UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"TÉCNICAS DE PREVENCIÓN CONTRA CÓDIGO MALICIOSO PARA PC'S"

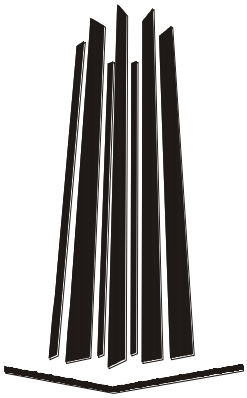
T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

MARISOL CHIQUITO RICO



ASESOR:

M. EN C. ERNESTO PEÑALOZA ROMERO

MÉXICO **2011**

Agradecimientos

A mi madre por su confianza y apoyo incondicional, por sus palabras de aliento que me han ayudado a sobreponerme en los momentos difíciles.

A mis hermanos que siempre me han dado ánimos para que me esfuerce y consiga lo que me propongo.

A mi asesor M. en C. Ernesto Peñaloza Romero por sus valiosos consejos y por el tiempo que invirtió en apoyarme para que concluyera el presente trabajo.

Índice

Introducción

La información es considerada uno de los recursos más valiosos para una organización, pero ésto no quiere decir que para las personas, que se encuentran en sus casas, no lo sea. La necesidad de proteger la información de terceras personas se hace cada día más indispensable.

Quienes manejen la información se preocupan de que ésta no sea robada, alterada, eliminada u observada por alguna persona no autorizada. Por estas y muchas más razones se debe de proporcionar protección y seguridad adecuada a la información para que se mantenga integra y disponible.

La finalidad de éste trabajo es proporcionar una idea general de las técnicas que pueden ser útiles contra el código malicioso, protegiendo el sistema de cómputo. Los puntos más sobresalientes, en términos generales, que se busca cubrir son:

- Explicar el valor que ha tenido, tiene y tendrá la información. Como ha cambiado la forma de transmitirla y sobre todo los riesgo que enfrenta al viajar en canales de comunicación inseguros (Internet).

- Describir los tipos de amenazas que podemos encontrar en la red, explicar algunas de las características más sobresalientes que ayuden a distinguirlas, así como las formas en que se pude infectar el sistema de cómputo.

- Definir que son los programas antivirus, como están formados y que técnicas utilizan para eliminar el código malicioso.

- Proporcionar algunas de las técnicas que pueden ser útiles en la prevención de código malicioso, destacando el papel tan importante que juegan los usuario.

A continuación se procede a describir como está conformado el trabajo, describiendo brevemente cada capítulo.

En el capítulo 1 se encuentran algunos de los motivos por los cuales es tan importante proteger la información, la necesidad de las personas por comunicarse juega uno de los principales papeles, originando un gran incremento de Internet. La red de redes hizo que la información viajara a grandes velocidades, enfrentándose a diferentes tipos de amenazas. Cada vez se hacen más evidentes los ataques que tienen como objetivo robar la información de los usuarios de Internet.

El capítulo 2 describe una gran gama de código malicioso: tipos de virus, gusanos, puertas traseras, caballos de Troya, etc. Cada uno de ellos cuenta con características principales que ayudan a distinguirlos entre sí, utilizan diferentes métodos de ataque. Entre los objetivos más comunes tenemos que buscan infectar los archivos del sistema, dañar los equipos, robar información personal, disminuir el rendimiento de la computadora o de la red, etc. Podremos darnos cuenta que desde hace décadas surgieron las primeras amenazas y como han cambiado con el paso de los años.

En el capítulo 3 se da una explicación de lo que son los antivirus informáticos, cómo están constituidos, cómo han tenido que cambiar sus métodos de detección a causa de la evolución del código malicioso. El por que su instalación en las computadoras no es un método infalible contra cualquier forma de código malicioso.

Para terminar, se presenta el capítulo 4 que proporciona una serie de medidas diseñadas para evitar que los sistemas de cómputo sean infectados frecuentemente. La diferencia que puede marcar un usuario informado sobre los peligros que corre su información, la utilización de los servicios de Internet en forma responsable, la implementación de políticas de seguridad, la utilización de

herramientas de software que ayuden a prevenir las infecciones, la utilización adecuada de los programas que vienen incluidos en el sistema operativo que se encuentra instalado en el equipo. Los beneficios y ventajas de proteger la información, equipos o redes.

Para terminar con el presente trabajo, se incluyen los puntos a los que se llegan tras la elaboración del mismo. Cada capítulo fue diseñado con la finalidad de informar y crear conciencia de las amenazas que pueden encontrar en la red, y de las cuales no serán capaces de protegerse, a menos que estén informados adecuadamente.

Capítulo 1

La información e Internet

En este capítulo se revisará, desde diferentes perspectivas, la importancia que representa la información en la vida de los seres humanos. También se dará un breve repaso de cómo ha cambiado la forma de transmitir la información.

1.1 Importancia de la información

La información se refiere al conjunto organizado de datos[1], los cuales constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que lo recibe. Por ejemplo, sí se organizan datos de un país, como son la cantidad de habitantes, extensión territorial, forma de gobierno, etc. y se escribe un libro con ellos, entonces, se puede decir que ese libro constituye una fuente de información de ese país. Para que la información pueda ser comunicable debe ser posible la interpretación de ésta.

"A diferencia de los animales, las personas puede manejar la información en sus cuatro estados: la adquieren, la almacenan, la organizan o la crean y la transmiten por medio de alguna tecnología. El lenguaje oral es un ejemplo de tecnología de la información, que utiliza el sentido del oído" [1]. La información puede ser adquirida con los cinco sentidos (vista, oído, olfato, tacto y gusto).

La información puede ser pública: cuando es visualizada por cualquier persona (por ejemplo, el número total de habitantes de un país); o privada: sólo puede ser visualizada por las personas que trabajan con ella (por ejemplo, el historial médico de un paciente).

[1] Es el antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho.

"Las características que definen la seguridad de la información son 4:" [1]

- Confidencialidad. Es la necesidad de que la información sólo sea conocida por personas autorizadas. Cuando la confidencialidad se compromete puede causar severos daños a su dueño, la información involucrada puede quedar obsoleta (por ejemplo, los planes de desarrollo de un nuevo producto llegan a manos de un empresa competidora y fabrican un producto con características similares al original).
- Integridad. Característica que hace que su contenido permanezca inalterado a menos que sea modificada por alguien autorizado. La falta de integridad puede estar dada por anomalías en el hardware, software, modificaciones por personas ajenas a ésta, etc.
- Autenticidad. Se refiere a que la información recibida sea confiable, que no origine confusión alguna.
- Disponibilidad. Es la capacidad de que la información este siempre disponible para ser procesada por las personas autorizadas. Se requiere que la misma se encuentre correctamente almacenada con el hardware y software funcionando perfectamente.

Cada una de estas características no tienen que estar vigentes simultáneamente, ni tienen la misma importancia en todas las circunstancias. Pueden haber ocasiones donde se requiera que la información sea autentica o que deba de ser primordialmente confidencial, como en el caso de competencia extrema.

1.2 La comunicación

Al ser humano le interesa la información, pero más aún la comunicación, que en realidad es una necesidad vital de nuestra especie. Habrá quien confunda la información con la comunicación, pero ambos conceptos son bastantes diferentes. La comunicación es el proceso durante el cual se transmite o comunica información a una o más personas, ésta no se ocupa del contenido que se transmite (la información) sino de la manera en que se lleva a cabo la transmisión.

Los primeros indicios de comunicación fueron los signos naturales (sonidos y gestos) que dieron origen al lenguaje, que es considerado el primer medio eficiente de transmitir la información que se ha adquirido mediante los sentidos.

La transmisión de la información empezó hace 100,000 años, cuando ya no era necesario que cada individuo redescubriera una y otra vez lo mismo, debido a que está podía ser transmitida de una generación a otra. Para conseguirlo se requería almacenarla en canciones, relatos o discursos, en la memoria de algunos individuos quienes la transmitirían a nuevas generaciones.

Cuando se inventa la escritura se dió un gran avance tecnológico cambiando la forma de transmitir y almacenar la información. Para llegar a este punto se tuvo que pasar por el arte rupestre de hace 31,000 años y los jeroglíficos egipcios que representaban sonidos o palabras, hasta la invención del alfabeto, el cual consiste en representar cada sonido mediante un símbolo.

Otro gran avance en la comunicación surgió en el siglo XV con la invención de la imprenta móvil, con ella se logró realizar copias de textos impresos en tela o papel.

Con el tiempo surgieron formas para codificar la información, por ejemplo el telégrafo, haciendo famoso el código Morse que emplea tres elementos (el pulso corto, el pulso largo y las pausas). Para la utilización de las computadoras también se implemento una forma de codificar la información y así poder almacenarla, transmitirla o procesarla. El código que se utiliza está formado por dos elementos el 0 y el 1, que representan el estado encendido y el estado apagado, éstos son utilizados para expresar cualquier texto, imagen, sonido o entidad aritmética.

La información almacenada o transmitida se encuentra en archivos, los cuales están formados por una secuencia de ceros y unos, permitiendo que los archivos

correspondientes se puedan almacenar en el disco duro de la computadora, en un disco flexible, etc.

Cada símbolo (un cero o un uno) es un bit y una secuencia de 8 bits se llama byte u octeto. Para representar un carácter (número o símbolo) su utiliza un octeto, haciendo posible codificar 256 caracteres distintos (mayúsculas, minúsculas, números y caracteres especiales).

En sus inicios las computadoras eran de propósito específico (la información procesada solamente era militar, del estado o científica), esto cambió después de la Segunda Guerra Mundial cuando se hicieron de propósito general. *"En 1981 IBM introduce la computadora personal (PC)"* [1], haciendo posible que las computadoras lleguen al hogar, oficina y escuelas. *"Según datos de Gartner el número de PC superó en el 2008 los mil millones de unidades en el mundo"* [2].

1.3 Internet

Internet es considerada una red de redes que utiliza el protocolo[2] TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet) para comunicarse. TCP/IP es un conjunto completo de protocolos diseñados para la interconexión de computadoras, independiente de su arquitectura y del sistema operativo que ejecuten, donde los dos más importantes son TCP e IP.

Como una de las características de TCP tenemos la garantía en la entrega de paquetes[3]. Cundo la computadora A envía un paquete a la computadora B, A espera la confirmación de que B recibió el paquete. Si después de un lapso de tiempo especifico A no recibe la confirmación de B, A reenviará el paquete. Para

[2] Conjunto de reglas usadas por las computadoras para comunicarse unas con otras a través de una red.
[3] La unidad de datos que se envía a través de una red la cual se compone de un conjunto de bits que viajan juntos.

que los datos puedan ser transferidos a la aplicación correspondiente, B debe de esperar todos los paquetes, si se pierde uno, será reenviado por A y si los paquetes llegan desordenados B los ordenara antes de pasarlos a la aplicación (Fig. 1.1).

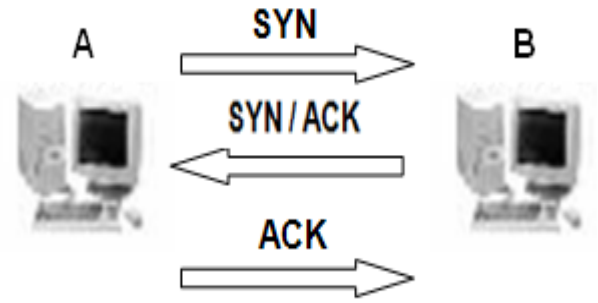


Fig. 1.1 TCP / Conexión en tres pasos.

El Protocolo IP se encarga de repartir los paquetes de información enviados entre la computadora local y los equipos remotos. Para conseguir su objetivo IP etiqueta cada paquete con información adicional, entre la que se encuentra la dirección IP de las dos computadoras. Con esta información IP garantiza que los datos recorran la red hasta su destino (que puede estar en cualquier parte de mundo), donde habrá ocasiones que el camino seleccionado sea el más corto, esto se logra con la utilización de unos dispositivos denominados encaminadores o routers.

Internet tiene sus orígenes en 1969 cuando la Agencia de Proyectos para Investigación Avanzada (Advanced Research Projects Agency en inglés ó ARPA) del Departamento de Defensa de los Estados Unidos conectó cuatro sistemas de cómputo, formando una red que se conoció como ARPAnet. La idea principal era que la información llegara a su destino aunque parte de la red estuviera destruida.

"En los ochentas, Internet incluyó a instituciones educativas, agencias gubernamentales, organizaciones comerciales, etc., logrando ampliar su alcance." [1] En la actualidad ofrece muchos servicios, entre los que se encuentran: el correo electrónico, la transferencia de archivo, acceso a sistemas remotos, conferencias interactivas, grupos de noticias y acceso a World Wide Web.

Con la llegada de Internet aumentaron los beneficios en término de un mayor acceso a la información, pero también incremento los riesgos que ésta corre. Debido a que la información que viaja por Internet debe de pasar por muchas computadoras y redes interconectadas para llegar a su destino.

Para darse una idea del rápido crecimiento de Internet, se muestran las siguientes dos imágenes que tan sólo varían cuatro años. En la figura 1.2 podemos observar muchas ramificaciones que van de un punto a otro, a diferencia de la figura 1.3, donde ya no son visibles los puntos de conexiones.

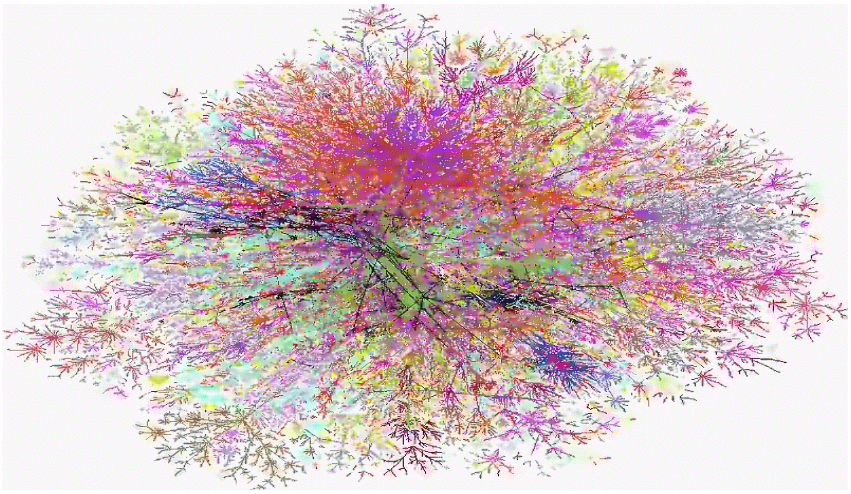


Fig. 1.2 Internet en 1998

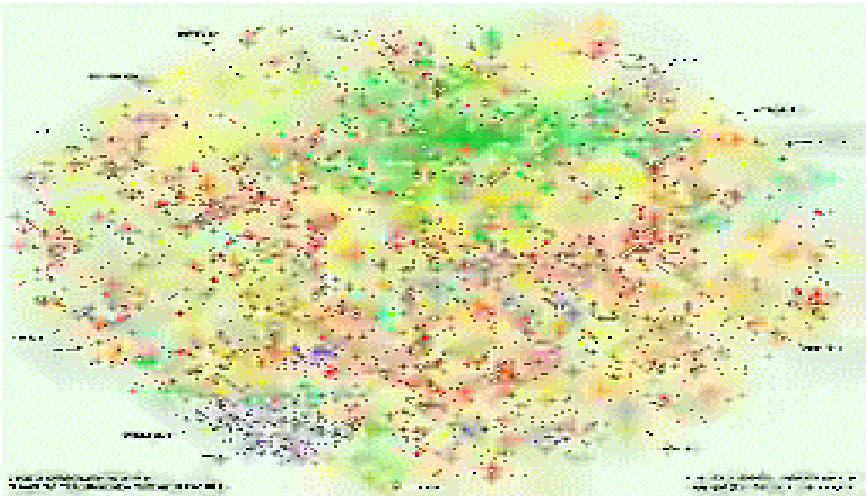


Fig. 1.3 Internet en el 2002

1.4 Tipos de amenazas

Antes de continuar, se explicará que un sistema de cómputo no son sólo los equipos, sino además, la colección de programas[4], medios de almacenamiento, datos o información, y personas involucradas. Los principales activos o recursos que se tiene que proteger en el sistema de cómputo son: los programas, los equipos y los datos.

Para que una circunstancia se ha considerada como amenaza debe de tener el potencial suficiente para causar perdida o daño al sistema. *"Existen cuatro tipos de amenazas principales a los sistemas que explotan las vulnerabilidades de los activos en el sistema. Estas amenazas son: interrupción, intercepción, modificación y fabricación"* [3].

En la ***interrupción*** el activo del sistema se pierde, quedando inutilizable o no disponible. Como ejemplo tenemos la eliminación de un programa o archivo de datos, la destrucción intencional o no de un dispositivo de hardware. Por otro lado, la ***intercepción*** se refiere a que una persona, proceso u otro sistema de cómputo logre el acceso no autorizado al sistema (por ejemplo, el copiado ilícito de un programa o archivo).

Cuando un intruso puede cambiar los datos en una base de datos[5], alterar un programa para que realice alguna acción ajena a su funcionamiento original, modificar datos en una comunicación, entre otras acciones, se considera una amenaza por ***modificación***, ya que el intruso es capaz de manipular los activos.

Por último, tenemos la ***fabricación*** que es cuando se consigue un objeto muy similar al atacado, de forma que sea difícil de distinguirlos entre sí. Retomando el ejemplo anterior de la base datos, con la fabricación, el número de registros aumentará.

[4] Es un conjunto detallado y explicito de instrucciones de computadora para realizar algún trabajo.
[5] Es un conjunto de datos relacionados y almacenados sistemáticamente para su posterior uso.

En la figura 1.4 se pueden observar los tipos de amenazas, donde (A) representa el origen de los datos, (B) el receptor y (I) es el atacante. En el flujo normal, A envía los datos a B, estos llegan sin haber sufrido pérdidas, alteraciones o que el atacante haya tenido acceso a ellos.

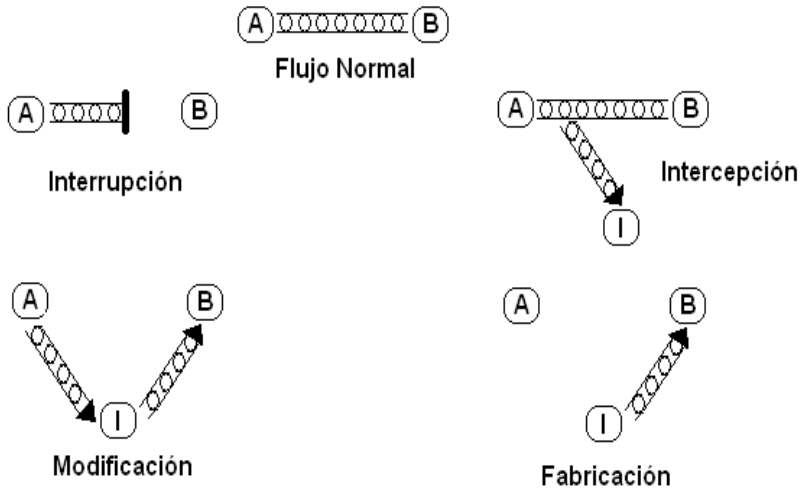


Fig. 1.4 Tipos de amenazas

Uno de los principales activos que se ven modificados por una infección de código malicioso (programas diseñados para dañar el sistema de cómputo) son los programas.

