COMUNICACIONES LIBRES

NOTICIAS DE LA AMC

Jesús Audelo González, Héctor Pérez Meana y Pedro Guevara López

Gusanos informáticos

Las tecnologías de la información y comunicaciones (TIC) dan soporte a las infraestructuras que sostienen a todos los países, los cuales se ven afectados al depender de las redes informáticas y de Internet para el desarrollo de su economía, sistemas de defensa militar, seguridad social, seguridad pública, sistemas de salud y otros sectores públicos y privados. Esto ocasiona que los sistemas informáticos siempre deban considerar el riesgo de sufrir ataques por parte de gusanos informáticos (WORMS) y de otros códigos maliciosos. Por ello, es de vital importancia tener la conciencia y el conocimiento de las repercusiones o impactos a nivel mundial que pueden desencadenar los ataques cibernéticos.

Introducción

Se conoce como *código malicioso* a todo aquel código que tiene como intención causar algún daño en un sistema de cómputo, ya sea de forma directa o indirecta; es decir, estos códigos pueden dañar directamente los sistemas, o bien hacer uso de la información que pueda estar almacenada o siendo utilizada en el equipo de cómputo. Existen diversos tipos de códigos maliciosos, pero los principales y más conocidos son: virus, adware, spyware, troyanos y gusanos.

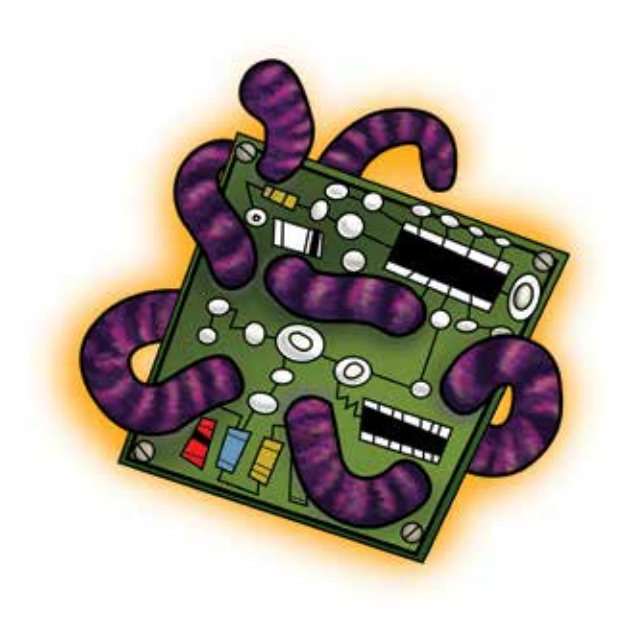
Cada uno de estos códigos maliciosos ejecuta diferentes acciones, o bien son ejecutados de diferente forma, que es lo que los caracteriza. Por un lado, los virus tienden a modificar o reemplazar archivos de sistema, sus daños pueden ir desde molestias al usar la computadora hasta destruir información. El adware tiene como objetivo principal mostrar publicidad específica, que puede aparecer al usar algún programa, sobre todo si se trata de versiones de prueba o evaluación. El spyware es un programa que puede recopilar cierta información contenida en algún equipo de cómputo, sin autorización del propietario; otra función que también puede ejecutar es la de redirigir las conexiones que realiza el equipo de cómputo.

Por su parte, los troyanos son programas que contienen en su código a otros programas, que suelen instalarse de manera conjunta cuando el usuario realiza lo que él considera una instalación común; sin embargo, al mismo tiempo se instala

en segundo plano un programa que tiene la capacidad de abrir puertas traseras, por las cuales es posible que se instalen más programas no deseados o se dañe la información contenida en un equipo de cómputo.

