayo de 2010.

Centro Nacional De Información y Comunicación Educativa. Cnice. (2008). *Consejos para evitar la infección virus informáticos*. [En línea]. República Dominicana. Disponible en: http://www.educando.edu.do/Portal.Base/Web/VerContenido.aspx?GUID=1bc1e829-b6c9-4515-b5d8-e0267a9dd661&ID=110541. Fecha de consulta: 1 de mayo de 2009.

Cisco Systems. (2004). *Guía del segundo* año *CCNA 3 y 4. 3a.* ed. Madrid: Pearson.

Lanstein, A. y Lin, P. (2009a). *Blocking the Covert channels used for malicious data theft*. Estados Unidos: FireEye Inc.

Lanstein, A. y Lin, P. (2009b). *New Ways to Detect These Malicious Web Infections*. Estados Unidos: ESET.

Microsoft. (2009a). *¿Qué son los virus, gusanos y troyanos?* [En línea] Disponible en: http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx. Fecha de consulta: 31 de marzo de 2009.

Microsoft. (2009b). *Actualización del software de Microsoft*. [En línea]. Disponible en: http://www.microsoft.com/latam/athome/security/update/msupdates.mspx#EYB. Fecha de consulta: 31 de marzo de 2009.

Microsoft. (2010a). Malicious Software Removal Tool. Disponible en: http://www.microsoft.com/security/malwareremove/default.aspx. Fecha de consulta: 29 de abril de 2010.

Microsoft. (2010b). "What is social engineering?" Disponible en: http://www.microsoft.com/protect/terms/socialengineering.aspx. Fecha de consulta: 21 de mayo de 2010.

Ospino, E. (2007). *Los antivirus ¿Qué debemos buscar en un buen antivirus?* [En línea]. Disponible en: http://foro.uptodown.com/showthread.php?t=49759. Fecha de consulta: 1 de mayo de 2009.

Oldfield, P. (2001). *Virus informáticos al descubierto*. Estados Unidos: Sophos Plc.

Panda Security. (2010). *Glosario*. [En línea]. Disponible en: http://www.pandasecurity.com/spain/homeusers/security-info/glossary/ Fecha de consulta: 29 de abril de 2010.

SANS Institute. SI. (2009). "*The Dark Side of Social Networking*", *en SANS OUCH!* 6(7):1-2.

Software Engineering Institute. SEI. (2008). *Cert Research annual report 2007*. Estados Unidos: Carnegie Mellon University.

Software Engineering Institute. SEI. (2009). *Cert Research annual report 2008* Estados Unidos: Carnegie Mellon University.

Universidad Nacional Autónoma de México. UNAM. (2010). *¿Qué es el malware?* México: Universidad Nacional Autónoma de México.

Wikipedia. (2009b). *Virus informático*. [En línea]. Disponible en: http://es.wikipedia.org/wiki/Virus_(computador). Fecha de consulta: 31 de marzo de 2009.

Wikipedia. (2009c). *Caballo de Troya*. [En línea]. Disponible en: http://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica). Fecha de consulta: 1 de mayo de 2009.

Wikipedia. (2009a). *Computer virus*. [En línea]. Disponible en: http://en.wikipedia.org/wiki/Computer_virus. Fecha de consulta: 31 de marzo de 2009.

Wikipedia. (2010). *Delito Informático*. [En línea]. Disponible en: http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico. Fecha de consulta: 29 de abril de 2010.

Zipfel, F. (2002). *Understanding the Virus Threat and Developing Effective Anti-Virus Policy*. Estados Unidos: SANS Institute.