1.5 ¿De quién y de qué se protege la información?

Existen personas que se dedican a buscar la forma de entrar a un sistema, pueden crear programas que les ayude manipular o dañar los recursos de la computadora. Son conocidas con diferentes nombres dependiendo de los objetivos que tengan y el daño que ocasionen al sistema.

A continuación se presentan algunos de los nombres más utilizados para nombrar a estas personas:

- Hackers: se referirse a un programador astuto que siempre está en una continua búsqueda de información, vive para aprender y todo para él es un reto.

- Crackers: es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos.

- Script kiddies: no tienen buenas habilidades técnicas, atacan usando programas hechos por otros y generan grandes problemas.

- Pirata informático: cualquiera que piratea un programa, es decir, que lo copia sin permiso del autor.

- Atacante: entidad que realiza un ataque. La entidad puede ser una persona, cualquier proceso, computadora o dispositivo. En caso de que el atacante sea una persona o grupo de personas, a veces son llamados delincuentes o criminales informáticos.

Entre la gran variedad de programas que pueden crear, tenemos a los virus informáticos (son programas que se pueden introducir en las computadoras y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables).

El tema de los virus informáticos podrá parecer reciente, pero ya tienen algunas décadas. El interés que se tiene en ellos se debe al rumbo que han seguido, pasando de poner inofensivos letreros en la pantalla a la destrucción, modificación y robo de la información del equipo, entre algunas cosas.

Algunos de los programas conocidos como código malicioso fueron creados con la intención de mejorar el rendimiento de las computadoras, por ejemplo los gusanos (son programas similares a un virus que, a diferencia de éste, realiza copias de sí mismo, o de partes de él). Sus creadores publicaron el artículo “The Worm Programs” [4] en 1982. La idea era crear estos gusanos para mejorar los servicios de mantenimiento y atención de los equipos de cómputo (este tema será revisado más a detalle en el siguiente capítulo).

Los problemas que origina el código malicioso se agravaron con la llegada de Internet y su gran incremento de usuarios, el medio de infección más popular era el disquete y ahora han aumentado las vías de propagación, entre las más comunes se encuentra el correo electrónico.

Inicialmente algunos de sus creadores les interesaba la fama que obtenían cuando irrumpían en un sistema, originando caos en la empresa. Ahora les interesa más no ser detectados para poder cumplir sus objetivos, entre los más comunes se encuentra el robo de información.

Cuando la información robada es acerca del producto de una compañía, es considerado espionaje industrial, es utilizada para obtener una ventaja competitiva o ganancia financiera. *"En ocasiones el atacante va directo a las finanzas de la compañía: facturas, números de cuentas de clientes, cualquier cosa que pueda obtener y que le produzca dinero"* [5].

El énfasis que se hace en proteger la información se debe a que la pérdida de ésta no sólo afectara a una empresa, sino a los clientes o usuarios que tienen derecho a mantener su privacidad. Un claro ejemplo es la venta de datos oficiales de instituciones del gobierno, "*como son el Instituto Federal Electoral (IFE), Registro Federal de Contribuyentes, etc. Y las empresas privadas no se salvan, ya que se pueden encontrar en Internet páginas web donde venden bases de datos de los usuarios de compañías como Telcel, Bancomer, Banamex, etc"* [6].

Este tipo de problemas se hacen más comunes en las empresas mexicanas, *"las cuales registraron desde el 2009 un incremento en ataques relacionados con el robo de información de acuerdo a la Encuesta Global de Seguridad de la Información de Ernst & Young"* [7].

Un atacante, en la actualidad, busca robar poco dinero de muchos usuarios, en lugar de un gran golpe que puede resultar más difícil. ¿Quiénes son esos

usuarios? Todos aquellos de hogares o negocios que no se den cuenta de la dimensión del problema, hasta que lo estén viviendo.

En México el principal lugar de acceso a Internet es el hogar y el 31% de los usuarios utilizan las redes sociales, según un estudio realizado por la Asociación Mexicana de Internet (AMIPCI) titulado Estudio de Hábitos de Usuarios de Internet 2010.

"Las dos principales redes sociales más vulnerables son FaceBook y Twitter"[8], donde la segunda ha tenido serios problemas con *"La Comisión Federal de Comercio (FTC) de los Estados Unidos quien la ha penalizado por sus fallas de seguridad que permitieron que el año pasado piratas informáticos irrumpieran en las cuentas de sus usuarios"*[9].

Además de la pérdida de información, el código malicioso puede hacer que el atacante manipule nuestro equipo y que éste pase a formar parte de una red controlada por una persona, quien puede encontrase al otro lado del mundo.

Los ataques de este tipo son muy frecuentes, es muy difícil encontrar a los responsables, éstos logran controlar a millones de computadoras que suelen estar dispersas en diferentes países.

El hecho de que las computadoras se encuentren en diferentes partes del mundo complica la posibilidad de rastrear a los atacantes. Esto se debe a que cuando un usuario utiliza los recursos de Internet, no se está conectando realmente a Internet, sino a una red que pertenece a un Proveedor de Servicios de Internet (ISP), cuya columna dorsal está conectada a otras redes, una de las cuales es Internet. Entonces se habla de involucrar a diferentes redes conectadas entre ellas, y además las autoridades correspondientes deben de localizar la o las computadoras que controlan la red completa (Fig. 1.5).

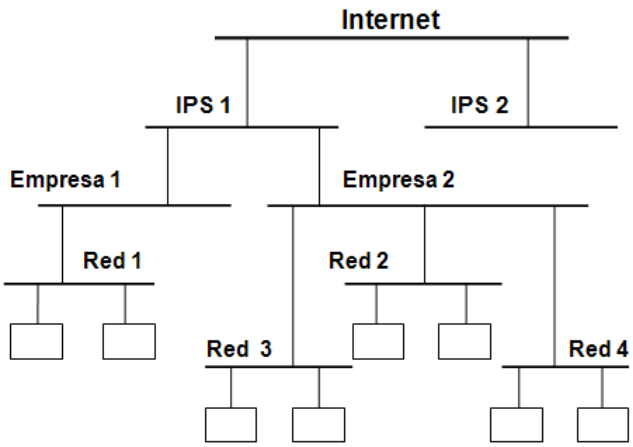


Fig. 1.5 Diagrama básico de conexión a Internet

A pesar de los esfuerzos realizados por las empresas, no estarán a salvo de sufrir alguna infección en sus sistemas, dado que muchos creadores de virus y gusanos tiene gran éxito utilizando la “ingeniería social” para propagar sus amenazas.

El término ingeniería social se refiere a las formas “no técnicas” que permiten usar puntos débiles en los sistemas. El atacante, generalmente cuenta con la experiencia necesaria para crear algún código malicioso que le permita manipular a las personas, convenciéndolas de que ejecuten acciones que normalmente no realizan y así revelen la información que éste necesita.

Una de las herramientas de defensa contra el código malicioso (malware) que más se utiliza es el antivirus que es un software que posee la función de detectarlo, su nombre está relacionado con los virus informáticos, pero actualmente son soluciones antimalware, capaces de detectar gusanos, virus, etc.

Hay muchas marcas de software antivirus (éste término será revisado a detalle en el capítulo 3), la mayoría tienen como función: detectar una amenaza, detenerla, identificarla por su tipo y nombre, prevenir o eliminarla del sistema. Previene la infección cuando un código malicioso es detectado al momento de intentar entrar al sistema. Lo elimina o desinfecta cuando se descubre que el sistema ya está infectado.

El método principal que utilizan los antivirus para detectar amenazas es por su “firma”. Cuando se dice que un antivirus está actualizado, se refiere a que se han mandado a las computadoras de los usuarios las firmas de los virus más recientes.

En los capítulos siguientes se explicará más a detalle los tipos de amenazas y las formas de prevenirlas.

Referencias Capítulo 1

[1] Daltabuit Godás Enrique, Hernández Hernández Leobardo. “La Seguridad de la Información”, 2007. LIMUSA.

[2] Firma de análisis Gartner, publicado en “Notici@scadadía on-line”. Miércoles 25 de Junio, sección de Tecnología. Disponible en http://www.noticiascadadia.com/noticia/13815-el-numero-de-pcs-en-uso-en-todo-el-mundo-supera-ya-los-mil-millones-de-unidades/. Leído el 12 Noviembre del 2010.

[3] Charles P. Pfleeger, Shari Lawrence Pfleeger. “Security in Computing”. 4at, edición. Octubre 2006. Prentice Hall.

[4] John F. Shoch y John A. Hupp, The Worm Programs –Early Experience with a Distributed Computation, ACM, 1982. Leído viernes 2 de julio 2010.

[5] Bogdan Dumitru, CTO de BitDefender, publicado en “El Universal on-line”. Lunes 13 de octubre del 2008, sección Computación. Disponible en: http://www.eluniversal.com.mx/articulos/50000.html.

[6] María de la Luz González, publicado en “El Universal on-line”. Miércoles 21 de Abril del 2010. Disponible en: http://www.eluniversal.com.mx/nacion/177168.html.

[7] Ricardo Lira, gerente de la firma Ernst &Young, publicado en “El Economista on-line”. Jueves 3 de Junio del 2010. Disponible en: http://eleconomista.com.mx/industrias/2010/06/03/desprotegidas-50-las-empresas-mexico-ey.

[8] Juan Portilla, director general de la empresa Symantec, publicado en “El Universal on-line”. Viernes 15 de enero del 2010, sección de Finanzas. Disponible en: http://www.eluniversal.com.mx/finanzas/76643.html.

[9] Gabriela Villareal, “La FTC obliga a Twitter a mejorar sus métodos de protección de la privacidad de sus usuarios”. http://www.viruslist.com/sp/news?id=208274580

[10] Javier Ulises Santillán Arenas, “Ingeniería Social, Técnica de Ataque Eficaz en Contra de la Seguridad Informática”. Disponible en: http://revista.seguridad.unam.mx/rs_unam_03/003_02/art_02.html

Capítulo 2

Código Malicioso

Cuando se utiliza una computadora se desea que funcione de forma correcta, sobre todo cuando se tiene algo urgente que hacer o entregar. Imaginemos que en ese preciso momento el equipo está demasiado lento o el programa solicitado no se visualiza en el escritorio, aún peor, la computadora no enciende, y no se sabe el motivo por el cual se encuentra en ese estado. Para tratar de evitar, la frecuencia, de este tipo de situaciones inesperadas, se necesita estar mejor informado sobre el uso adecuado del sistema de cómputo. Todos estos contratiempos no aparecen mágicamente, se deben a atacantes que buscan obtener algún beneficio. Algunos de los motivos más comunes son: venganzas por ofensas, enriquecimiento rápido, por razones políticas, obtener lugares preferenciales en las noticias, etc.

En este capítulo se explicará, de forma general, qué es el código malicioso y una forma en la que se puede clasificar. Para poder entender más a fondo el código malicioso revisaremos como han surgido nuevas formas de infección, desde sus inicios hasta la actualidad.

2.1 ¿Qué es el código malicioso?

El código malicioso (malware[6]) es un programa diseñado para dañar el sistema de cómputo. El atacante se introduce al sistema explotando cualquier debilidad que le permita infiltrase y pasar el mayor tiempo posible desapercibido, con el fin de robar información, dañar los archivos ó algún otro motivo. Una de las debilidades más comunes que el atacante utiliza es la ignorancia o curiosidad de los usuarios.

Por ejemplo un usuario que en su tiempo libre consulta su correo electrónico, se encuentra con un mensaje que tiene un título que llama su atención y lo abre, sin tomar en cuenta quién lo envió, el contenido puede ser breve y llamativo con la intención de que el usuario descargue el archivo adjunto que supuestamente le

[6] Acrónimo, en ingles, de las palabras “malicious” y “software”

proporcionará la información completa. Este archivo puede contener algún tipo de código malicioso que se instalará en el sistema y el usuario simplemente no se dará cuenta. Este es un ejemplo de la gran cantidad de formas en que se puede infectar el sistema.

Los atacantes son personas que buscan tener algún benéfico o simplemente por ocio. Hay quienes creen que el código malicioso es diseñado por las empresas que ofrecen soluciones de antivirus (este término será explicado en el siguiente capítulo). *"Según Rubén Bayud, ingeniero en sistemas de la filial mexicana de la empresa Trend Micro, hacer antivirus o crear algún gusano no es negocio"* [7].

El código malicioso se comporta de forma inesperada. Puede hacer cualquier cosa, como escribir un mensaje en la pantalla de la computadora, detener un programa en ejecución, generar un sonido o borrar un archivo almacenado en el disco duro.

Para el segundo semestre del 2008 México contaba con una tasa de infección por código malicioso del 77% y a nivel mundial *"16 de cada mil computadoras fueron limpiadas de código malicioso"* [8], es importante tomar conciencia de los riesgos que originan, la rapidez con que se propagan y la incapacidad que se tiene para evitar todos los incidentes.

Todos los programas informáticos creados para realizar acciones ilegales o perjudícales son considerados código malicioso, no sólo se habla de destrucción de datos o inhabilitar sistemas de cómputo, sino de pérdidas económicas, robo de información, bromas, negación de servicios, como es el acceso a internet, al correo electrónico, etc.

Las empresas utilizan con más frecuencia el correo electrónico, sitios web[7], bases de datos con cuentas de crédito de usuarios, transacciones electrónicas, etc. Estos acontecimientos le proporcionan al atacante mayor ventaja para crear programas maliciosos o combinaciones de estos, e intentar obtener algún beneficio. Imagine el caso de una empresa financiera que es atacada con algún tipo de código malicioso y su atacante logra entrar al sistema, robándose los números de cuenta de los usuarios, la pérdida evidente es económica, pero además se verá afectada la confianza de los clientes en la empresa.

Existen organizaciones que emiten notificaciones de nuevas forma de código malicioso, vulnerabilidades en los sistemas operativos o programas, así como también de nuevas actualizaciones y manuales para mantener el sistema de cómputo más seguro.

Algunos de los servicios mencionados anteriormente los podemos encontrar en UNAM/CERT (Equipo de respuesta a Incidentes de Seguridad en Cómputo). Donde un *incidente* es cualquier cosa que pueda causar algún daño a la organización, afectando o interrumpiendo su operación.

El esfuerzo por detectar los incidentes lo antes posible, detener la propagación, prevenir mayores daños al sistema, concientizar al usuario, la mitigación de vulnerabilidades, la instalación de las actualizaciones de los programas y la utilización de un antivirus que este actualizado, pueden ayudar a una organización a proteger sus activos o recursos (programas, equipos y datos).

[7] Punto de la red con una dirección única y al que pueden acceder los usuarios para obtener información. Normalmente un sitio web dispone de un conjunto de páginas organizadas a partir de una página principal, e integra archivos de varios tipos, tales como sonidos, fotografías, o aplicaciones interactivas de consulta (formularios).

2.2 Tipos de código malicioso

No existe una clasificación formal del código malicioso, con mucha frecuencia se encuentran combinaciones y cada día surgen nuevas forma de atacar. La clasificación puede hacerse de diferentes formas. Se pueden tomar criterios basados en la técnica de programación utilizada o en la clase de resultados que se obtienen.

La siguiente clasificación del código malicioso está compuesta de varios criterios, los cuales son: la forma en que se propagan, sus objetivos y cómo funcionan (en términos generales).

- Virus
- Puertas traseras
- Caballo de Troya
- Gusanos
- Programas Espía
- Adware
- Engaños
- Spam
- Phishing
- Pharming

2.2.1 Virus

El nombre de virus informático, dado a este tipo de programas, surge de las analogías que se pueden hacer con los virus biológicos. Por un lado tenemos a los virus biológicos, que son fragmentos de ADN[8] (virus animal) o ARN[9] (virus vegetal) cubierto de una capa proteica. Se reproducen únicamente en el interior de células vivas, tomando el control de sus enzimas y metabolismo. Sin el cual son tan inertes como cualquier macromolécula[10].

[8] Ácido desoxirribonucleico
[9] Ácido ribonucleico
[10] Molécula de gran tamaño. Término utilizado para designar moléculas de proteínas, ácidos nucleicos y otras moléculas voluminosas.

Y por otro lado tenemos a los virus informáticos, que son programas o una sección de programa de computadora que puede formar parte de un programa ejecutable u otro archivo, capaz de ejecutar instrucciones. Cuando un virus se reproduce, el virus resultante puede ser igual al original.

Como ejemplo de estas similitudes que existen entre estos dos tipos de virus tenemos: un virus biológico se intercala dentro del código genético de las células a las que infecta y crea duplicados de sí mismo para propagar la infección, de la misma manera un virus informático se intercala dentro del código de los programas y crea también duplicados de sí mismo para infectarlos. Ambos virus causan modificaciones y/o daños sobre sus huéspedes.

Al igual que los virus biológicos, cada espacie de virus informático actúa de manera distinta, lo que dificulta su detección. Y por esta razón los virus pueden pasar un largo tiempo dentro de su huésped.

En el resto del documento se manejará el término de virus, para referirnos a este tipo de código malicioso.

Los virus son conocidos como programas dañinos. Pero el Dr. Vesselin Bontchev[11], dice que un virus puede ser dañino o no dependiendo del ambiente en el que se encuentre, esto incluye la máquina, sistema operativo, las aplicaciones, otros programas instalados y el usuario mismo.

Casi siempre los virus son escritos para dañar un ambiente en específico. Los atacantes suelen diseñar un mayor número de virus para Windows, ya que es un sistema muy común, utilizado por la mayoría de usuarios y el cual presenta una cantidad considerable de vulnerabilidades. Cuando se habla de una vulnerabilidad se refiere a cualquier debilidad que pueda explotarse para causar pérdida o daño al sistema.

[11]Dr. Vesselin Bontchev nació en Varna, Bulgaria. Se graduó en la Universidad Técnica de Sofía en 1985 con una maestría en ciencias de la computación

2.2.1.1 Partes de un virus

Los virus están compuestos de tres partes, la primera de ellas es la que distingue a un virus de los demás tipos de código malicioso. A continuación serán explicadas:

- **Infección**: es la manera o maneras en que se propaga el virus. Esta es una de las características claves que definen a un virus.
- **Disparador:** es un mecanismo que define el momento en que será activado el efecto dañino.
- **Carga útil:** también conocido como "Playload", contiene el código del virus que determina el objetivo a dañar, este puede ser desde la aparición de un mensaje en la pantalla o la eliminación de archivos del equipo, hasta inhabilitar completamente el acceso al sistema. El daño causado puede ser intencional, como se describió anteriormente, o accidental, esto llega a suceder si el código del virus tiene errores de programación.

2.2.1.2 Clasificación de los virus

Existen distintas formas de clasificar a los virus, entre la más comunes podemos encontrar las que se basan en los componentes de la computadora que pueden infectar, ya sean programas o unidades lógicas del disco, o por las estrategias utilizadas para ocultarse de los usuarios y de los programas antivirus. En este documento los virus son asignados de acuerdo a la primera clasificación, antes mencionada.