Finalmente, y motivo de este trabajo, están los conocidos como gusanos informáticos. Éstos son considerados entre los códigos con mayor peligrosidad, ya que como característica principal tienen la capacidad de propagarse por sí mismos; es decir, una vez que uno de estos códigos es liberado no requiere de la intervención humana nuevamente para seguir replicándose en otros equipos de cómputo. Además, utiliza las redes de comunicaciones, como Internet, para alcanzar su propósito. De ahí la relevancia y el énfasis que se le da a éstos.

El gusano *Morris* se considera como el primer gusano informático. Liberado en 1988, fue creado por Robert Tappan Morris, cuando era estudiante en la universidad de Cornell. Al parecer, la intención de este programa no era la de hacer daño, pero eso no fue lo que ocurrió. El gusano se dispersó con tal velocidad que colapsó muchos servidores de su época, causando daños en la Fuerza Aérea de los Estados Unidos y algunas universidades. A partir de entonces ha surgido una gran cantidad de sucesores que han causado muchos estragos en los sistemas de comunicación. Pero no sólo es el hecho del surgimiento de la gran variedad de gusanos, sino las técnicas que se han ido desarrollando para lograr que estos códigos maliciosos irrumpan en los sistemas informáticos.



Gusanos representativos por su afectación

En el año 2001, poco tiempo después de la presencia del gusano *Ramen*, apareció el gusano *li0n*; en un principio se creía que éste era una derivación del primero por la similitud con la que se llevaban a cabo sus procedimientos de propagación. El *li0n* fue desarrollado en China y atacaba principalmente a servidores Linux que corrieran el servidor de nombre BIND 8.1 –que es el servidor más popular usado por los sistemas basados en Unix–, que nuevamente tenía la vulnerabilidad de un desbordamiento de memoria. De este gusano se dieron tres variaciones, las cuales fueron muy similares entre sí, ya que compartían los principales componentes básicos: un escáner de puertos TCP, un programa (el Exploit) diseñado para explotar una vulnerabilidad, específica del BIND, y un conjunto de programas que se encargan de recolectar todos los demás componentes del gusano para hacerlo funcionar. La primera versión se descargaba de un servidor montado en FreeBSD, el cual es un sistema operativo multiusuario basado en UNIX, alojado en China. Las otras versiones usaban la misma estrategia usada por el gusano *Ramen*: recolectaban información de equipos previamente infectados, pero éstos comenzaban a realizar un escaneo de puertos en la red; el gusano generaba al azar un rango de direcciones para localizar a sus objetivos potenciales, y una vez que alguno respondía a la vulnerabilidad, éste lanzaba el Exploit BIND contra el objetivo. Si el ataque tenía éxito, el gusano se conectaba con el servidor para descargar los programas faltantes para ejecutarse y de nuevo realizaba dicho procedimiento para buscar nuevos objetivos.

En el mismo 2001 surgió el gusano *Cheese*, el cual fue considerado como un tropiezo en el ramo de los códigos de ataque autónomos (característica principal de los gusanos para propagarse por sí mismos). Éste pretendía eliminar los servicios ya antes instalados por el gusano *li0n*, que se encontraban en las rutas principales en donde está el compilador que ejecuta las órdenes escritas directamente en código máquina. La estructura de *Cheese* no era muy compleja, ya que sólo atacaba equipos con un puerto abierto que pudiera atacar, pero hacía evidente que las configuraciones en los servidores eran inseguras y muchas veces mal

Figura 1. El gusano *Sadmin* es uno de los más revolucionarios por usar una plataforma para propagarse y atacar otra plataforma. (Fuente: http://me.kaspersky.com/en/images/sadmind55-9432.gif).

realizadas, lo que daba como consecuencia equipos fáciles de infectar. Sin embargo, era sencillo que alguien lo pudiera manipular y volverlo muy peligroso. De ahí el llamado tropiezo.

De manera cronológica se tuvo también en el 2001 la aparición de otros gusanos importantes, como *sadmin/IIS*, *X.c. Telnetd* y *Adore*, en donde se podía apreciar que la constante seguían siendo los sistemas Linux, y ahora algunas versiones de Solaris –sistema operativo de SUN Microsystems– y servidores IIS –servidor web de Microsoft Windows–, aprovechando en algunos casos viejas vulnerabilidades que aún podían ser explotadas.