Virus de Sector de Arranque

Cuando se enciende o reinicia una computadora el BIOS[12] se ejecuta; luego se lee y ejecuta el primer sector físico del disco inicio (disco duro, disquete, etc.), dependiendo de los parámetros de configuración del BIOS, y le pasa el control a este sector. Los virus de sector de arranque se aprovechan de la secuencia de encendido.

[12] Basic Input Output System

En el caso de un disco duro, ese primer sector es el MBR[13], es un pequeño programa escrito en lenguaje ensamblador, está ubicado en el *Cilindro 0 cabeza 0 Sector 1***.** Este programa buscará en la tabla de particiones la partición (contenida dentro del MBR) lista para arrancar el equipo. Cuando la encuentra, pasa del disco a la memoria el sector de arranque de ésta, le da el control a éste para que proceda a cargar y ejecutar el sistema operativo[14].

Los virus de este tipo infectan un equipo cuando éste se inicia con un disquete infectado. El virus se carga cuando se lee y ejecuta el sector de arranque del disquete, antes de cargar el S.O., se mostrará en la pantalla el siguiente mensaje "Non-system disk or disk error" y con esto el disco duro estará infectado.

Una vez que el virus infecta el MBR se carga en la memoria, a esperar que se introduzca un disquete para escribir su código vírico, en lugar del código original, en el sector de arranque (ésta es la única forma de infectar un disquete).

Para el caso de los discos duros, existen tres formas diferentes de que sean infectados por un virus de arranque, las cuales se explican a continuación:

1. El virus sustituye el código de arranque original del disco por una versión propia, guardando el original en otra parte del disco (Fig. 2.1); en ocasiones marca este lugar como defectuoso, para protegerlo de posibles accesos, esto suelen hacerlo algunos virus que no crean una rutina propia de arranque, por lo que una vez residentes en memoria, efectúan una llamada al código de arranque original, para iniciar el sistema y así aparentar que se ha iniciado con normalidad. Como ejemplo tenemos a el virus *Michelangelo*, cuando infecta un equipo mueve el MBR localizado en *Cilindro 0 cabeza 0 Sector 1* al *Cilindro 0 cabeza 0 Sector 7.*

[13] Master Boot Record, conocido también como “Registro de Inicio Principal”
[14] Es el conjunto de programas que permiten interactuar al usuario con los recursos de un sistema de cómputo.

2. El virus sobrescribe una parte del MBR sin afectar la tabla de particiones, porqué necesita de ella para localizar la partición activa y continuar con la secuencia.
3. En este caso el virus modifica las entradas de la tabla de particiones, en el momento que el MBR busca la partición activa, el virus puede asegurarse de que al cargar el sector de arranque también él sea inicializado. Así, el sector de arranque quedará infectado por el virus (Fig. 2.2).

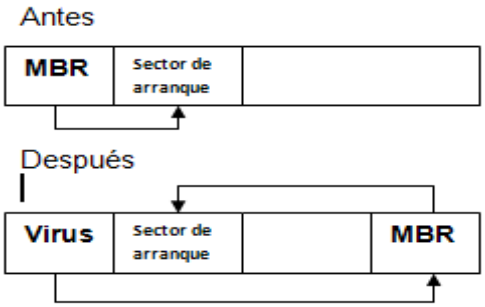


Fig. 2.1 Virus en el MBR (caso 1)

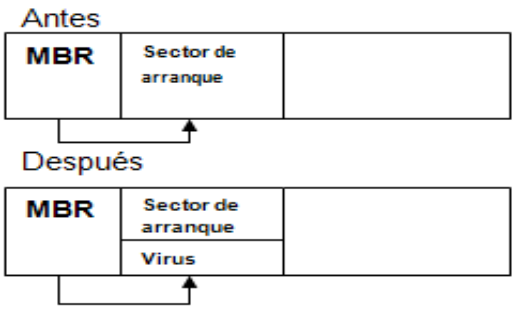


Fig. 2.2 Virus en el MBR (caso 3)

Virus de Archivo

Un virus puede afectar de diferentes formas un archivo, entre las más comunes tenemos: los que infectan archivos ejecutables (por ejemplo, .exe, .com, .bat), los que crean copias de los archivo, etc.

Para infectar los archivos ejecutables, existen varios métodos. Algunos virus insertan una copia de sí mismo antes de la primera instrucción del archivo (**virus anexados al inicio**). De esta forma, todas las instrucciones del virus se ejecutan en primer lugar, después de la última instrucción del virus, se pasa el control a la primera instrucción del archivo ejecutable para que realice su función. Los creadores de estos virus no se preocupan por saber algo de los archivos que serán infectados, ya que estos simplemente son portadores del virus.

Otra forma, es cuando el **virus se anexa al final** del archivo a infectar. El virus modifica el archivo, en el momento que éste es ejecutado, se pasa el control a las instrucciones contenidas en el código del virus. Los archivos con extensiones

.com y .exe utilizan diferentes secuencias de órdenes que le dicen a la computadora sobre el punto de entrada (las posiciones de memoria donde comienza la ejecución del código informático) del programa, entonces el virus puede modificar estos datos, apuntado a su propio código y ejecutarlo, después salta a la ubicación de inicio original (Fig. 2.3).

Los **virus que rodean** los archivos tienen el control antes y después de su ejecución. Para lograrlo se coloca el encabezado del virus en la parte delantera del archivo y se anexa el código del virus hasta el final (Fig. 2.4). El programa original se reconstruye como un nuevo archivo en el disco duro para que después tenga una correcta ejecución. Esta técnica es utilizada por algunos virus que infectan archivos PE[15] utilizados en versiones de Windows.

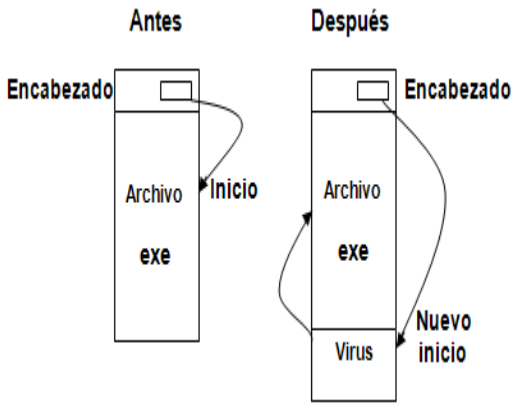


Fig. 2.3 Virus anexado al final

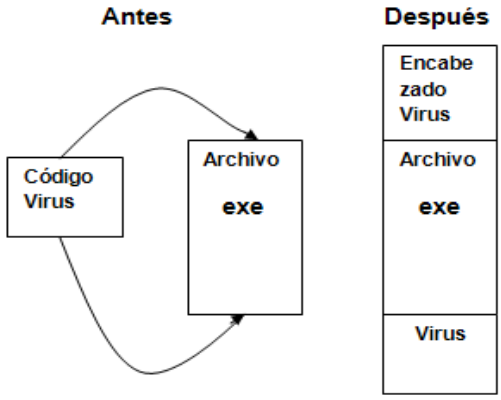


Fig. 2.4 Virus que rodean

Así como los métodos, antes descritos, no impiden el funcionamiento de los archivos ejecutables, existen otros que los dejan inutilizables. Por ejemplo, los virus de sobreescritura, estos reemplazan al código del archivo infectado con el suyo propio, borrando el código original. El archivo se vuelve inservible y no puede ser restaurado.

[15] Los archivos Ejecutables Portátiles de Windows (PE por sus siglas en inglés) son simplemente archivos ejecutables que funcionan en todos los sistemas operativos de Microsoft de 32-bit.

Para terminar esta categoría revisaremos los **virus acompañantes**, los cuales no modifican al archivo anfitrión. En su lugar, crean un archivo duplicado que contiene el virus. El virus puede ponerse en la ruta de búsqueda, con el mismo nombre de archivo destino, de modo que el virus se ejecutará en primer lugar cuando se intente ejecutar el archivo original.

Tomaremos como ejemplo el funcionamiento del sistema MS-DOS[16], cuando se quiere ejecutar un archivo y no se coloca la extensión de éste, MS-DOS busca primero el archivo con extensión .com, luego .exe y después .bat. Los virus se aprovechan de esta secuencia, en el momento que encuentran un archivo con extensión .exe crean otro de igual nombre y en el mismo lugar, pero con extensión .com que incluye el código del virus.

Virus Macro

Hay aplicaciones que permiten a los archivos de datos, como procesador de texto, manejar “macros”. Una macro es un pequeño pedazo de código escrito en un lenguaje que suele ser interpretado[17] por la aplicación y son utilizadas para realizar tareas repetitivas o complejas.

Cuando se trabaja con algún archivo, la aplicación realiza varias acciones: abre el archivo, lo guarda, lo imprime, cierra, etc. Para realizar estas acciones se necesita de una plantilla (macro global) que utiliza el programa para crear y abrir archivos. Si la plantilla está infectada, cada documento que se crea o se abre con esa plantilla también será infectado (Fig. 2.5), ya que el virus es activado cuando se ejecuta la macro. Estos virus no dependen del S.O. que tenga el equipo, sino de la aplicación que utilice el archivo.

[16] MicroSoft Disk Operating System, Sistema operativo de disco de Microsoft.
[17] Un intérprete toma la primera instrucción, la verifica, la enlaza y la ejecuta. Cada que es ejecutado revisará el código. Al final no se dispone de un programa que se pueda ejecutar sin él.

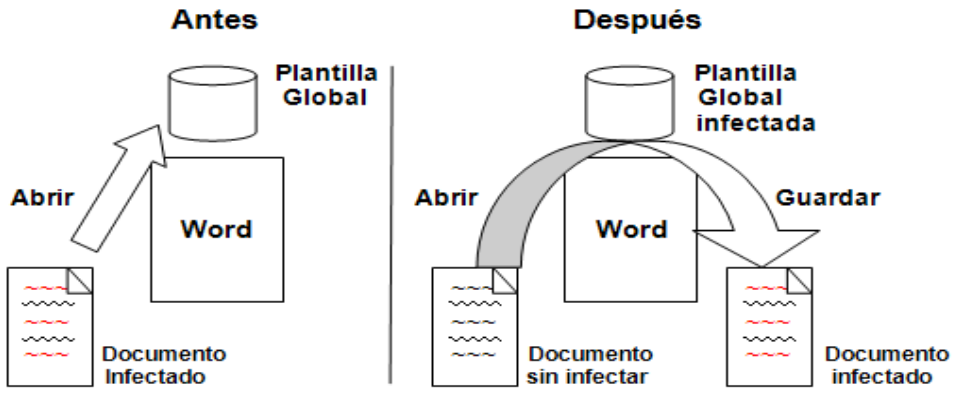


Fig. 2.5 Proceso de infección

Cuando una macro está dañada no necesariamente debe de contener un virus que origine un malfuncionamiento. A continuación se presentan algunos problemas en específico con los virus de macro:

- Un virus de macro ocasiona cambios accidentales o deliberados, incluso a su propio formato, creando un nuevo virus. Esto puede ocurrir de forma automática: cuando se convierten documentos de una versión de Word a otra, la conversión puede crear nuevos virus de macro en el proceso.

- Se pueden generar errores cuando el virus intenta propagarse, o en una desinfección incompleta, originando nuevas variantes. El software antivirus puede crear virus de forma accidental.

- Un virus de macro que fue creado de forma accidental puede “arrancar” las macros del entorno al que afecta, convirtiéndose en un nuevo virus.

Virus Multipartitas

Estos virus utilizan varios métodos de infección, por lo general infectan los archivos y sectores de arranque. Existen desventajas, para estos virus. Uno de los principales inconvenientes es la complejidad.

¿Por qué más complejo? Supongamos que un virus infecta un tipo de archivo, por ejemplo uno con extensión .com, necesita cierta cantidad de código para alcanzar su objetivo, pero uno que infecta dos tipos diferentes de archivos, .com y .exe, tendría más del doble de código. El virus no sólo tendría que saber cómo tratar con ambos tipos de archivos, sino también cómo distinguir entre ellos para conseguir infectarlos. Aplicando la misma lógica a los virus multipartitas. El virus debe de tener el código necesario para infectar dos objetivos muy diferentes, así como los medios para identificarlos. El tamaño del código es mucho más grande y requiere más recursos para procesarse. Se puede reducir el tamaño, pero esto generalmente significa una reducción en la función que realizaría. Un ejemplo de este tipo de virus es Invader.

Virus Script

Como en el caso de los virus de macro, un virus script se compone de código que puede ser interpretado, pero en este caso, por un servicio administrado por el S.O. Por ejemplo, el servidor de Windows Scripting utilizado en algunos sistemas de Microsoft Windows, este puede ejecutar scripts[18] en VBScript[19].

Estos virus son muy comunes, ya que son mucho más fáciles de escribir y modificar que otros tipos de virus. Un atacante que no sea muy calificado puede revisar y modificar el código, y distribuirlo a los demás. Se pueden encontrar docenas de variantes de un solo virus, la mayoría con cambios insignificantes.

Uno de los medios más comunes de infección es la utilización de canales IRC (Internet Relay Chat) mejor conocido como chat, permite la comunicación entre usuarios de Internet “en tiempo real”, se necesita de un software conocido como “cliente IRC” (por ejemplo, mIRC).

[18] Es un archivo con un conjunto de instrucciones que permiten automatizar una tarea.
[19] Visual Basic Script Edition es un lenguaje interpretado.

Con el software instalado el usuario se conecta a un servidor[20] chat, el cual está conectado a otros servidores y así conforman una red IRC. De ésta forma el usuario puede conectarse a uno o más canales IRC.

El usuario puede entablar conversaciones de dos tipos: públicas, todo el canal visualiza lo que el usuario digita; privadas, se realiza entre dos usuarios.

En este punto, es donde se pueden aprovechar de los usuarios, porque se puede enviar un virus script, logrando infectar a todos los usuarios conectados en ese canal.

2.2.1.3 Técnicas de ocultamiento de un virus

Cuando un atacante desea que su virus se extienda lo más posible, le incluye a éste una o más técnicas de ocultamiento para que sea más difícil de detectar. Las siguientes son técnicas de ocultamiento comúnmente utilizadas:

Auto-Cifrado

Esta técnica permite cifrar el cuerpo del virus. La posibilidad de utilizar diferentes claves para el cifrado, le dan al virus la habilidad de parecer uno distinto en cada infección, a pesar de que el código oculto es el mismo. El problema es que el virus al estar cifrado necesita de una rutina que descifre su cuerpo, la cual es la primera que se ejecuta para poder transferirle el control y sin ella el virus no funcionaria.

Para utilizar esta técnica se deben de tener tres partes bien definidas: una clave de descifrado, el código del virus (cifrado) y el código de la rutina de descifrado (sin cifrar).

[20] Sistema informático (computadora) que presta ciertos servicios y recursos (de comunicación, aplicaciones, archivos, etc.) a otros equipos (denominados clientes), los cuales están conectados en red a él.

Existen diferentes formas para cifrar el código del virus, una de las más sencillas se realiza utilizando la operación lógica XOR, que es una operación reversible. Por ejemplo, 6 XOR 3 = 5 es reversible, resultando 5 XOR 3 = 6, donde la clave es el número 3. Si la clave es cambiada se puede obtener un cifrado diferente.

Polimorfismo

Los virus que utilicen esta técnica contienen una seria de pequeñas rutinas que se ensamblan y así obtener una apariencia del virus diferente, cada que se reproduce.

En un inicio el virus tiene una rutina de descifrado y una porción cifrada (rutina de armado y copia, y contiene piezas para ensamblar), cuando se crea la copia, el virus utiliza algunas piezas de ensamblado para crear una nueva rutina de descifrado y así generar el virus con un cifrado diferente cada que se copie o después de un cierto número de copias.

Metamorfosis

La idea de esta técnica es alterar el contenido del propio virus, en lugar de ocultar con un cifrado diferente. El virus puede ser modificado de varias maneras, por ejemplo, mediante la adición de secuencias de código innecesario o cambiando la secuencia de instrucciones independientes en el código original. El código modificado tiene que volverse a compilar para crear un virus ejecutable que sea fundamentalmente diferente al original. Esta técnica no es muy utilizada, ya que el virus debe de ser capaz de desmontar y volver a montar el código.

Stealth (Camuflaje)

Es una de las técnicas más utilizadas por los virus, ya que oculta todo signo que pueda delatar la presencia de éste en el equipo.

- Por ejemplo, cuando un archivo es infectado, generalmente aumenta de tamaño. Para que esto no se pueda observar, el virus sólo incluye su código de infección en los espacios libres (sin contenido) del archivo. Con esto, aunque aumente el tamaño del archivo, el virus hará creer al sistema que éste no ha variado.

- Al infectar un archivo, se produce una modificación, cuya fecha y hora queda registrada, cambiando las características del archivo. El virus evita esto manteniendo la fecha y hora que estuvieran establecidas antes de la infección.

- Para evitar ser descubiertos, los virus ocultan algunos de los archivos que infectan, cambiando sus atributos y poniéndolos como oculto.

Esto lo consigue vigilando las peticiones del sistema operativo e interceptarlas, para proporcionar información falsa y evitar que se percaten de su existencia.

Existen virus que pueden detectar cuando se ejecuta un antivirus y descargar de la memoria parte de su propio código, cargándolo de nuevo cuando el antivirus ha terminado su búsqueda. Para utilizar esta técnica el virus tiene que estar residente en memoria (característica que permite a determinados programas permanecer en memoria, después de haberse ejecutado).

Armouring (acorazado)

Cuando un virus es detectado y aislado, el analista estudia su funcionamiento para preparar la correspondiente rutina de desinfección. La intención de ésta técnica es que el análisis del código sea lo más difícil posible y así retrasar la detención. Para esto se utilizan diferentes métodos, entre las cuales se encuentran los Anti-Debugging empleadas para evitar que un virus sea

descompilado y así ver su código original. También se suele incluir un Anti-Dissasembly que utiliza un grupo de técnicas para impedir que se desensamble el virus, aunque éste incluya código para confundir al analista.

Tunnelig

Con ésta técnica los virus tratan de protegerse de los módulos residentes de los antivirus que monitorean todo lo que sucede en la máquina para interceptar todas las actividades "típicas" que pudieran realizar. Entonces el virus se anticipa a interceptar las peticiones, obteniendo las direcciones de memoria en donde se encuentran y evitar que el antivirus lo detecte.

Su principal inconveniente es que requiere de una programación compleja, ya que en el momento de ejecutar una instrucción se produce una interrupción, colocando un ISR (Interrupt Service Routine) para dicha interrupción; entonces, se ejecutan instrucciones comprobando cada vez si se ha llagado al punto deseado, hasta recorrer toda la cadena de ISR's colocadas al final.

2.2.1.4 Ejemplo de virus

El siguiente ejemplo representa un virus elemental que busca un programa, lo infecta y pasa el control al programa infectado (Fig. 2.6). Se presentara en pseudocódigo de acuerdo a la convención que utilizo el doctor Fred Cohén en su tesis doctoral titulada "Computer Viruses":

:= se utiliza en las definiciones de programas y subrutinas
: se usa al final de un nombre para usarlo como etiqueta de una instrucción
; separa instrucciones
= asignar valores a las variables y comparaciones
~ implica negación
{ y } son para agrupar instrucciones

```
Programa virus_elemental :=
{
      Procedimiento infecta :=
      {
            archivo =
archivo_ejecutable_tomado_al_azar;
            inserta_virus_al_inicio_del_archivo;
            regresa;
      }
      Programa_principal :=
      {
            infecta;
            brinca_final;
      }
final:
}
```

Fig. 2.6 Ejemplo de virus.

A grandes rasgos, el virus busca un archivo ejecutable y se coloca antes de la primera instrucción del archivo recién infectado. Después brinca al final de virus, donde está la primera instrucción del programa original para que ejecute de manera normal.

2.2.1.5 Nomenclatura

Para asignar un nombre a un virus o cualquier otro malware, se sigue ciertas reglas de nomenclatura propuestas por CARO[21]. Está no es una institución dedicada a establecer estándares, pero varias firmas de antivirus utilizan algunas de sus reglas para asignar los nombres.

El malware es agrupado en familias, de acuerdo a su similitud de código y con el principio fundamental de que el nombre debe de ser único, es decir, todas las variantes distintas, sin importa que tan pequeñas sean, deben de tener un nombre diferente a cualquier otro.

Forma General

Prefijo.Familia.Variante

[21] Computer Antivirus Reserch Organization, estudia el fenómeno de los virus informáticos.

El prefijo está formado por el tipo y la plataforma. El tipo nos indica si se trata de un virus o de otro código malicioso (en este caso la explicación será únicamente para los virus). La plataforma puede ser el sistema operativo que afecta (por ejemplo, Windows), una aplicación (por ejemplo, una macro de Word) o un intérprete de lenguaje (por ejemplo, VBS). No se trata del tipo de archivo que infecte. En la tabla 2.1 se muestran algunos de los prefijos reconocidos en el convenio:

Prefijo	Comentario
A97M	Virus que infectan archivos Microsoft Access 97.
BAT	Virus de archivos por lotes. Requiere del intérprete de comandos de DOS, Windows o casi cualquier plataforma que ejecute archivos por lotes.
Boot	Virus que infectan el MBR o el sector de arranque del disquete.
JS	Virus creado en Java Script.
Linux	Virus que afectan a Linux y otros estrechamente ligados a él.
MacOS	Afectan a equipo con sistema operativo Mac instalado.
MSIL	Requiere de Microsoft Intermediate Language (plataforma .NET).
O97M	Virus de macro que afectan al menos dos aplicaciones de Office 97 (y posteriores) y/u otras aplicaciones afines (Visio, Project, etc.).
PHP	Creado en lenguaje PHP.
P98M	Virus de macro que infecta a Project 98.
PP97M	Virus de macro que afecta a Microsoft Power Point 97.
Unix	Virus que infecta a Unix.
VBS	Virus creado en Visual Basic Script.
W2M	Virus de macro para Microsoft Word 2.0.
W32	Requiere de Windows de 32 bits (Windows 9x, ME, NT, 2000, XP)
W64	Requiere de Windows de 64 bits.
W97M	Virus de macro para Microsoft Word 97
X97M	Virus de macro para Microsoft Excel 97

Tabla 2.1. Ejemplos de prefijos.

La familia del virus es determinada por un conjunto de características que lo identifican como una identidad totalmente nueva y diferente. Suele tomarse en cuenta alguna característica distintiva del virus, una cadena de texto o efecto. Para construir el nombre de una familia se utiliza con el juego de caracteres [A-Za-z0-9_-], es decir, las letras en mayúsculas y minúsculas, dígitos, guiones bajos.

Un virus suele ser lanzado varia veces con pequeños cambios, a estos se les conoce como variantes. Para armar una variante se utilizan letras mayúsculas, asignadas en forma consecutiva, cada que una nueva especie de una misma familia es descubierta. La primera variante de una familia siempre inicia con la letra A, la siguiente será B y así sucesivamente. Cuando se ha alcanzado la Z, el próximo tipo de virus descubierto que pertenezca a esa familia se le asignara AA, después AB, etc., hasta la AZ. A las variantes posteriores se les asignara BA hasta BZ, y así sucesivamente hasta llegar a ZZ.

El orden que se asigna a las variantes refleja el orden de su descubrimiento, no el orden aparente de su creación o cualquier orden, ya que nuevas variantes aparecen muy frecuentemente (varias veces al día), a diferencia de encontrar una nueva familia, que suele suceder esporádicamente.

Se suele usar un modificador que proporcione información adicional acerca de los virus, tales como su principal medio de propagación. En la tabla 2.2 se muestran los modificadores establecidos:

Modificador	Concepto
@m	Propagación lenta del virus por medio del correo electrónico, por lo general en respuesta a un correo recibido.
@mm	Distribución masiva de mensajes.

Tabla 2.2. Modificadores.

En el acuerdo se estableció que las firmas de antivirus pueden agregar un comentario al final del nombre, después del carácter “!”. Los más comunes se encuentran en la tabla 2.3:

Comentario	Concepto
cav	Estos virus escriben su código en las secciones de los archivos que se sabe que están vacías. Por ejemplo, los virus de cavidad pueden copiarse a sí mismos en las partes no utilizadas de encabezados de archivos exe, en los vacíos que se encuentran entre secciones de archivos exe.
dam	Virus dañado.
dll	Virus que utiliza componentes de una Biblioteca de enlace dinámico, comúnmente conocida coma DLL (*dynamic-link library*).

dr	Virus que utiliza un dropper (contiene un código que instala y ejecuta todos los archivos de la carga útil) para que lo libere.
gen	Virus que se detecta mediante una firma genérica. Son detectados por los antivirus sin utilizar cadenas de código especiales.
inf	Los utilizan los virus para auto ejecutarse.
irc	Virus que utiliza IRC para propagarse. Tenga en cuenta que esto no significa que el virus se escriba como una secuencia de comandos de IRC o mIRC.
kit	Estos virus son creados con algún "Kit de construcción"
pak	Comprime los virus.
p2p	Un virus diseñado para propagarse por las redes peer-to-peer.
rootkit	Lo utiliza el virus para ocultar los cambios realizados en la computadora.

Tabla 2.3. Comentarios.

En la tabla 2.4 se presentan algunos ejemplos de la nomenclatura:

Nombre	Descrpción	Familia	Variante	Mod
W97M/Invade	Macro de Word 97	Invader	----	----
W32/Doctor.A	Windows de 32 bits	Doctor	A	----
W97M/Marker.AH	Macro de Word 97	Marker	AH	----
VBS/Grouch.A	Visual Basic Script	Grouch	A	----
W97M/Melissa.AU@mm	Macro de Word 97	Melissa	AU	@mm
Boot/WYX	Infectan el MBR o BR (Disquete)	WYX	----	----
W97M/Wazzu.X	Macro de Word 97	Wazzu	X	----

Tabla 2.4. Ejemplos de nomenclatura.

2.2.1.6 Nivel de amenaza

Un mismo virus es detectado por varios especialistas, cada uno de estos lo designa con un nivel, así permite informar sobre la amenaza que representa en un momento dado. Cada quien utiliza los criterios que cree adecuados para ubicar el virus en un nivel, además, los niveles manejados también son variables.

Como ejemplo, se presenta los siguientes *"niveles de peligrosidad, los cuales utilizan dos criterios. El primero, su propagación, indica lo extendido que se encuentra el virus. En segundo lugar tenemos el nivel de daño, indica el perjuicio*

que un virus causa al infectar un sistema informático (aparición de mensajes en pantalla, pérdidas o alteraciones de información, sistemas colapsados, etc.):" [9]

- **Baja:** amenaza leve, ya que aunque el virus es dañino, está poco extendido.
- **Media:** quiere decir que bien el virus está relativamente extendido y su infección causa perjuicios, o bien está poco extendido pero su infección puede causar daños importantes.
- **Alta:** amenaza importante, ya que bien el virus está muy extendido y su infección causa daños, o bien está relativamente extendido y además su infección causa grandes perjuicios.
- **Muy alta:** amenaza muy importante, ya que está muy extendido y su infección causa grandes perjuicios.

2.2.2 Puertas traseras

Es un punto de entrada al sistema, por el cual un atacante puede acceder de forma remota sin que lo detecten. Por ejemplo el atacante utiliza alguna vulnerabilidad en particular que le permite el acceso a un equipo con permisos de administrador[22], pero con el tiempo esta puerta trasera es cerrada, impidiendo que el atacante tenga acceso de nuevo al sistema. El hecho de que la vulnerabilidad original que le permitió la entrada fuera cerrada no ayuda mucho, porque el atacante pudo instalar otras puertas traseras en el sistema.

Estas puertas traseras pueden ser insertadas en el código durante el desarrollo de cada módulo de un sistema, tal vez para probar de forma independiente el funcionamiento del módulo, para permitir el acceso al módulo por si llegara a fallar en el futuro o para modificaciones. Además de estos usos el desarrollador pudo dejar la puerta trasera para acceder al sistema una vez que esté funcionando.

[22] Es cuando un usuario tiene derechos administrativos, es decir, puede modificar la configuración del sistema, como instalar programas, cambiar la configuraciones de los servicios, administrar cuentas de usuarios, etc.

Cuando se organiza el sistema en módulos o componentes facilita la realización de pruebas independientes y así garantizar un funcionamiento correcto, al integrar cada uno de ellos.

Algunas de las causas de que existan las puertas traseras son:

- El desarrollador olvidó quitarla una vez que su utilidad se termina.
- Intencionalmente se queda en el programa para tener acceso con fines maliciosos.
- La deja para dar mantenimiento al programa terminado.

Una puerta trasera pueden ser aprovechada por los desarrolladores originales o utilizada por cualquier persona que la descubra.

Cuando el atacante logra una conexión con el equipo puede realizar un conjunto de acciones en el sistema, tales como la transferencia de archivos, la adquisición de contraseñas o ejecutar algún comando. Las puertas traseras pueden ser utilizadas para crear un zombi.

2.2.2.1 Zombi

Un Zombi es un equipo que ejecuta un programa, llamado "bot"[23]. Estos son pequeños programas instalados por los atacantes, con la intención de tomar el control remoto del equipo del usuario sin su conocimiento o consentimiento.

En ocasiones los bots utilizan la combinación de código malicioso para poder infectar un mayor número de equipos en el menor tiempo posible y evitar ser detectados. Cuando el programa es instalado en una máquina lo primero que hace es comunicase al Centro de Comando y Control (C&C), para que el atacante pueda controlarla.

[23] Es una abreviatura de la palabra robot.

Al grupo de equipos que ejecuten el mismo tipo de bot se le conoce como una red-zombi (botnet). Donde el atacante puede manipular, cada uno de los equipos o la red completa, por medio de instrucciones enviadas de forma remota. Las instrucciones más comunes son: descargar y ejecutar archivos, que le permitan instalar cualquier tipo de código malicioso en el equipo; descargar actualizaciones de sí mismo, para mejorar sus funciones o modificar su comportamiento; activar o desactivar la forma de propagación.

Una red zombi está conformada por miles o millones de equipos, los cuales se encuentran en diferentes ciudades del mundo. Un ejemplo es la red Mariposa que fue desactivada el 23 de diciembre del 2009 por la operación conjunta de Panda Security, Defence Intelligence, FBI y la Guardia Civil española.

"La red Mariposa afecto a casi 13 millones de equipos distribuidos en más 190 países. Donde la India se coloca en el primer lugar de infecciones, con el 19.14%; el segundo lugar lo tiene México, con un 12.85% y le sigue Brasil, con 7.74%. Los países con el nivel más bajo de infección son Argentina, con un 1.10% y Estados Unidos, con un 1.05%" [10]. Entre la información robada se encontraron números de cuentas bancarias, de tarjetas de crédito y nombres de usuarios. Los equipos comprometidos pertenecen a usuarios domésticos, empresas, agencias gubernamentales y universidades.

Con frecuencia una red zombi es utilizada para lanzar un ataque conocido como denegación de servicio distribuido (DDoS, ***D****istributed* ***D****enial* ***o****f* ***S****ervice*). DDoS es un procedimiento coordinado, realizado por un conjunto de computadoras. Tiene como propósito generar una inundación de paquetes para sobrecargar un equipo o una red completa. Para lograr esto el atacante tiene que controlar cientos o miles de máquinas que estén conectadas a Internet.

Este control lo obtiene instalando un software en cada uno de los equipos, el cual recibirá las órdenes. En este punto el atacante tiene que tener permisos de administrador. Aparte de instalar el software en el equipo el atacante registra la dirección IP[24] y con esto está lista para realizar el ataque DDoS.

Cuando se realiza un DDoS el atacante lo coordina desde una computadora, que bien podría ser su propia máquina o una diferente. Para disminuir el riesgo de ser descubierto utiliza una máquina diferente, la cual lleva el nombre de "Master" y es la encargada de recibir los comandos del atacante, este equipo enviará las instrucciones a los "zombis", quienes en respuesta a estos iniciaran el DDoS en contra del objetivo (Fig. 2.7).

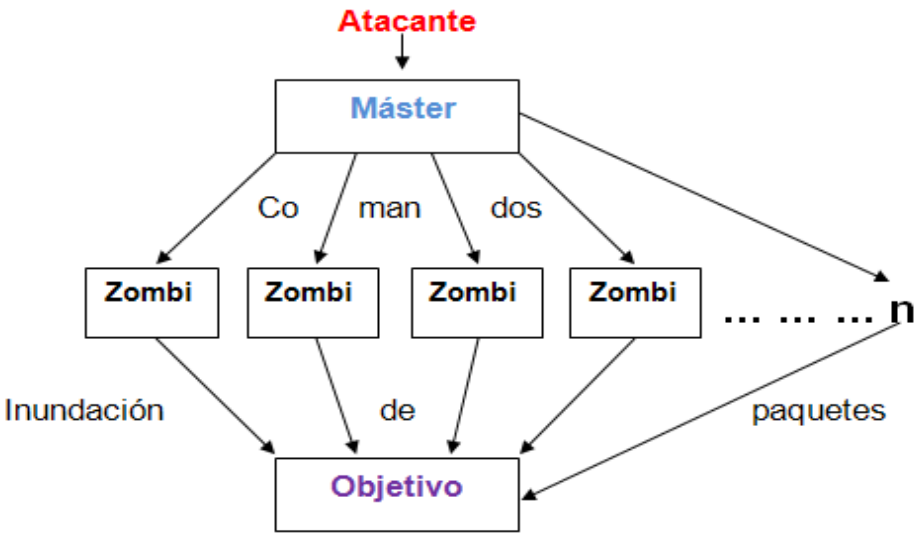


Fig. 2.7 Modelo básico de una herramienta de ataque DDoS

2.2.3 Caballo de Troya

Un caballo de Troya es un programa que se hace pasar por una aplicación inofensiva, que proveen algo interesante para el usuario, pero que tiene ocultas otras funciones. Son llamados así por el caballo de madera de la mitología griega (comúnmente conocidos como troyanos).

[24] Es el número con el que se identifica la interfaz de una computadora u otro dispositivo al conectarse a la red.

Podemos encontrar una gran cantidad de métodos de infección, porque estos dependen del ingenio de los atacantes. Algunos de los ejemplos más comunes son: archivos enviados por correo electrónico que simulan ser una imagen, un archivo de música; la descarga de un video o de un juego que se encuentran en alguna página electrónica.

Un caballo de Troya no es un virus, porqué no puede reproducirse. Este hecho no quiere decir que no puedan ser destructivos. Este tipo de programas tienen una gran variedad de objetivos, entre los cuales podemos encontrar el robo de contraseñas, permitir el acceso remoto (puerta trasera), suprimir los nombres de los procesos maliciosos que encuentran activos en el equipo, etc.

Un ejemplo de infección sería la descarga e instalación de un supuesto, video juego en la computadora y cuando lo ejecuta puede pasar alguna de las siguientes acciones:

a) Aparentemente el juego funciona normal, pero sin que se dé cuenta el usuario está realizando una acción de forma paralela.
b) En un inicio el juego trabaja correctamente, pero después cambia e inicia una acción maliciosa. Por ejemplo, abrir una puerta trasera.
c) Desde un principio comienza a eliminar los archivos del sistema.

Este tipo de código malicioso se ha encontrado en páginas del gobierno mexicano, como fue el caso del *"sitio oficial de la Comisión Federal de Telecomunicaciones (Cofetel), donde los usuarios no se percataban que su información estaba siendo enviada a otro sitio"*[11].

Un caballo de Troya utiliza algunas herramientas que le permiten cumplir con su objetivo, por ejemplo un Keylogger.

Un Keylogger registra las pulsaciones del teclado de un equipo. El objetivo de estos programas no es el de dañar el equipo, sino de robar información del

usuario, porqué pueden registrar el contenido de los mensajes escritos en el correo electrónico o las direcciones de este, nombres de usuarios, contraseñas e información financiera (por ejemplo, número de identificación personal [PIN] o el de la tarjeta de crédito).

Un ejemplo de este tipo de programas es Keylogger-Pro, es considerada como una herramienta legítima que permite capturar las pulsaciones del teclado realizadas en un archivo, y posteriormente enviar los datos a través del correo electrónico. Puede ser instalado en equipos que tengan Windows 2003/XP/200/NT/ME/98/95 [12]. El problema de este tipo de herramienta radica en el uso que le dan los atacantes.

Los Rookits son otro ejemplo, estos son programas diseñados para mantener en forma encubierta el control del equipo. Pueden evitar que se detecten una serie de acontecimientos maliciosos, por ejemplo, cuando se abre una puerta trasera, si se modificó o reemplazó algunos archivos del sistema e incluso puede instalar programas, que pueden ser maliciosos, sin la autorización del usuario.

El hecho de que el rootkit puede ocultar los cambios realizados en el equipo hace muy difícil determinar cuando éste está infectado, y además saber que fué los que modificó, puede utilizar funciones del sistema para pasar desapercibido.

En un inicio los rootkit aparecieron en el sistema UNIX y eran una colección de una o más herramientas que le permitían al atacante conseguir y mantener el acceso al usuario más privilegiado de la computadora (en los sistemas UNIX, este usuario se llama *root* y de ahí su nombre).

Los rootkit también suelen ser utilizados para obtener los permisos necesarios para poder dirigir el ataque DDoS, descrito anteriormente.

"En el 2009 se han registrado nuevos ejemplares de caballos de Troya, alcanzando un 66%" [13] del total de código malicioso. Esto se debe, especialmente, al interés económico de los atacantes, ya que son utilizarlos para el robo de información bancaria.

2.2.4 Gusanos

Un gusano es un programa que se copia así mismo y no necesita de un programa anfitrión para infectar a una víctima. Se propaga por sí mismo, porque puede crear copias capaces de auto ejecutarse. Estos programas se aprovechan de las vulnerabilidades conocidas en las aplicaciones, cuando han infectado el equipo pueden dejar una puerta trasera y enviarse a través de la red y así infectar un mayor número de equipos, que bien podrían formar parte de una red zombi.