La lista de gusanos es enorme. Los que se mencionan en este trabajo son sólo algunos de los más importantes, pero no deben dejarse a un lado algunos otros, debido al impacto y la importancia que tuvieron: del año 1997, *mIRC Script.ini*; en 1999, *Melissa*; de 2001, *Love Letter*, 911, *Leaves*, *Code Red I*, *Code Red II* y *Nimda*; en 2002, *Apache*, MSN *Messenger*, *SQL Snake* y *Deloder*; en 2003, *Sapphire*. Para el año 2013 están los gusanos: *AutoIT.XY*, *AutoRun.CBP*, *DorkBot.HI*, *EmailWorm.00400f38d1*, *Worm.Java.AutoRun.c*, *Murkados* y *Gamarue.BB*, entre otros.

A partir de su surgimiento, o posiblemente a partir de que se dio a conocer el impacto que era posible alcanzar al aprovechar fallas y huecos de seguridad en los sistemas por medio de los gusanos, éstos comenzaron a tener un mayor auge. El impacto que han tenido a lo largo de su historia es enorme, tanto en el aspecto funcional de los sistemas como en el aspecto económico. Es en este último en donde se puede apreciar la magnitud de los daños causados. Por ejemplo, la empresa Mi2g publica el impacto económico causado por diversos gusanos (véase Tabla 1).

Todos estos gusanos son, sin duda, un ejemplo de las fallas de seguridad que los sistemas tienen. Algunos de ellos se valen de técnicas similares o con los mismos principios, y algunos otros utilizan nuevas técnicas; incluso existen los que atacan las mismas vulnerabilidades, pero en diferentes versiones de éstas. Otros utilizan las redes sociales, como los mensajeros instantáneos y de correo electrónico, aprovechando la vanidad de las personas: estos gusanos pueden enviar mensajes de remitentes falsos o con preguntas que harán que se abran correos ilícitos que tienen como objetivo de trasfondo el comprometer los equipos al ejecutar algún código que les dará acceso al sistema; toman el control del equipo o de la cuenta de correo para propagarse a los contatos de su libreta de direcciones. Además de esto, están los factores que los desarrolladores de los gusanos pueden usar a su favor, como pueden ser los servicios utilizados del sistema, debido a que presentan vulnerabilidades similares en diferentes versiones de sus aplicaciones (Arce, 2003; Song *et al.*, 2001; Moore *et al.*, 2003).

Primeras repercusiones en la economía global

El impacto que ha causado la evolución de las tecnologías de la información y comunicaciones (TIC) a

Tabla 1. Impacto económico causado por gusanos desde 1999 hasta 2003.

Gusano	*Año*	*Miles de millones de dólares anuales*
Melissa	1999	1.11
Love Bug	2000	8.75
Sir Cam	2001	2.27
Code Red	2001	2.62
Nimda	2001	0.68
Bugbear	2002	2.70
BadTrans	2002	0.68
Klez	2002	14.89
Slammer	2003	1.05
SoBig	2003	30.91

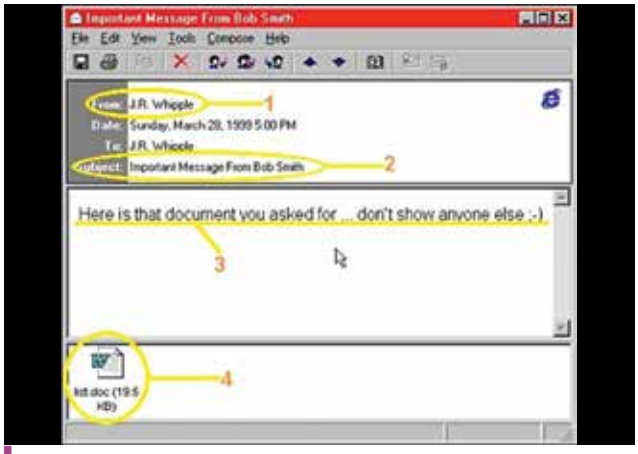


Figura 2. Mensaje enviado por el gusano *Melissa*. (Fuente: http://www.zdnet.com/ten-computer-viruses-that-changed-the-world_p4-3040093590/).