Inicialmente los gusanos se utilizaron para el mantenimiento y administración de los equipos de cómputo en Xerox PARC (Palo Alto Research Center) y en 1982 los investigadores John F. Shoch y John A. Hupp publicaran el artículo "The Worm Programs" [14], donde uno de ellos utilizo el nombre de "gusano vampiro" (para referirse a estos programas).

Una noche dejaron un gusano funcionando en un grupo pequeño de máquinas del laboratorio, donde su puestamente se crearía una copia por equipo. A la mañana siguiente este se escapo e infecto alrededor de 100 equipos, los cuales quedaron paralizados. Cuando intentaron eliminarlo este volvía a aparecer, por eso implementaron otro programa que fuera de una máquina a otra "matando" las copias que había creado el gusano.

Los gusanos están compuestos, principalmente, de tres partes:

- Mecanismo de ataque
- Carga útil (Playload)
- Seleccionar nuevo objetivo

El mecanismo de ataque es utilizado para explotar las vulnerabilidades necesarias que le permitan al gusano copiarse a sí mismo en el equipo destino.

La parte que se encarga de llevar a cabo las acciones maliciosas contra el huésped comprometido es la carga útil. Algunos gusanos no la tienen, sino simplemente se dispersan y consumen los recursos del equipo. Cuando el gusano consigue ejecutar la carga útil y este tiene los privilegios de administrador puede hacer daño al equipo. Entre las acciones más comunes se encuentra la de borrar el disco duro, o instalar un rootkits y dejar una puerta trasera. El atacante puede incluir en la carga útil un programa encargado de buscar en la computadora información del usuario y enviarla a un correo electrónico donde él pueda recogerla después.

Cuando el gusano es ejecutado en el equipo atacado, se intenta propagar de nuevo. Para ello, debe de localizar un equipo destino que sea vulnerable a su mecanismo de ataque. Para seleccionar un nuevo objetivo, algunos gusanos utilizan las direcciones IP que se encuentren numéricamente cercanas a la IP del equipo comprometido. Por ejemplo, si la dirección IP del equipo infectado es 192.168.1.134, el mecanismo de selección buscara al azar las direcciones IP que comiencen con 192.168.1, antes de buscar cualquier otra. Esto mejora las posibilidades de que la dirección IP elegida tengo un equipo utilizándola, porque a menudo los equipos de una red tienen las direcciones similares.

Otra formas en la que se puede propagar un gusano es por medio del correo electrónico, esto lo logra localizando archivos con extensiones específicas (por ejemplo, doc, txt, etc) dentro del equipo infectado y así poder enviar una copia de sí mismo a todas las direcciones del correo encontradas. Algunos gusanos pueden infectar el equipo una vez que el usuario abre el archivo adjunto recibido en su correo.

2.2.5 Programas Espía

Los programas espía o spyware son aplicaciones que recompilan información personal o modifican, en ocasiones, la configuración del equipo sin el consentimiento del usuario. La información recabada puede ser enviada a empresas publicitarias u otro tipo de organizaciones que lucran con ella.

En la información que recaban estos programas podemos encontrar: las páginas web visitadas, la frecuencia con que se visitan e incluso cuanto tiempo tarda el usuario en el sitio, que tipo archivos se descargan, el contenido del disco duro, que programas están instalados.

Los programas espía pueden ser instalados en los equipos por medio de un caballo de Troya o un gusano que proviene del correo electrónico. En ocasiones el usuario instala algún programa gratuito o visita páginas web que contiene código malicioso que explota alguna vulnerabilidad del navegador, permitiendo la instalación encubierta de un spyware.

Algunos programas espía realizan cambios molestos en la computadora infectada. Por ejemplo, modifican la página de inicio del explorador o agregan a él componentes que el usuario no necesita. Esto provoca que el funcionamiento del equipo sea más lento y en ocasiones llegan a bloquearlo.

Cuando los programas que recolectan información son instalados con el conocimiento del usuario y este comprende completamente los datos que serán recolectados y adonde serán enviadas, entonces estos programas no se consideran como espías.

Pero, estos mecanismos de los cuales se sabe de su existencia y funcionamiento, y además el cómo se desactivan, no evita que algún usuario sea afectado por el mal uso que se les dé. Como ejemplo podemos mencionar a las cookies

persistentes, que son pequeños archivos de texto que el navegador almacena en el disco duro del equipo, cuando se visitan sitios web. Estos sitios suelen usarlas para asignar a los visitantes un número de identificación individual que notificara al sitio de las visitas subsecuentes.

El problema radica en que toda la información personal que se introduce en el sitio web se puede almacenar en las cookies, por ejemplo el número de cuenta de la tarjeta de crédito, nombres de usuarios, registrar productos y servicios, etc. Las cookies se pueden utilizar para rastrear las actividades del usuario y con la información recabada formar un perfil detallado de él. Los usuarios afectados no tendrán ni la más mínima idea del contenido de su perfil y a quien será enviado.

Por lo general, estos perfiles son vendidos a terceras personas que los utilizan para mandar anuncios y otros contenidos al usuario. Por estas razones pueden ser consideradas como programas espía.

2.2.6 Adware

Los programas adware[25] muestran publicidad asociada a productos y/o servicios ofrecidos por los propios creadores o por terceros. El adware puede ser instalado de muchas formas (por ejemplo, al instalar un programa gratuito). Esto lo puede logran mostrando mensajes o ventanas intercaladas entre las ventanas de instalación del programa original. Entonces el usuario da su inadvertido permiso para instalarlo en el equipo.

Cuando el adware está instalado en el equipo, intenta conectarse a un servidor, que le indica los anuncios a mostrar. Cuando el usuario está conectado a internet, se abre una conexión con la máquina remota y así poder mostrar una ventana publicitaria.

[25] Contracción de **AD**vertisement - anuncio - y software

A pesar de que el adware no produce alguna modificación visible del sistema, si afecta su rendimiento, ya que consume los recursos del equipo (memoria, espacio en el disco duro, etc.). *"El año pasado, del total de nuevo código malicioso registrado, el adware se coloca en segundo lugar con un 17.62% de ejemplares"* [13]. Por lo general, los adware utilizan información recabada por programas spyware y así determinar el tipo de anuncios que le serán mostrados al usuario. Con frecuencias estos dos programas trabajan juntos.

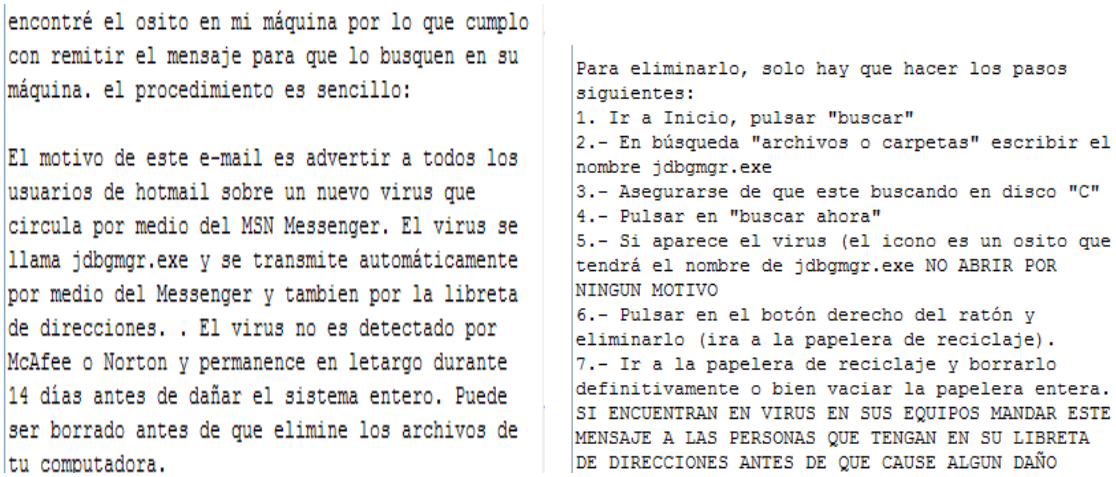
2.2.7 Engaños

Los engaños (en inglés: hoaxes) son mensajes distribuidos por el correo electrónico, con el fin de hacer creer a los lectores, que algo falso es real. El contenido de estos mensajes es muy variado, pero el objetivo, en casi todos ellos, es de generar alarma y confusión en los usuarios.

Entre el contenido más común de los hoaxes, se pueden encontrar alertas falsas de nuevos virus u otras amenazas, historias creíbles sobre personas enfermas o secretos para hacerse millonario. Por lo general, se invita al usuario a reenviar el correo a todos sus contactos.

Un ejemplo, es el *JDBGMGR.EXE* [15], catalogado como un falso virus. Este es un mensaje que llega por correo electrónico, no contiene algún archivo adjunto. En la figura 2.8 podemos observar el mensaje, donde se solicita al usuario borrar el archivo jdbgmgr.exe localizado en c:\windows\system, mencionando que supuestamente está infectado por el virus y además, en la parte inferior del mensaje se solicita que sea reenviado para evitar algún daño, esto con el fin de afectar a un mayor número de usuarios.

El archivo jdbgmgr.exe lo tienen las versiones anteriores a Windows XP y si es borrado ocasiona problemas con algunas páginas web.



encontré el osito en mi máquina por lo que cumplo con remitir el mensaje para que lo busquen en su máquina. el procedimiento es sencillo:

El motivo de este e-mail es advertir a todos los usuarios de hotmail sobre un nuevo virus que circula por medio del MSN Messenger. El virus se llama jdbgmgr.exe y se transmite automáticamente por medio del Messenger y tambien por la libreta de direcciones. . El virus no es detectado por McAfee o Norton y permanence en letargo durante 14 días antes de dañar el sistema entero. Puede ser borrado antes de que elimine los archivos de tu computadora.

Para eliminarlo, solo hay que hacer los pasos siguientes:
1. Ir a Inicio, pulsar "buscar"
2.- En búsqueda "archivos o carpetas" escribir el nombre jdbgmgr.exe
3.- Asegurarse de que este buscando en disco "C"
4.- Pulsar en "buscar ahora"
5.- Si aparece el virus (el icono es un osito que tendrá el nombre de jdbgmgr.exe NO ABRIR POR NINGUN MOTIVO
6.- Pulsar en el botón derecho del ratón y eliminarlo (ira a la papelera de reciclaje).
7.- Ir a la papelera de reciclaje y borrarlo definitivamente o bien vaciar la papelera entera.
SI ENCUENTRAN EN VIRUS EN SUS EQUIPOS MANDAR ESTE MENSAJE A LAS PERSONAS QUE TENGAN EN SU LIBRETA DE DIRECCIONES ANTES DE QUE CAUSE ALGUN DAÑO

Fig. 2.8 Correo electrónico (Versión en español)

2.2.8 Spam

El spam es correo electrónico no solicitado, anónimo y masivo. El anonimato lo consigue enviándolo con direcciones de remitentes falsas o pertenecientes a otras personas, para ocultar su verdadero origen. Estos correos son enviados en forma masiva, porque los spammers (individuos o empresas que generar spam) hacen dinero con el pequeño porcentaje de destinatarios que responden. El hecho de que no sea solicitado depende del usuario, porqué es quien decide recibirlo o no.

Generalmente, el spam es utilizado con fines publicitarios, políticos, estafas financieras, pornografía, bienes y servicios, también hay casos donde infecta el equipo con otra clase de código malicioso (caballos de Troya o gusanos). Los mensajes en cadena que son enviados por amigos o conocidos, donde se pide que este sea reenviado a la mayor cantidad de amigos, también entrar en esta categoría.

Los correos en cadena son un riesgo para el usuario, porqué este puede reenviar el correo sin tomar la precaución de utilizar la opción de copia oculta (para no difundir sus direcciones de correo).

Los spammers tienen que conseguir el mayor número posible de direcciones de correo válidas, que sean realmente utilizadas por los usuarios, para mandar el spam. Esto lo pueden lograr comprando bases de datos de usuarios a particulares o empresas, por supuesto esta actividad puede ser ilegal, sin embargo, es una de las formas más comunes. Otra forma es el uso de programas automáticos, que recorren Internet en busca de direcciones en páginas web, grupos de noticias[26], etc.

Uno de los métodos más comunes para el envió masivo, es por medio de redes de zombi, las cuales son creadas o compradas por spammers, esto les permite mandar el spam sin que el usuario se entere.

"*Según, McAfee un 97% del total de correos en el mundo son spam"* [16] y un usuario le demora tres segundos verlo y borrarlo. Aunque algunos de los mensajes no son vistos debido a filtros anti-spam, los cuales no evitan que lleguen a los correos de los usuarios e invierta tiempo en eliminarlo, afectando directamente en su desempeño laboral y las finanzas de la empresa.

2.2.9 Phishing

El termino Phishing es una variación de la palabra en inglés fishing, que en español significa "ir de pesca". El término se refiere al hecho de enviar a un usuario un correo electrónico haciéndose pasar por una empresa legítimamente establecida en un intento de engañar al usuario para entregar información personal o privada. El correo dirige normalmente al usuario a visitar un sitio web donde se le pide actualizar la información personal, como contraseñas y tarjetas de crédito o números de cuentas bancarias, que la organización legítima ya tiene. Y con esta información suplantar la identidad de la víctima.

[26] Es uno de los servicios de Internet, mediante el cual varias personas se conectan para discutir e intercambiar información sobre temas concretos de interés común.

No se habla de enviar un sólo correo electrónico a un único usuario, sino de enviar miles de correos a miles de usuario. Esto lo hace el atacante, conocido como “phisher”, para obtener la información en los primeros días, ya que la mayoría de los usuarios responden en las primeras 24hrs.

Como el mensaje es distribuido masivamente, algunos de los receptores serán efectivamente clientes de la organización legítima. A los cuales se les engaña diciendo que por algún problema de seguridad es necesario que proporcione nuevamente sus datos.

El phishing utiliza el factor miedo, para inducir al usuario a ingresar la información en el sitio del atacante. Agrega al correo electrónico frases como “su cuenta caducara en 24hr” o “si no ingresa la información en las próximas horas…”, esto hace que el usuario se preocupe por responder lo antes posible y no se detenga a confirmar la veracidad del mensaje.

En un intento del atacante por aumentar la eficacia del engaño, crea el sitio web falso con el logotipo, estructura, imágenes y los colores de la página original.

Como ejemplo de un ataque phishing tenemos al servicio de subastas en Internet eBay. Después de que el atacante diseño la página web fraudulenta envía el correo electrónico que se muestra en la figura 2.9 (versión en español), en el cual se puede leer como tratan de ejercer presión sobre el usuario.

Asunto: Advertencia Actualización de la tarjeta de crédito/débito
[1]Registrarse en eBay
[2][poweredByLogo_112x22.gif]
Estimado cliente: [3][SYIStart_LiveHelp_75x20.gif]
Lamentamos informarle que procederemos a cancelar su cuenta de eBay si no actualiza la información de su cuenta. Para poder solucionar este problema, [4] **haga clic aquí** para volver a introducir la información de su cuenta. Si el problema no puede resolverse, su cuenta se suspenderá por un período de 24 horas, a partir del cual su cuenta quedará cancelada.
Tal y como queda estipulado en la Sección 9 del Acuerdo de usuario, podemos emitir una advertencia inmediata y suspender temporal o indefinidamente, o rescindir por completo, su suscripción y negarnos a ofrecerle nuestros servicios si consideramos que sus acciones pueden causar pérdidas financieras o responsabilidades legales a usted mismo, a nuestros usuarios o a nosotros. Podemos asimismo tomar estas medidas en caso de que no podamos verificar o autentificar la información que nos haya proporcionado.
Debido a la suspensión de esta cuenta, se le prohíbe hacer uso alguno de eBay, incluido el registro de una nueva cuenta. Tenga en cuenta que esta suspensión no lo redime de sus obligaciones previamente acordadas en lo referente a cualquier pago debido a eBay.
Atentamente,
Departamento de Safeharbor, eBay,Inc
El equipo de eBay.
Éste es un mensaje automático. No responda a este mensaje.
[5]Acerca de eBay | [6]Anuncios | [7]Centro de seguridad | [8]Políticas | [9]Mapa del sitio | [10]Ayuda

---

Fig. 2.9 Correo de ejemplo

Después de que el usuario hace clic en el enlace, es conducido a una página de inicio de sesión falsa, para que introduzca su nombre de usuario y la contraseña. Como se muestra en la Fig. 2.10. Seguidamente, se muestra a la víctima una página en la que supuestamente se le permitirá actualizara el perfil de su cuenta (Figura 2.11) y desde la cual se le trasmitirá al atacante la información altamente confidencial de la víctima, como los datos de su tarjeta de crédito, el número de seguro social, la dirección particular, el número del permiso de conducir y el nombre de soltera de su madre.

A continuación se proporcionan algunos consejos para tratar de reducir el riesgo de sufrir un ataque por phishing:

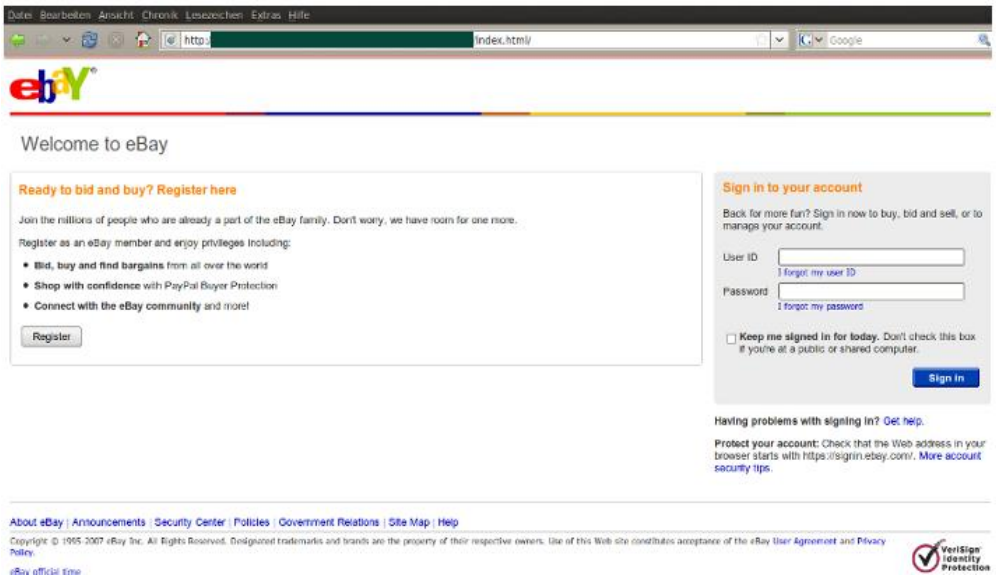


Fig. 2.10 Página Web falsa.

Fig. 2.11 Supuesta actualización.

- Si desea ingresar a la página web legitima escriba la dirección en su navegador de Internet y no haga clic en el enlace proporcionado por el correo electrónico.
- Para comprobar que la página web es segura debe de empezar con **https://** (Fig. 2.12a) y un pequeño candado cerrado debe aparecer en la barra de estado del navegador (Fig. 2.12-b).

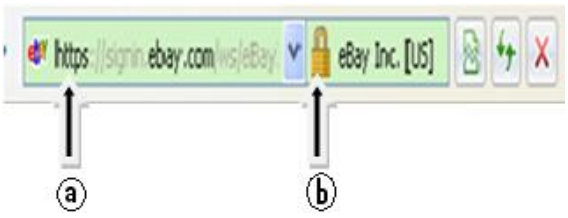


Fig. 2.12 Barra de estado del navegador

El usuario debe de poner atención en los sitios web que visita, *"por el motivo de que al mes, más de 200 marcas son imitadas; a nivel mundial México representa 0.5% del fraude"* [17]. *"Para el segundo semestre del 2008 se encontraron en México 270 páginas web fraudulentas"* [18].

2.2.10 Pharming

El pharming consiste en explotar una vulnerabilidad del DNS[27], que le permite al atacante cambiar el nombre de dominio de un sitio en Internet y así poder redirigir el navegador del usuario a páginas web falsas.

Una diferencia principal entre phishing y el pharming, es que el primero debe su éxito a la ingeniería social[28], aunque no todos los usuarios caen en los trucos y su difusión es limitada. Por el contrario, el pharming puede atacar a un número de usuarios mucho mayor.

"Por otro lado, el pharming no se lleva a cabo en un momento concreto, como lo hace el phishing, a través del envío de sus correos, ya que las modificaciones del DNS quedan en el equipo, a la espera de que el usuario acceda al servicio" [4] (por ejemplo, bancario, de subastas en línea, etc.).

Para llevar a cabo el ataque pharming se necesita de alguna aplicación instalada en el sistema a atacar, que realice las acciones necesarias para efectuarlo. Evidentemente, esta aplicación debe de llegar primero al equipo de la victima. Como ocurre en los otros tipos de código malicioso, las entradas más comunes al equipo son: correo electrónico (la más frecuente), descargas por Internet, copias desde un disco o una memoria USB[29].

[27] Domain Name Server, Servidor de Nombres de Dominio. Es el equipo responsable de resolver los nombres de las direcciones de Internet a su dirección real.
[28] Consiste en tratar de conseguir información confidencial de los usuarios mediante su manipulación.
[29] Universal Serial Bus, es un dispositivo de almacenamiento, se utiliza para guardar información que puede requerir el usuario.

Para comprender mejor como se hace un ataque pharming se explicara, brevemente, el funcionamiento de un DNS. Este se encarga de lo que se llama resolución de nombres, esto es cuando el usuario teclea una dirección, por ejemplo www.unam.mx, esta debe ser convertida a una dirección IP numérica, como 132.248.10.7. Cuando se hace una petición a la página www.unam.mx, se direcciona al servidor DNS más cercano, el cual localiza la dirección IP correspondiente. Para los usuarios es más fácil recordar una dirección que utilice letras, que una formada por números.

Los DNS almacenan tablas con nombres comunes (como pueden ser www.unam.mx, www.eluniversal.com.mx) y su dirección numérica. Cuando un "pharmers[30]" logra lanzar un ataque de "envenenamiento" del DNS con éxito, lo que hace es modificar la tabla del equipo. Consiguiendo redirigir a una importante cantidad de víctimas desprevenidas a una serie de sitios web falsos.

Un ataque pharming puede ser dirigido a un equipo en concreto, esto se realiza manipulando un archivo de texto llamado hosts que relaciona en forma unívoca las direcciones IP con los nombre de sitios web. Este archivo es utilizado para resolver nombres de dominio a través de direcciones IP en forma local y no se tenga la necesidad de acceder a los DNS.

El archivo lo podemos encontrar en cualquier equipo, la ubicación depende del tipo de sistema que se esté utilizando. Por ejemplo:

- En sistemas Windows 95/98/ME este archivo se encuentra en **C:\Windows\Hosts**
- En sistemas Windows NT y 2000 se aloja en **C:\Winnt\System32\drivers\etc**
- Cuando se trata de sistemas Windows 2003 se localiza en **C:\WINDOWS\system32\drivers\etc**

[30] Es el nombre que se le da a un atacante que realiza ataques Pharming.

- En sistemas con Windows XP se ubica en **C:\Windows\System32\drivers\etc**
- En los sistemas Linux, se encuentra alojado en **/etc/hosts**

En la figura 2.13 se puede observar un ejemplo del archivo hosts, versión Windows XP, el cual incluye una breve explicación.

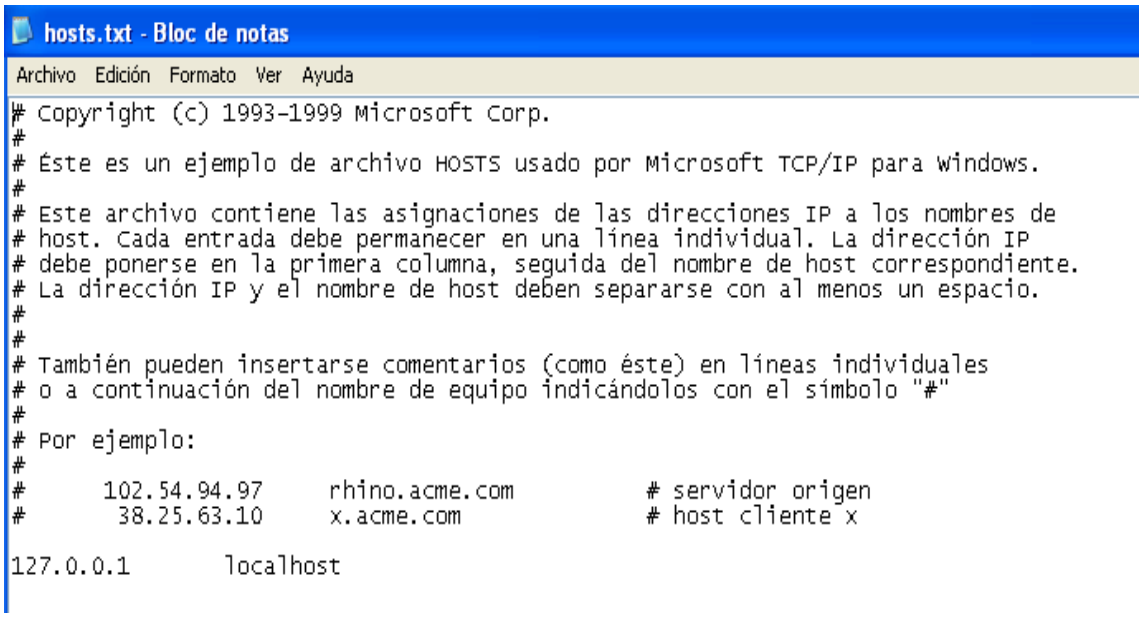


Fig. 2.13 Archivo Hosts

Los atacantes agregan, al archivo hosts, diferentes nombres de páginas web de empresas bancarias o financiaras relacionadas a una correspondiente dirección IP que apuntara a un sitio falso.

En el momento que el usuario intente acceder a cualquiera de las entidades bancarias, modificadas por el atacante, será redireccionado a la dirección IP que se encuentre en el archivo; es decir, a la página web falsa que resulta ser muy similar a la página web legítima (ataque de phishing), esto sucede aún cuando el usuario escriba la dirección de la pagina en la barra del navegador.

"En el 2008 se dio a conocer una vulnerabilidad en los módems[31] *2Wire, la cual permitía modificar los DNS locales. Esto se conseguía utilizando un correo electrónico, que eran enviados a las víctimas, para infectar el equipo, y así poder redirigir todas las solicitudes de www.banamex.com a un sitio fraudulento"* [19], para poder robar sus números de cuenta y contraseñas.

2.3 Historia del código malicioso

"Para 1949 el matemático John Von Neumann ya había establecido la idea de programa almacenado"[5] y en su artículo "Theory and Organization of Complicated Automata" presenta por primera vez la posibilidad de desarrollar pequeños programas replicantes y capaces de tomar el control de otros programas de similar estructura.

A finales de los cincuentas, en los laboratorios Bell Computer, tres programadores: *"Robert Thomas Morris, Douglas Mcllroy y Victor Vysottsky crean un juego denominado CoreWar"*[1]. Éste consistía en que cada jugador podía presentar varios programas llamados "organismos", los cuales se iniciaban al mismo tiempo para atacar y destruir a los programas del oponente y, lo más importante, reproducirse. El objetivo del juego era borrar los programas del oponente y ganar más memoria. El vencedor era el que tuviera más organismos "vivientes" al final del juego.

"A principios de los setentas apareció Creeper, que era capaz de reproducirse asimismo en forma autómata, fue detectado en ARPANET (el precedente de Internet)" [1]. Los sistemas infectados mostraban un mensaje en la pantalla periódicamente: "I´m a creeper… catch me if you can!" (Soy una enredadera, atrapame si puedes).

[31] Dispositivo que convierte las señales digitales de una computadora a señales analógicas que puedan ser transmitidas a través del canal telefónico.

Como aparecían continuamente copias de Creeper, crearon el programa Reaper para que se dedicara a destruir cuanta copia de Creeper encontrara hasta eliminarlas todas.

En 1983 Fred Cohen presentó, en un seminario de seguridad informática, el primer experimento con virus informáticos propiamente dichos en una computadora VAX/ 11/750 bajo Unix. Se trataba de realizar un programa capaz de modificar a otros para introducir en ellos una copia de sí mismo.

Cohen publica en 1984 sus estudios en "Computer Viruses - Theory and Experiments", donde define por primera vez a los virus informáticos, el que dice:

"Definimos un virus informático como un programa que puede infectar otros programas, modificándolos para incluir una copia posiblemente evolucionada de sí mismo. Un virus puede propagarse a través de un sistema informático o de redes de computadoras usando la autorización de cada usuario para infectar sus programas. Cada programa que se infecta también puede actuar como un virus y por lo tanto la infección crece" [3].

Para 1985 surgió el virus Brain escrito por un programador Pakistaní de 19 años, Basit Farrq Alvi, y su hermano Amjad. Además de infectar la zona de arranque, cambiar el nombre del disco a "(c) Brain", el virus no hacía nada: no tenía carga útil y no corrompía los datos. *"Brain incluía una línea de texto que contenía los nombres de los programadores, direcciones y número de teléfono"* [6]. Fue introducido en Estados Unidos y el resto del mundo en copias ilegales de programas famosos que los hermanos vendían a los turistas.

Brain fue también el primer virus en utilizar la técnica de ocultamiento stealth: cuando detectaba un intento de leer el sector infectado, el virus mostraba los datos originales, como si no estuvieran infectados.

En diciembre de 1986 un alemán, Ralf Bunger, creó un programa al que llamó Virdem, éste podía copiarse a si mismo añadiendo su código ejecutable en los archivos .com y borrar archivos del sistema huésped.

En 1987 aparase el virus Vienna, capaz de infectar solo archivos .com sobre el sistema operativo MS-DOS 2.0, o superior. Berna Fix fue la primera persona capaz de neutralizar un virus. El código utilizado para neutralizar a Vienna fue publicado por Ralf Burger en su libro Virus informáticos, en el explica como el código del virus puede ser modificado para eliminar su capacidad de reproducción, pero también menciona cómo se crean los virus. Con esto da origen a lo que hoy se conoce como variantes.

"Robert Tappan Morris estudiante del MIT (Instituto Tecnologico de Massachusetts) crea el primer gusano de reproducción masiva, en 1988, fue capaz de infectar y colapsar el 10% de ARPANET, incluyendo la NASA y el MIT, durante 72 horas" [6]. Al igual que el gusano Christmas Tree, el virus enviaba copias ilimitadas de sí mismo y sobrecargaba las redes. El gusano aprovecho una vulnerabilidad en los sistemas operativos UNIX en las plataformas VAX y Sun Microsystems. Además, utilizo varios métodos innovadores para ganar acceso al sistema, como la recolección de contraseñas.

Chamaleon fue el primer virus polimórfico, apareció a inicio de los 90s, evoluciono a partir de dos virus, Vienna y Cascade. De este último se utilizaron características de autocifrado, no sólo le dan la capacidad de cifrarse, sino que su código también cambia con cada infección. Para 1996 surge BackOrifice, fue un troyano diseñado con herramientas que le permitían conectarse a un equipo de forma remota. Antes de concluir con esta década y dar paso al nuevo siglo, surge el virus Melissa.

Melissa comenzó a llegar a miles de correos en un archivo adjunto, al momento de abrirlo con Word 97 o 2000 el virus de macro se activa, abre el Outlook, y se auto envía a los primeros cincuenta contactos de la libreta de direcciones. Las

personas que recibían el correo lo abrían creyendo que era de alguien conocido, entonces infectaban sus equipos y continuaba la cadena de propagación. Este virus ocasionaba la salida de información confidencial de los usuarios, porque el archivo que se adjuntaba al correo podría ser cualquiera que estuviera en su sistema.

Inicia el nuevo siglo con la presencia del "gusano del amor": LoveLetter en Manila, Filipinas. Al igual que Melissa utiliza el correo electrónico para propagarse. El nombre se debe a uno de los asuntos incluidos en el mensaje "ILOVEYOU", estaba diseñado para enviar al atacante las contraseñas y los nombre de usuarios almacenados en los equipos infectados.

El año 2001 iniciaba con el virus de Anna Kournikova, creado con un popular generador de gusanos, el VBSWG (Visual Basic Script Worm Generator). Estos generadores toman algunas ideas de los virus polimórficos, contienen una serie de rutinas prefabricadas que son ensambladas para formar un virus a partir de una serie de opciones seleccionadas por el usuario.

En julio del 2001 CodeRed infecta a miles de decenas de servidores que ejecuten Microsoft Windows NT o Windows 2000, el gusano intenta ingresar al sistema a través del puerto 80, explotando una vulnerabilidad.

El gusano Slammer aparece en el 2003 infectando a menos computadoras que CodeRed y a diferencia de éste, actuó dos veces más rápido infectando a más del 90% de las computadoras vulnerables tan solo en 10 minutos después de iniciar su propagación, esto se debe a que duplica su área de propagación cada 8.5 segundos y alcanza 55 millones de equipos rastreados por segundo en solo 3 minutos, según datos proporcionados por CAIDA (Cooperative Association for Internet Data Analysis).

Bueno los gusanos están de moda ya que en el 2004 MyDoom se convierte en el gusano que más rápido se propaga por el correo electrónico, superando así a cualquier otro virus o gusano anterior. Una característica significativa de éste es que usa la "ingeniería social" para persuadir a los usuarios de abrir los archivos adjuntos del correo. Su objetivo principal era un ataque DDoS al grupo SCO (propietaria de uno de los sistemas UNIX más difundido) y Microsoft. En ocasiones este tipo de ataques son realizados para demostrar la efectividad de la red zombi y así poder venderla.

En la actualidad el código malicioso sigue en aumento y cada día surgen nuevas combinaciones que explotan cualquier vulnerabilidad que les permita sacar algún beneficio. Con el aumento en la utilización de los dispositivos de almacenamiento que se conectan a través del puerto USB, por ejemplo, teléfonos celulares, cámaras fotográficas, iPod, etc., han creado una vía de ataque altamente explotable por el código malicioso.

Referencias Capítulo 2

[1] Jesus De Marcelo. “Virus de Sistemas Informaticos e Internet”. Alfaomega.

[2] Richard B. Levin. “Virus informáticos: tipos, protección, diagnosis, soluciones”. McGraw-Hill, 1992.

[3] Fred Cohen. “Computer Viruses - Theory and Experiments”. North-Hollad, 1984.

[4] Fernando de la Cuadra. “Pharming, nueva técnica de fraude”. Panda Software, 2005.

[5] McAfee. “A Brief History of Malware”. McAfee System Protection Solutions Octubre del 2005.

[6] Cristian Borghello. “Cronología de los virus informáticos”. ESET para Latinoamerica, 2006.

[7] Rubén Bayud, Ingeniero en Sistemas de la empresa Trend Micro, publicado en “El Universal online”. Viernes 20 de febrero de 2004, Sección de Finanzas. http://www2.eluniversal.com.mx/pls/impreso/noticia.html?id_nota=38501&tabla=finanzas

[8] Christian Linacre, Gerente de Seguridad en Microsoft Latinoamérica, publicado en “El Universal online”. Miércoles 08 de Abril de 2009, Sección de computo. Disponible en: http://www.eluniversal.com.mx/articulos/53445.html

[9] Panda Security, “Índice de peligrosidad”. Disponible en: http://www.pandasecurity.com/spain/homeusers/security-info/about-malware/technical-data/date-4.htmn

[10] Panda Security, “La red Mariposa afectó a 13 millones de usuarios en 190 países y 31.901 ciudades diferentes”. Disponible en: http://www.pandasecurity.com/spain/homeusers/media/press-releases/viewnews.aspx?noticia=10102

[11] Websense Inc, empresa de seguridad en páginas de Internet, publicado en “La Jornada on Line”. Lunes 14 de Mayo del 2007.

[12] Penda Security, “Datos tecnicos”. Disponible en: http://www.pandasecurity.com/spain/enterprise/security-info/about-malware/technical-data/

[13] INFORME ANUAL PandaLabs 2009

[14] John F. Shoch y Jon A. Hupp. “The Worm Programs Early Experience with a Distributed Computation” Communications of the ACM, 1982.

[15] Symantec, Datos técnicos. Disponible en: http://www.symantec.com/es/es/security_response/writeup.jsp?docid=2002-041208-2143-99&tabid=2

[16] McAfee, publicado en “Universal online”. Miércoles 15 de Abril del 2009. Sección de Cómputo. Disponible en: http://www.eluniversal.com.mx/articulos/53554.html

[17] David Herrerías Corzo, Banamex, publicado “El Universal online”. Miércoles 25 Junio 2008. Sección de Cómputo. Dsiponible en: http://www.eluniversal.com.mx/articulos/47660.html

[18] Mattica, Laboratorio de Computo forense en México, publicado en “Milenio online”. El 11 de junio del 2009.

[19] Juan Pablo Castro, ingeniero de la firma Trend Micro, publicado en “El Universal onlinea”. Martes 15 de enero del 2008. Sección de finanzas. Disponible en: http://www.eluniversal.com.mx/finanzas/62156.html

[20] Brian Krebs, washingtonpost.com, “A Short History of Computer Viruses and Attacks”. Disponible en: http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26?start=15&per=18

[21] Infoplease, “Computer Virus Timeline”. Disponible en: http://www.infoplease.com/ipa/A0872842.html#axzz0wFAKaU00

[22] David Emm, “Ante amenazas cambiantes, soluciones cambiantes: una historia de los virus y los antivirus”. Disponible en: http://www.viruslist.com/sp/analysis?pubid=207270980

[23] Symantec, “Crimeware: Caballos de Troya y spyware”. Disponible en: http://www.symantec.com/region/mx/avcenter/cybercrime/trojans_spyware.html

[24] Alejandro Franco, “”Que es el spyware”. Disponible en: http://www.datacraft.com.ar/internet-spyware.html

[25] James Butler, Sherri Sparks, “Windows rootkits of 2005”. Disponible en: http://www.symantec.com/connect/articles/windows-rootkits-2005-part-one

[26] Nikolay Grebennikov, “Keyloggers: Diferentes implementaciones en el sistema operativo Windows (segunda parte)”. Disponible: http://www.viruslist.com/sp/analysis?pubid=207270921

[27] Panda Security, “Spam: mensajes de correo no solicitados”. Disponible en: http://www.pandasecurity.com/spain/enterprise/security-info/types-malware/spam/

[28] Gerald Scheidl, “Virus Naming Convention 1999 (VNC99)”. Disponible en: http://members.chello.at/erikajo/vnc99b2.txt

[29] Alegsa, “Técnicas de ocultamiento de lo virus”. Disponible en: http://www.alegsa.com.ar/Notas/60.php

Capítulo 3

Programas Antivirus

En este capítulo se hablará del funcionamiento de los programas antivirus, así como de su estructura. Se ha dedicado un capítulo completo a este tipo de herramienta debido a que es utilizado por la mayoría de usuarios.