Figura 3. Mensaje enviado por el gusano *I love you,* el cual simulaba ser un mensaje legítimo. (Fuente: http://www.spywareremove.com/removeILoveYouWorm.html).

Figura 4. Mensaje con el que el gusano *Code RedA* sustituía la página principal de los servidores web. (Fuente: http://www.securelist.com/en/images/pictures/virus2/1098.gif).

nivel mundial y prácticamente en cualquier ámbito es algo eminente. Hoy día son indispensables para el desarrollo económico mundial y, en general, su evolución ha traído consigo una mayor productividad, lo que se ve reflejado en un aumento de ingresos per cápita, y a su vez desemboca en innovaciones, productos y servicios de mayor calidad.

El uso de las TIC forma una parte sumamente importante dentro de la columna vertebral de la economía moderna. El impacto que se genera cuando éstas se ven afectadas por alguna razón –principalmente en el flujo de información, cuando deja de circular– resulta en que gran parte de los sectores de la economía quedan vulnerables. Entre tales sectores están el financiero, de comercio, transporte y las industrias del sector manufacturero. De igual manera, se ven afectados los sectores de servicios públicos esenciales, como la medicina o la defensa nacional. Debido a la importancia de la información y al impacto que pueden llegar a generar en el ámbito socioeconómico, es necesario protegerlas de ataques cibernéticos que puedan vulnerar su integridad, confidencialidad y disponibilidad.

No existe metodología alguna que pueda indicar con precisión cuál es el impacto causado por los ataques cibernéticos de un gusano. Por otra parte, decir que se fue víctima de uno de estos códigos maliciosos tampoco es algo que el sector privado desee ventilar, ya que esto también repercutiría en su imagen. Por ello, los datos que se pueden llegar a obtener son resultado de análisis empíricos y basados en estimaciones de información recabada por medio de encuestas.

Esta información arroja que las pérdidas económicas unos días después de sufrir un ataque suelen ir de 1% hasta 5% del valor de las acciones. Un promedio estimado por The New York Stock Exchange menciona que estas cifras ascienden a un monto de entre 50 y 200 millones de dólares para los accionistas de empresas en Estados Unidos. Varias compañías de consultoría en seguridad informática han estimado que las pérdidas económicas a nivel mundial causadas por ataques atribuidos a virus y gusanos en el año 2003 oscilaron en los 13 000 millones de dólares. La Comisión Europea estima que más de un millón de personas son víctimas de algún crimen cibernético a diario en todo el mundo, lo que implica una pérdida aproximada de

750 000 millones de euros al año. En el reporte anual 2011 de la empresa Symantec, se anuncian pérdidas directas e indirectas a nivel mundial provocadas por ciberataques de alrededor de 388 000 millones de dólares.

Caso de los gusanos *Conficker* y *Stuxnet*

Los gusanos informáticos han tenido la característica de causar diferentes daños, aunque posiblemente en sus inicios no fuera esa su intención. A lo largo de la historia diversos gusanos han impactado seriamente tanto al gobierno como a la economía a nivel mundial. Un caso particular fue el gusano *Code Red*, que afectó directamente los equipos del Pentágono, un órgano sumamente importante para el departamento de defensa de Estados Unidos; su ataque colapsó los servidores web en julio de 2001, con un costo estimado de 2.6 miles de millones de dólares en pérdidas. Otro caso igualmente importante fue el del gusano *Nimda*, que en septiembre de 2001 colapsara millones de equipos que corrían el sistema operativo Windows en todo el mundo, al infectar servidores en Europa, Asia y Estados Unidos. En este último país se estimó una afectación a 130 000 computadoras, entre equipos personales y servidores.