3.1 ¿Qué es un Antivirus?

Desde los setentas empezó a surgir la necesidad de crear programas cuyo objetivo primordial era eliminar un virus en específico. Como fue el caso de Reaper. En la actualidad se utilizan los antivirus que son un software que puede detectar, evitar y tomar medidas con el fin de neutralizar o quitar el código malicioso. Su nombre está relacionado con los virus, pero actualmente son soluciones antimalware, capaces de detectar gusanos, caballos de troya, virus, etc.

Los antivirus tienen módulos residentes en memoria (TSR, Terminate and Stay Resident) que se encargan de impedir la entrada de cualquier virus y verifican constantemente las operaciones que intentan realizar cambios al sistema por métodos poco frecuentes. Éstos son activados antes de que se inicie cualquier programa para darle poco tiempo de ejecución a los virus y detectarlos antes de que alteren algún dato.

Dependiendo de cómo esté configurado el antivirus, el módulo TSR estará pendiente de cada operación realizada en los archivos (por ejemplo, copiado, modificación o creación) y todas las descargar de Internet, también vigilará las operaciones que intenten realizar un formateo al disco duro y protegerá los sectores de arranque de éste.

Además, el antivirus debe de utilizar al mínimo los recursos del sistema para realizar sus funciones y no afectar significativamente en el rendimiento de otras aplicaciones.

Los antivirus realizan tres tareas principales:

- Detención. Detectar si un código es un virus o no. De forma simplificada se utiliza un valor booleano: si, el código está infectado, o no. Para este fin el antivirus analiza los archivos (puede ser en tiempo real o a petición del usuario) en búsqueda de una amenaza. Uno de los problemas que se tienen en la detención es que un atacante puede crear un virus, el cual no será detectado por el antivirus durante un tiempo determinado, cuando el antivirus sea actualizado podrá detectar el virus, entonces el atacante diseñara otro, convirtiéndose en un ciclo.

- Identificación. Una vez detectada la amenaza se procede a describir de que se trata, tanto por su tipo (virus, gusanos, caballos de troya, etc.) y su nombre (Michelangelo, Invader, etc.).

- Desinfección. Es el proceso de prevenir o eliminar el código malicioso detectado. Previene la infección cuando un código malicioso es detectado al momento de intentar entrar al sistema. Lo elimina o desinfecta cuando se descubre que el sistema ya está infectado. El desinfectar no quiere decir que todo se vuelve aponer exactamente en el mismo estado en el que estaba antes de que el virus infectara la computadora. Debido a que algunos efectos causados por la carga útil no pueden ser revertidos.

El hecho de que la identificación y la desinfección requieran de la detención como requisito previo, hace de esta última la más importante de las tres tareas antes mencionadas.

3.2 Modelo de un Antivirus

Un antivirus está constituido por dos módulos principales, conocidos como Módulo de Control y Módulo de Respuesta.

El Módulo de Control realiza la *"Verificación de Integridad que posibilita el registro de posibles cambios en los archivos ejecutables y las zonas críticas de un disco duro"* [5].

El Módulo de Respuesta cuenta con una función de "Alarma" que consiste en detener la acción del sistema ante la sospecha de la presencia de un virus, gusano, etc. e informar al usuario de la posible existencia de éste por medio de un aviso en pantalla. Si la identificación ha sido positiva puede ofrecer la opción de erradicar la amenaza.

3.3 Métodos de detención

Así como los virus fueron cambiando con el paso del tiempo, también los antivirus tuvieron que evolucionar para ofrecer técnicas que permitan la detención del código malicioso, entre las cuales podemos incluir a:

3.3.1 Verificación de Integridad

Este método se encarga de verificar que algunos sectores sensibles del sistema no sean alterados sin el consentimiento del usuario. Se puede aplicar tanto a archivos como al sector de arranque de las unidades de almacenamiento. Calcula la suma de comprobación de cada archivo, mediante un algoritmo que puede ser el CRC[32], el que será único según su contenido.

El antivirus crea un registro por cada uno de los archivos que puede incluir los siguientes datos: nombre, tamaño, fecha de creación o modificación y la suma de comprobación. Cuando tiempo después se inicia la verificación de cada uno de los archivos serán explorados aplicándoles el CRC y así obtener un valor que es comparado con el que se guardó en el registro. Si ambos valores son iguales, se

[32] Código de Redundancia Cíclica. Consiste en verificar el número de bytes que forman un archivo, sin importar su longitud, y devuelve un valor de longitud fija como salida.

puede decir que el archivo no sufrió ningún cambio durante el tiempo que transcurrió entre el registro antiguo y el reciente.

Pero, si los valores son diferentes puede significar que un virus inyecto parte de su código en el archivo cambiando el valor obtenido en la reciente exploración (Fig. 3.1), entonces el antivirus tendrá que alertar al usuario de la modificación del archivo.

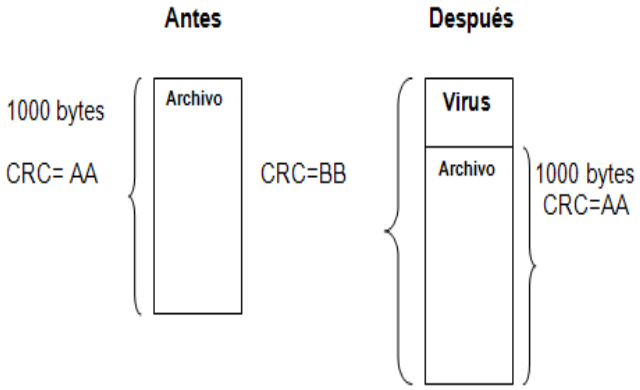


Fig. 3.1 Ejemplo de uso del CRC

Para obtener el registro de los archivos se debe de tomar una “foto” del contenido de la unidad de almacenamiento desinfectada con la cual se podrán hacer las comparaciones. El inconveniente es que se debe de estar seguro de que el sistema estaba limpio en el momento de la creación del registro.

Un verificador de integridad no puede detectar virus en los archivos recién creados, o en los que son modificados legítimamente, por ejemplo, mediante una actualización de software. Se necesita de la intervención del usuario para determinar si los cambios identificados son resultado de la actividad del virus o fueron hechos de forma legítima.

3.3.2 Exploración por firmas

Tradicionalmente, los antivirus han dependido en gran medida de la detención basada en “firmas” (también son conocidas como vacunas). Una firma es un

conjunto específico de bytes (una cadena de caracteres) que identifican exclusivamente a un virus, pero una que no sea propensa a encontrarse por accidente en un archivo que no ha sido infectado. Las firmas son altamente eficaces para la identificación de código malicioso o de sus variantes.

Se puede llegar a creer que existe una única secuencia de bytes en cada código malicioso que es utilizada por todos los antivirus para identificarla. Esto no es así, cada antivirus pueden utilizar cadenas de búsqueda y algoritmos (que son capaces de buscar, en cientos de miles firmas, múltiples patrones de manera eficiente) muy diferentes para detectar el mismo código malicioso.

El fabricante del antivirus genera una base de datos con las firmas, permitiéndole al software determinar si el archivo es una amenaza o no. Básicamente, se coteja cada archivo a analizar con la base de datos y, si existe coincidencia (es decir, existe en la base una firma que corresponde con el archivo), se identifica el archivo como código malicioso.

El proceso de generación de firmas puede variar dependiendo de cada fabricante, pero, por lo general está compuesto de los siguientes pasos:

1. Aparece un nuevo código malicioso.
2. El laboratorio de la empresa antivirus recibe una muestra de ese código.
3. El analista desensambla el código y crea la firma para la nueva amenaza.
4. El usuario actualiza el producto con la nueva base de firmas y comienza a detectar el código malicioso.

Este método posee las siguientes desventajas:

- La necesidad de mantener actualizada la base de datos.
- El programa no puede detectar código malicioso que no esté en la base de datos.

- El sistema debe de contar con una firma por cada variante de un mismo código malicioso.
- Cuando aparece una nueva amenaza debe de pasar cierto tiempo para que el laboratorio cree la firma correspondiente, dando la oportunidad de que la amenaza se propague.
- La firma debe de ser probada antes de enviarla a los usuarios, ya que puede causar conflictos con el software del antivirus, con el sistema operativo o con alguna aplicación instalada en el equipo.
- Es menos eficaz contra los virus polimórficos**.**

El tiempo que se tarda en generar una nueva firma es variable, depende de ciertas circunstancias como son: el tiempo que tarda el laboratorio en descubrir la nueva amenaza, las características del código malicioso, la dificultad para crear la firma, etc.

La exploración, también conocida como scanning, se ejecuta en el acceso de un dispositivo móvil (por ejemplo, disquete, memoria USB, etc.) al equipo o por demanda, se encargan de analizar partes del sistema solamente cuando el usuario lo ordena. Es utilizado en ocasiones especiales, por ejemplo cuando se cree que algún archivo está infectado.

Este método tiene como ventaja la identificación de un virus antes de que se ejecute el programa que lo contiene (sólo si la base de datos cuente con la firma), además presenta una baja incidencia en informes de falsos positivos (éste término será revisado en la sección 3.3.5).

A continuación se presentan dos ejemplos de firmas de virus:

- **96e1c622051e19ed5efbc8ab47e9c67**, firma en MD5[33] del gusano Messeenger.exe

[33] Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5.

- **134 178 156 177 9 51 219 241 94 28 193 220 86 193 214**, firma en hexadecimal del virus VBS/Lovelettr.

3.3.3 Bloqueadores de conducta

Los bloqueadores de comportamiento son programas residentes en memoria encargados de vigilar el comportamiento sospechoso y decidir si es malicioso o no: si el programa rebasaba un rango predeterminado de acciones aceptables, será bloqueado.

El bloqueador tiende a buscar dos tipos de comportamiento del código: Réplica, el código replicable sugiere fuertemente la presencia de un virus o gusano, es más fácil identificar un virus que se reproduce escribiendo una copia directa de sí mismo que una evolucionada de si (virus polimórfico); Daño Potencial, el código potencialmente dañino refleja la posibilidad de una carga útil. Este último comportamiento suele ser ineficiente en los casos donde no hay una carga útil o cuando no es evidentemente dañina.

Si el bloqueador de comportamiento detecta que un programa intenta abrir un archivo ejecutable y escribir en él, puede mostrar una advertencia donde le pide permiso al usuario para conceder el acceso al archivo. Desafortunadamente, estos eventos pueden ser excesivos y a menudo se vuelven menos aceptables.

El usuario tiene que tomar la decisión de detener o no el presunto comportamiento no deseado, en lugar del software. Además, cada clase de virus puede tener un comportamiento significativamente diferente, originando que el número de patrones que causan las infecciones tienda al infinito.

Con este método se puede detectar código malicioso desconocido (es decir, no identificado previamente), no requiere de una base de datos con las firmas de los virus conocidos y pueden ser capaces de funcionar en los sistemas ya infectados.

3.3.4 Análisis heurístico

El análisis heurístico surgió como respuesta a la necesidad de identificar amenazas desconocidas, tienen la capacidad de detectar un archivo malicioso aunque la base de datos no cuente con la firma correspondiente.

La heurística es definida por la Real Academia Española como “Técnica de indagación y del descubrimiento” y además aclara que: “En algunas ciencias, manera de buscar la solución de un problema mediante métodos no rigurosos, como por ejemplo, tanteo, reglas empíricas, etc.”. Existen más definiciones, pero esta última es la que mejor se aplica a la utilización de la heurística en tecnologías de antivirus.

La programación heurística, comúnmente es considerada como una de las aplicaciones de la inteligencia artificial y como herramienta para la resolución de problemas. Desde la perspectiva de los sistemas expertos, se construye bajo reglas extraídas de la experiencia y las respuestas generadas por tal sistema mejoran en la medida en que “aprende” mediante la adquisición de experiencias y así aumenta su base de conocimiento.

Con el paso del tiempo los analistas de virus fueron adquiriendo experiencia sobre las técnicas usadas por programas maliciosos, las cuales se utilizaron para crear una lista de características sospechosas, asignando un puntaje a cada una. Cuando el escáner analiza el código buscando estas características; si el puntaje supera una marca predefinida, el archivo es señalado como sospechoso o potencialmente malicioso

La exploración heurística es similar a la exploración por firmas, a diferencia de que no se buscan firmas específicas, sino ciertas instrucciones o comandos dentro de un programa que no se encuentra catalogado como una aplicación legitima.

Las instrucciones suelen estar relacionadas con mecanismos de replicación de los virus, la rutina de distribución de un gusano, la rutina de carga de un troyano, etc.

En 1989 surge el primer antivirus capaz de realizar un análisis heurístico y en sus inicios los métodos heurísticos no ofrecían oposición a los virus polimórficos, pero actualmente intentan detectar las rutinas de descifrado y la ruptura de las mismas.

Como ventaja de este método tenemos la capacidad de detectar tanto código malicioso conocido como desconocido. La desventaja que tiene es que es un método basado en la búsqueda de posibles actividades en lugar de patrones específicos y está lejos de ser una forma de detención fiable. Suele acusar falsamente a programas legítimos de ser virus, por ejemplo si la computadora cuenta con dos programas antivirus, uno detectaría como amenaza al otro y viceversa.

3.3.4.1 Tipos de heurística

Se pueden encontrar diferentes métodos de heurística que utilizan distintas reglas para evaluar los archivos y determinar si son código malicioso o no. A continuación se explicarán los tres métodos más utilizados:

1. Heurística genérica: se analiza qué tan similar es un objeto a otro, que ya se conoce como malicioso. Para que un archivo sea detectado como variante de un código malicioso, éste previamente debe de ser lo suficientemente similar al archivo previamente identificado.

2. Heurística pasiva: se intenta determinar, después de un análisis, las acciones que realizará el programa y si estas son sospechosas se detectará a éste como código malicioso.

3. Heurística activa: trata de crear un entorno seguro y ejecutar el código de forma tal que se pueda conocer cuál es el comportamiento del código. El virus no se ejecutaría en el equipo real y así no causaría daño. Este tipo de heurística también es conocida como “sandbox”, “virtualización” o “emulación”.

Asimismo, cada algoritmo posee diferentes niveles de profundidad. Con una menor profundidad del análisis heurístico (conocido también como modo seguro), menor será la probabilidad de que se detecte un código malicioso desconocido, se tendrá una menor emisión de falsas alarmas (falsos positivos) y menor uso del procesador. Con una mayor profundidad se incrementa la probabilidad de detención de código malicioso, emisión de alarmas y un mayor uso del procesador.

3.3.5 Falsos positivos y Falsos negativos

Cada uno de los métodos descritos anteriormente genera en mayor o menor medida errores, conocidos como falsos positivos y falsos negativos. Un falso positivo es cuando el antivirus anuncia que un archivo está infectado, cuando en realidad no es así. En el caso contrario tenemos los falsos negativos que se dan cuando el antivirus no puede detectar un virus en un archivo infectado (puede ser por la falta de firmas en la base de datos del antivirus).

Los falsos positivos se pueden producir cuando un patrón en el código del archivo coincide con el que se encuentra en la base de firmas de los virus. Esto puede ocurrir debido a una firma defectuosa o después de la desinfección inadecuada de un archivo.

En lo que concierne al método heurístico la eliminación de los falsos positivos no siempre resulta posible, porque el objetivo de la programación heurística no es producir el resultado “perfecto” sino uno “lo suficientemente bueno”.

Un falso positivo puede hacer que los archivos legítimos, deban suprimirse, haciendo que el sistema operativo o el programa ya no funcione correctamente. Como ejemplo tenemos *"la actualización 5958 liberada por la empresa McAfee, provocando un falso positivo cuando confundió un virus llamado W32/Wecorl.a con el archivo svchost.exe*[34] *del sistema operativo Windows XP SP3, causando el inmediato reinicio del sistema y aunque puede volver a encender, seguirá lanzando la alarma hasta que se instale una nueva actualización que corrija el problema"* [1]. *"Según la empresa se afecto al 0,5% de de sus 125 millones de clientes"* [2].

3.4 ¿Cómo comprobar el funcionamiento de un programa Antivirus?

Cuando instala un programa antivirus abra pensado si ¿estará funcionando? o ¿lo abre instalado bien?, estas y otras preguntas más pasaran por su mente. Una posible solución es la utilización de un archivo llamado EICAR test file, traducido al español archivo de prueba EICAR.

La organización EICAR (European Institute for Computer Antivirus Research; en español: Instituto Europeo para la Investigación de los Antivirus Informáticos), desarrollo en 1996 lo que hoy se conoce como EICAR test file. Tiene como objetivo probar que el antivirus se encuentre activo, dándole a éste la oportunidad de detectarlo durante la exploración del equipo, no representa ningún riesgo para la computadora, porque no es realmente un virus.

La mayoría de antivirus son capaces de reconocerlo. Éstos lo detentan como un virus llamado "EICAR-AV-Test" o similar. Para usar el archivo EICAR puede ser descargado de las direcciones mencionadas en la figura 3.2 o generar uno nuevo. En la Fig. 3.3 podemos observar una de las alertas que pueden ser mandas por los antivirus al tratar de descargar el archivo.

[34] Es el encargado de ejecutar los servicios que corren desde una librería dinámica en lazada. Cuando se inicia la computadora se ejecuta este proceso que comprueba el registro y hace una lista de servicios que necesitan ser cargados para el correcto funcionamiento del sistema.

http://www.eicar.org/download/eicar.com

http://www.eicar.org/download/eicar.com.txt

http://www.eicar.org/download/eicar_com.zip

http://www.eicar.org/download/eicarcom2.zip

Fig. 3.2 Direcciones electrónicas

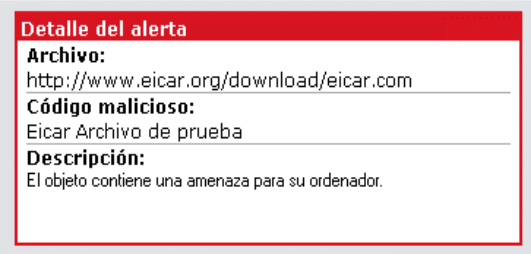


Fig. 3.3 Detalle de la alerta.

La primera dirección, la que se muestra en el ejemplo de alerta, puede servir para verificar que el antivirus intercepta las descargar de Internet y su posterior ejecución. La segunda opción permite visualizar el código del archivo en el navegador. Las dos últimas con tiene el mismo archivo, la única diferencia es que se descargan en archivos comprimidos (.zip).