Debido a su impacto no es posible dejar de mencionar al *Conficker*, un gusano que apareció en octubre de 2008. Entre los serios daños causados, se estiman a nivel mundial 12 millones de equipos infectados. Este gusano aprovecha algunas vulnerabilidades de equipos que corren los sistemas operativos de Windows, en sus versiones 2000, XP, Vista, Server 2003, Server 2008 y 7; *Conficker* desactiva ciertas características administrativas de los equipos, con lo cual evita su actualización e instalación de parches para resolver la vulnerabilidad. Además tiene la capacidad de controlarlos de forma remota, lo que convierte a los equipos infectados en equipos llamados "zombis". Los equipos que han sido infectados forman parte de lo que se conoce como una "botnet", la cual tiene la capacidad de controlar a todas esas máquinas para que lleven a cabo algún tipo de tarea; la más común es un ataque de denegación de servicios distribuido (DDos). Tales características le dieron a este gusano la capacidad a nivel mundial de afectar servicios de bancos, sistemas de telefonía, sistemas de seguridad, control de tráfico aéreo, sistemas de servicios médicos, y prácticamente cualquier infraestructura que corriera dichos sistemas operativos y tuviera conexión a Internet. Pero no obstante el daño causado por este gusano, existen tres variantes del mismo: *Conficker A*, *Conficker B* y *Conficker C*, con la misma capacidad destructiva.

Otro ejemplo del impacto causado por este gusano es el de marzo de 2009 en la aerolínea Southwest Airlines, que tras verse afectada, y ante la latencia de un impacto mayor, tuvo que tomar medidas precautorias para evitar errores en la asignación de vuelos y otros servicios que pudieran representar problemas más serios (Mills, 2009*a*). En general, se estimó que hasta el año 2009 las pérdidas ocasionadas por el gusano *Conficker* eran de alrededor de 9.1 miles de millones de dólares a nivel mundial (Danchev, 2009). De igual manera, este gusano infectó cientos de computadoras en hospitales, lo que provocó la falla de equipos de monitoreo de frecuencia cardiaca y de resonancia magnética, y ocasionó que fueran canceladas las citas de los pacientes que no fueran de extrema urgencia (Condon, 2009; Mills, 2009*b*).

El caso más reciente de un ataque informático perpetrado por un gusano es el conocido como *Stuxnet*. Éste fue liberado en el año 2010, e inmediatamente que se detectó fue clasificado como una amenaza crítica, ya que atacó directamente las estaciones nucleares de Irán, lo que afectó su programa de protección nuclear. Posteriormente, este gusano se detectó en la India e Indonesia, y además infectó decenas de miles de equipos alrededor de todo el mundo.

Se cree que fue diseñado para atacar equipos de la corporación Siemens, que es la infraestructura utilizada para controlar el enriquecimiento de uranio en plantas nucleares (Lee, 2011). Se trata de uno de los gusanos más sofisticados que se ha visto hasta el momento, está diseñado tanto para robar información industrial como para reprogramar procesos en sistemas industriales (que por lo general se usan para controlar plantas suministradoras de agua, plataformas petroleras y centrales eléctricas, entre otras más).

Este gusano va más allá de un ataque dirigido; en la literatura que se puede consultar al respecto, se especula una alianza de Estados Unidos e Israel para sabotear la posible construcción de armamento atómico por

parte de Irán. Sin embargo, la información que rodea a este poderoso gusano aún es difusa, ya que a pesar de los diferentes estudios que muestran firmas importantes de programas antivirus, como Symantec, Panda, McAfee, Kaspersky y Eset, respecto al gusano *Stuxnet* comentan diversas maneras en las que puede propagarse e incluso mencionan la participación de varias empresas. Entre ellas está Realtek Semiconductor (una de las más grandes de manufactura de componentes de computadora), ya que para que el gusano pasara desapercibido, éste debía contar con un certificado de dicha empresa, lo cual facilitó la forma en que se pudo ocultar y parecer parte de un programa válido, y de esa manera no ser detectado. Inclusive los programas que instala el gusano para realizar los cambios en los equipos infectados se ocultan de la misma manera. Además, se presume la existencia de otro certificado proveniente de la empresa Microsoft, con el cual el gusano contaría con dos certificados que le habrían permitido autenticarse como válido. Si bien estos detalles ya lo hacen por sí mismo efectivo para alcanzar su meta, a esto se debe agregar que su código contaba con cuatro vulnerabilidades llamadas "de día cero"; es decir que son fallas desconocidas de los sistemas operativos de los equipos, las cuales es posible explotar con las últimas actualizaciones, inclusive a pesar de contar con programas de protección como antivirus y firewalls. Parte muy importante para la efectividad del gusano *Stuxnet* es que tiene la capacidad de atacar sistemas basados en Unix y Windows NT, que son las principales plataformas en las cuales corren los sistemas SCADA (principal objetivo del gusano), por lo que su efectividad es muy alta; además de incluir diferentes programas que ejecutaría dependiendo de las condiciones en las que se encontraran estos sistemas.

Debido a todas estas características que reúne el gusano *Stuxnet*, se considera como parte de una nueva era en los ataques dirigidos.

Conclusiones

Es eminente el impacto a nivel mundial que genera el ataque de los gusanos informáticos. El simple hecho de saber que un país pueda atacar a otro país por medio de uno de estos códigos parecería un cuento de ciencia ficción; pero hoy día es una realidad que afecta de manera económica al propio desarrollo de los países debido a su gran dependencia en las TIC, que de manera irónica son algo indispensable para que la economía y el desarrollo como nación logren despuntar.

Estos tipos de ataques muestran la peligrosidad de los gusanos informáticos, pero sobre todo del impacto que pueden generar a nivel mundial, debido a que las TIC han ido evolucionando de tal manera que se encuentran inmersas en prácticamente todos los ámbitos socioeconómicos de cada país, y de ser atacadas, repercutirían directamente en la estructura de un Estado. Por ello es muy importante no sólo hacer conciencia de los problemas implícitos que puede conllevar el uso de las TIC, sino estar preparados para casos en los que puedan llegar a darse diferentes ataques por código malicioso, como los gusanos informáticos, para garantizar que éstos tengan las menores afectaciones y los servicios que puedan dejar de funcionar se restablezcan lo más pronto posible. Para eso es necesario desarrollar planes de respuesta a incidentes que contemplen la posibilidad de ser vulnerados por este tipo de amenazas.

Recomendaciones para el lector

A continuación se mencionan algunos consejos para tratar de minimizar la posibilidad de ser víctima de uno de estos códigos maliciosos.

Es importante considerar las ventajas que implica comprar programas originales, es decir, que contemos con las licencias adecuadas. En primera instancia, la del sistema operativo, ya que esto nos da acceso a las actualizaciones del sistema, que constantemente lanzan los parches que nos protegen de estos códigos. De igual manera se tiene que hacer con la paquetería que se instale a nuestros equipos, ya que también cuentan con esta serie de actualizaciones y en muchas de las ocasiones es a través de ellos que se puede ser más vulnerable.

En segundo lugar, tener un programa antivirus. Pero no sólo hay que instalarlo y esperar que éste nos proteja incondicionalmente, se debe hacer una buena elección, según las necesidades de cada usuario. Es importante familiarizarse con el programa, de tal manera que se tenga la capacidad de configurarlo de manera correcta para que realmente haga la función para la cual fue diseñado.

Y finalmente, resaltamos la concientización de los usuarios de los equipos de cómputo, la prevención al usar dispositivos portátiles como memorias, y en general cualquier dispositivo que tenga la capacidad de transferir información entre equipos. Es importante separar las actividades que puedan ser de trabajo de las de uso personal, con la finalidad de establecer relaciones de confianza, como en el caso del correo electrónico, ya que muchas de las amenazas aprovechan este medio debido a su gran uso y se puede ser víctima de la ingeniería social con la que son desarrollados muchos servicios de correo.

Jesús Audelo González cuenta con el título de Ingeniero en Computación y los grados de Maestro en Ciencias de Ingeniería en Microelectrónica y Doctor en Ciencias en Ingeniería en Comunicaciones y Electrónica, todos obtenidos en la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán, perteneciente al Instituto Politécnico Nacional. Actualmente labora en la Dirección General para Prevención de Delitos Cibernéticos de la Policía Federal. Su principal área de interés son los sistemas de seguridad informática.
jaudelo@ipn.mx

Héctor Pérez Meana recibió el título de Ingeniero Electrónico de la Universidad Autónoma Metropolitana, el grado de maestría de la Universidad de Electro-Comunicaciones de Tokio, Japón, y el grado de Doctor del Instituto Tecnológico de Tokio. Actualmente es Profesor Titular "C" en la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán del Instituto Politécnico Nacional. Es miembro de la Academia Mexicana de Ciencias y del Sistema Nacional de Investigadores, nivel II. Sus áreas de interés son el procesamiento de señales, el reconocimiento de patrones, la autenticación y protección de información, y temas afines.
hmperezm@ipn.mx

Pedro Guevara López cuenta con el título de Ingeniero Electricista y los grados de Maestro en Ciencias de la Computación y Doctor en Ciencias de la Computación, todos obtenidos en el Instituto Politécnico Nacional. Actualmente es profesor investigador de la Escuela Superior de Ingeniería Mecánica y Eléctrica. Sus áreas de interés son los sistemas en tiempo real, el modelado de sistemas dinámicos y sistemas embebidos.
pguevara@ipn.mx

Bibliografía

Arce, I. y E. Levy (2003), "An Analysis of the Slapper Worm," *IEEE Security and Privacy*, 1(1):82-87.

Condon, S. (2009), "Feds' red tape left medical devices infected with computer virus", *CNET News*. Disponible en: http://news.cnet.com/8301-1009_3-10232284-83.html?part=rss&subj=news&tag=2547-1_3-0-5, consultado el 2 de mayo de 2009.

Danchev, D. (2009), "Conficker's estimated economic cost? $9.1 billion", *ZD Net*. Disponible en: http://www.zdnet.com/article/confickers-estimated-economic-cost-9-1-billion/, consultado el 23 de abril de 2009.

Lee, R. (2011), "Stuxnet and the Paradigm Shift in Cyber Warfare", *Controlglobal*. Disponible en: http://www.controlglobal.com/articles/2011/stuxnet-paradigm-shift-in-cyberwarfare.html?page=1, consultado el 19 de mayo de 2009.

Mills, E. (2009*a*), "Conficker worm targets Southwest Airlines site", *CNET News*. Disponible en: http://news.cnet.com/8301-1009_3-10185639-83.html?part=rss&tag=feed&subj=News-Security, consultado el 2 de marzo de 2009.

Mills, E. (2009*b*), "Conficker infected critical hospital equipment, expert says", *CNET News*. Disponible en: http://news.cnet.com/8301-1009_3-10226448-83.html, consultado el 23 de abril de 2009.

Moore, D., V. Paxson, S. Savage *et al.* (2003), "The Spread of the Sapphire/Slammer Worm", *CAIDA*. Disponible en: http://www.caida.org/publications/papers/2003/sapphire/sapphire.html, consultado el 19 de mayo de 2015.

Song, D., R. Malan y R. Stone (2001), "A Snapshot of Global Worm Activity", *Laboratory for Advanced Systems Research*. Disponible en: http://www.lasr.cs.ucla.edu/classes/239_3.winter03/papers/snapshot_worm_activity.pdf, consultado el 9 de noviembre de 2001.