El EICAR test file está constituido por 68 caracteres ASCII, los cuales se presenta a continuación:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Para crear el archivo de prueba, debe de copiar y pegar el código mostrado anteriormente en el bloc de notas, guarde el archivo con el nombre que desee y con extensión .COM. Si transcribe el código, ponga especial atención en el tercer carácter (X5O…..) es la letra “O” y no el número cero.

Como una opción adicional, *“al código se le puede agregar espacios en blanco o los caracteres tab, LF, CR, y CTRL-Z. La única condición es que no debe de exceder los 128 caracteres de longitud y sólo utiliza letras mayúsculas”* [3].

En el caso de que el archivo EICAR.COM se llegara a ejecutar no debe de preocuparse por su computadora, recuerde que no hay peligro de daño alguno (no es un virus real), lo único que observara será la aparición de una ventana DOS con el siguiente texto:

EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

Referencias capítulo 3

[1] InfoSpyware, http://www.infospyware.com/blog/mcafee-antivirus-falso-positivo-w32wecorl-a-deja-sin-funcionar-a-millones-de-pcs-en-el-mundo/

[2] McAfee, publicado en “ABC.ES on-line”. Jueves 22 de Abril del 2010. Disponible en: http://www.abc.es/hemeroteca/historico-22-04-2010/abc/Tecnologia/mcafee-reconoce-cientos-de-miles-de-afectados-por-el-fallo-de-su-antivirus_ 14084132909.html

[3] eicar, “The Anti-Virus or Anti-Malware test file”. Disponible en: http://www.eicar.org/anti_virus_test_file.htm

[4] Markus Schmall, “Heuristic Techniques in AV Solutions: An Overview”. Disponible en: http://www.symantec.com/connect/articles/heuristic-techniques-av-solutions-overview

[5] Trucos Windows.net, “Estudio sobre virus informáticos parte 2”. Disponible en: http://www.trucoswindows.net/conteni5id-6-SEGURIDAD-Estudio-sobre-virus-informaticos-parte-2.html

[6] Segu-Info,“Virus - Programas Antivirus”. Disponible en: http://www.segu-info.com.ar/virus/programa.htm

[7] Alisa Shevchénko, “Evolución de las tecnologías de detección de códigos nocivos”. Disponible en: http://www.viruslist.com/sp/analysis?pubid=207270954

Capítulo 4

Técnicas de prevención contra código malicioso

Para finalizar este trabajo se mencionan cuatro elementos fundamentales, que son: las políticas, concientización de los usuarios, reducción de vulnerabilidades y la disminución de amenazas. Con esto se busaca ayudar a prevenir incidentes ocasionados por el código malicioso dentro de una organización.

Algunas de las técnicas proporcionadas en éste trabajo pueden ser implementadas por usuarios que se encuentran en sus hogares, y estén interesados en mejorar la protección de su información, entre ellas se encuentran las políticas de prevención.

4.1 Políticas

Una política puede entenderse como una regla que hay que seguir obligatoriamente, pueden ser enunciadas de forma positiva o negativa. En forma positiva la política puede indicar qué debe de hacerse y, algunas veces, cómo. Las prohibiciones son un ejemplo de políticas negativas.

Una política de prevención contra el malware debe de ser planteada de forma general para poder proporcionar flexibilidad en su aplicación y disminuir la necesidad de actualizarla de forma frecuente. Es importante recordar que una política no constituye una garantía para la seguridad de la organización, pero en conjunto con los demás elementos pueden hacer frente.

Se puede dar el caso de que ciertas políticas no sean aceptadas por los usuarios, sobre todo por aquellos que serán afectados de forma directa. Para lograrlo se les debe de dar la oportunidad de revisarlas y hacer comentarios sobre ellas antes de implementarlas.

Entre los propósitos más comunes que debe de cumplir una política se encuentran:

- La protección de la información.
- Establecer las reglas que guíen el comportamiento de los usuarios y los administradores del sistema.
- Autorizar al personal de seguridad para vigilar e investigar.
- Ayudar a minimizar el riesgo.
- Ayudar a hacer partícipe, al personal, en los esfuerzos de la compañía para asegurar sus activos.

4.1.1 Elementos de las políticas

De acuerdo a la OCDE[35] los elementos de las políticas son: [1]

1. *Concientización. Los participantes deberán ser consientes de la necesidad de contar con sistemas y redes de información seguros, y de tener conocimientos de los medios para ampliar la seguridad.*
2. *Responsabilidad. Todos los participantes son responsables de la seguridad de los sistemas y redes de información.*
3. *Respuesta. Los participantes deben de actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.*
4. *Ética. Los participantes deben respetar los intereses legítimos de terceros.*
5. *Democracia. La seguridad de los sistemas y redes de información debe de ser compatible con los valores esenciales de una sociedad democrática.*
6. *Evaluación del riesgo. Los participantes deben de llevar a cabo evaluaciones de riesgo.*
7. *Diseño y realización de la seguridad. Los participantes deben de incorporar la seguridad como un elemento esencial de los sistemas y redes de información.*

[35] Organización para la Cooperación y el Desarrollo Económico

8. *Gestión de la seguridad. Los participantes deben de adoptar una visión integral de la administración de la seguridad.*
9. *Reevaluación. Los participantes deben de revisar y reevaluar la seguridad de su sistema y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad*.

4.1.2 Algunas políticas útiles

En la publicación del Instituto Nacional de Estándares y tecnología (NIST) titulado "Guide to Malware Incident Prevention and Handling" [2], se menciona una serie de políticas que pueden ayudar a la prevención de incidentes por código malicioso:

- Requerir la exploración de los medios ajenos a la organización antes de que sean usados.

- Exigir que los archivos adjuntos del correo electrónico, incluyendo los archivos comprimidos (por ejemplo, los archivos con extensión .zip), sean guardados en las unidades locales para ser escaneados antes de ser abiertos.

- Prohibir el envío o la recepción de ciertos tipos de archivos (por ejemplo, los archivos con extensión .exe) vía correo electrónico.

- La restricción o prohibición del uso de software innecesario, como las aplicaciones de usuario que se utilizan a menudo para transferir malware (por ejemplo, el uso personal de la mensajería instantánea (Chat) externos, servicios peer-to-peer para compartir archivos, etc.), y los servicios que no son necesarios o duplican los equivalentes proporcionados por la organización (por ejemplo, el correo electrónico) y podrían contener vulnerabilidades adicionales que pueden ser explotadas por malware.

- La restricción en el uso de los privilegios de administrador por los usuarios, ayuda a limitar los privilegios a disposición de los programas maliciosos introducidos en los sistemas por los usuarios.

- Exigir que los sistemas se mantengan al día con las actualizaciones del sistema operativo, aplicaciones y parches.

- Restricción en el uso de medios extraíbles (por ejemplo, disquetes, CD, USB), en particular en sistemas que tienen un alto riesgo de infección, tales como áreas de acceso al público.

- Especificar qué tipos de programas de prevención (por ejemplo, el software antivirus, detección de spyware, y utilidades de eliminación) son necesarios para cada tipo de sistema (por ejemplo, servidor de archivos, servidor de correo electrónico, servidor proxy, estación de trabajo, asistente personal digital [PDA]) y de aplicación (por ejemplo, cliente de correo electrónico, navegador web), y una lista de los requisitos de alto nivel para la configuración y el mantenimiento del software.

- Permitir el acceso a otras redes (incluidas Internet) sólo a través de los mecanismos aprobados y garantizados por la organización.

- Requerir cambios en la configuración del cortafuegos (éste término será revisado en la sección 4.3.1) para ser aprobados a través de un proceso formal.

- Restricción en el uso de dispositivos móviles en redes de confianza.

4.2 Concientización

Se considera que los usuarios han sido y siempre serán el punto más débil, el código malicioso toma ventaja de su ignorancia. La ingeniería social se está convirtiendo en una de las formas más comunes en que los atacantes hacen contacto con los usuarios, tratan de convencerlo de descargar y ejecutar archivos, que comúnmente, llegan a ellos por medio del correo electrónico.

El hecho de que los usuarios sean de los primeros en enfrentarse contra el código malicioso, debe de ser motivo suficiente para que sean armados con el conocimiento para identificar y manejar los incidentes ocasionados. Para esto el usuario requiere de una formación, capacitación y sesiones de sensibilización que les permita cumplir con su parte.

La idea de crear un programa de concientización es explicar las reglas necesarias para el buen uso de un sistema de información. Estos programas deben de incluir una orientación acerca de la prevención de incidentes ocasionados por el malware y así poder ayudar a disminuir su frecuencia y gravedad.

Los usuarios son una parte importante en la prevención de incidentes, deben de ser consientes de las forma en que el código malicioso entra en los sistemas, los infecta y se propaga. Además, de la incapacidad de los controles técnicos para evitarlos.

Un usuario capacitado puede ayudar a prevenir la propagación de los gusanos que ingresan al sistema por los archivos adjuntos del correo electrónico, los cuales necesitan de una persona para ser ejecutados. El mismo usuario puede ser capaz de detectar si el servicio de red disminuye su velocidad y comentarlo al administrador.

El usuario debe de comprender que no sólo las herramientas de seguridad actualizadas y configuradas deben de protegerlo, sino que sus propios hábitos pueden ofrecen la primera y más importante barrera contra el malware.

"En México una de las principales actividades sociales en línea es el correo electrónico, con un 75% y le sigue la mensajería instantánea, con el 59%" [4], como se puede observar en la figura 4.1. Éste tipo de hábitos pueden ocasionar perdidas o daños, si no son manejados adecuadamente, a la organización y aquellos usuarios que se encuentran en sus casas.

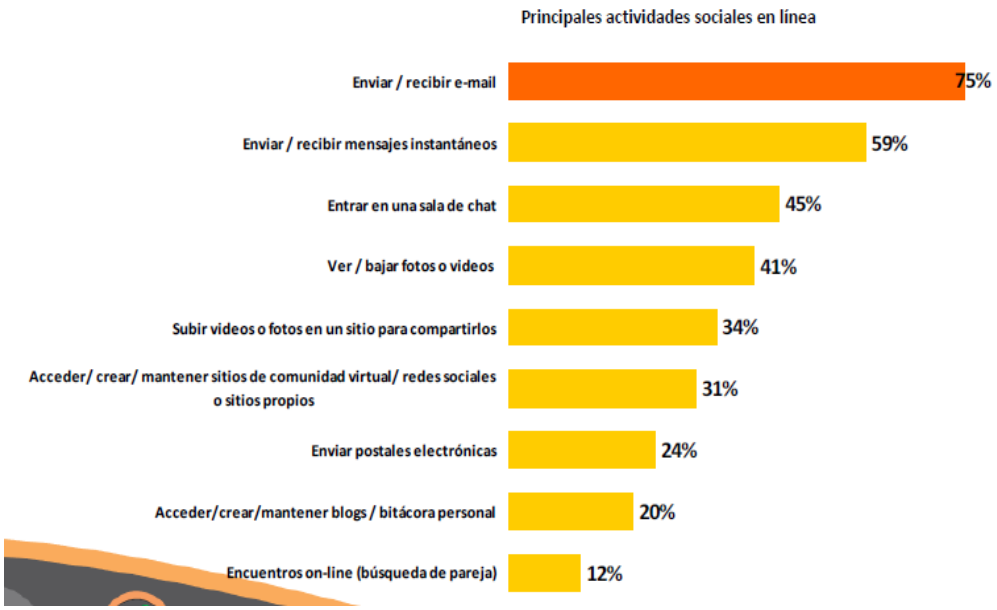


Fig. 4.1 Principales actividades sociales en línea [4]

No se trata de que el usuario deje de utilizar los servicios ofrecidos por Internet, la idea es que tome precauciones y mejore la forma en que los utiliza. A continuación se presentan algunos ejemplos de buenas prácticas: [2]

- *No abrir correos electrónicos o archivos adjuntos que parezcan sospechosos, sobre todo si son de remitentes desconocidos.*
- *No hacer clic en las ventanas emergentes (pop-up) que puedan parecer sospechosas.*
- *No visitar sitios Web que puedan contener código malicioso.*

- *No abrir archivos con extensiones que puedan estar asociados con programas maliciosos (por ejemplo, .bat, .com, .exe, .vbs).*
- *No desactivar los mecanismos de seguridad adicionales (por ejemplo, el software antivirus, detección de spyware y utilidad de eliminación, cortafuegos personal).*
- *No descargar o ejecutar aplicaciones de fuentes no confiables*.

Tal vez la insistencia que se tiene con el tema del correo electrónico pueda parecer tediosa o incluso ridícula, pero su mala utilización, no solo causaría la instalación de un programa malicioso, sino que el hecho de responder a un correo sospechoso puede conllevar consecuencias no deseadas.

Por ejemplo, una de ellas es la posible recepción de más correos basura (spam) o un intento de fraude. Cuando se responde a este tipo de correos electrónicos, los atacantes son capaces de detectar automáticamente, a través de sus sistemas, las cuentas vivas o atendidas. Si queda registrado que un correo basura ha sido abierto o contestado, los atacantes insistirán enviando más correo basura o fraudulento en un intento de realizar más negocio con la persona que se ha podido mostrar interesada o crédula.

Regresando al tema de las organizaciones, estas deben de hacer que los usuarios sean capaces de identificar una posible infección del equipo, cómo reportarla, y lo que pueden hacer para ayudar en su tratamiento (por ejemplo, actualizar el software antivirus, iniciar la exploración del equipo en busca de una amenaza).

El usuario debe de ser consciente de los cambios temporales que pueden surgir en el intento de contener la infección del sistema, como puede ser la desconexión, de los equipos infectados, de la red y el bloque de ciertos tipos de archivos provenientes del correo electrónico.

Las organizaciones deben de incluir en su programa de sensibilización las técnicas que los delincuentes utilizan para engañar a los usuarios para que revelen la información. Además, deben de incluir en el programa algunas recomendaciones para evitar los taques de phishing. A continuación se presentan algunas recomendaciones: [2]

- *Nunca responda a solicitudes recibidas por correo electrónico que desean obtener información financiera o personal. Las organizaciones no deberían pedir información por e-mail, ya que el correo electrónico es susceptible a ser controlado por terceros quienes no están autorizados. En su lugar, llame al número telefónico legitimo de la organización, o si se conoce la dirección del sitio Web de ésta consúltela en el navegador Web. No utilice la información proporcionada por el e-mail.*
- *No proporcionar contraseñas, números PIN, u otros códigos de acceso en respuesta a correos electrónicos o ventanas emergentes no solicitadas. Sólo ingrese esa información en la dirección del sitio Web de la organización.*
- *No abra archivos adjuntos de correos electrónicos sospechosos, incluso si provienen de remitentes conocidos. Si un archivo adjunto es recibido de forma inesperada, contacte al emisor (de preferencia por un método que no sea e-mail, como el teléfono) para confirmar que el archivo adjunto es legítimo.*
- *Cuando realice transacciones en línea (pagos, compras, transferencias) compruebe que usa una conexión segura (protocolo HTTPS, validez y vigencia del certificado).*

Es importante recordar que los usuarios día con día manejan contraseñas que les permiten el acceso a los diferentes sistemas informáticos, por ejemplo el sistema operativo, el chat, el correo electrónico. Por desgracia muchos usuarios manejan contraseñas débiles que bien pueden ser descubiertas con facilidad.

Los gusanos como Conficher cuentan con la capacidad de consultar un listado de más de 200 contraseñas que son comúnmente utilizadas por los usuarios, verifica si alguna de estas funciona. Encaso que le permita el acceso, realiza una copia de esta en un equipo remoto.

En ocasiones la utilización de contraseña fuerte puede causarle complicaciones al usuario, por esta razón se recomienda utilizar contraseñas fuertes y recordables. El usuario puede mostrarse ingenioso, realizando una combinación de letras mayúsculas o minúsculas, agregarle uno o das números, tal vez adicionar caracteres especiales como son: $, #, o %. Las siguientes contraseñas son consideradas fuertes: JoseEntr@, Contraz3na#, UNOuno1-.

A pesar de que la organización instruya a sus usuarios sobre los problemas que genera el malware, éstas no deben basar la seguridad informática de la empresa en un único método de prevención, sino que los programas de concientización deben de ser un complemento a otras medidas de seguridad.

4.3 Reducción de Vulnerabilidades

Como ya se había mencionado anteriormente una vulnerabilidad es cualquier debilidad que al ser explotada causa daño al sistema. Un fabricante de software se enfrenta a dos situaciones diferentes cuando se descubre una vulnerabilidad: que sea conocida públicamente, o que no. Cuando se dan a conocer al público antes de que se tenga la actualización correspondiente, los atacantes aprovechan la oportunidad para crear programas malicioso y así infiltrarse en los sistemas desprotegidos.

En ocasiones los clientes o usuarios acusan a los fabricantes de tardarse demasiado en ofrecer una solución a la vulnerabilidad. Su principal preocupación es que “perciben” el peligro de utilizar ese software. Para un fabricante, éste tipo de situaciones no le convienen, ya que dejan su imagen en entredicho.

Cuando la vulnerabilidad no se hace pública, quedando en secreto entre el descubridor y el fabricante, se lleva un ritmo para solucionarla muy distinto al primero. Los clientes no se sienten en peligro y el fabricante no sufre presión por los medios de comunicación, permitiendo que se busque una solución con más calma, por parte del fabricante.

El tiempo que se tarda un fabricante en dar solución a una vulnerabilidad que no es pública, puede variar de entre unos cuantos días hasta más de un año. En el estudio realizado por Hispasec Sistemas titulado *"¿Cuánto tardan los grandes fabricantes de software en arreglar una vulnerabilidad?"*[5], se concluyo que el promedio es de 6 meses para dar solución a una vulnerabilidad, independientemente de su gravedad. En este estudio participaron los siguientes fabricantes: HP, Computer Associates, Adobe, Apple, Microsoft, Novell, Symantec, Oracle, IBM y Sun.

Cuando se sabe de una vulnerabilidad se debe de proceder a eliminarla, para esto existen varios métodos, como son la aplicación de parches (éste término será revisado en la siguiente sección) para actualizar el software, o volver a configurarlo dejando deshabilitado el servicio vulnerable.

Retomando el tema de los dispositivos de almacenamiento masivo que se utilizan a través de conexiones del tipo USB, como las memorias, los teléfonos celulares, etc., representa un punto vulnerable para cualquier sistema informático, debido a su uso masivo y a la facilidad de conexión.

El malware se vale de un archivo llamado **autorun.inf** que se encarga de ejecutar el código malicioso (generalmente un archivo ejecutable) en forma automática cuando el dispositivo es insertado en la computadora.

Esta funcionalidad se encuentra habilitada por defecto, entonces el sistema operativo busca en el dispositivo que fue insertado un archivo de texto plano (autorun.inf). Si lo encuentra, ejecuta las instrucciones especificadas en el mismo.

Es importante resaltar que el archivo autorun.inf no es el malware y que sólo enlaza un archivo ejecutable que si podría serlo. Para el ejemplo que se muestra en la Fig. 4.2 el código malicioso que se ejecuta es el bltkcde.exe. La cantidad de malware que utiliza este tipo de archivos para propagarse es indefinida.

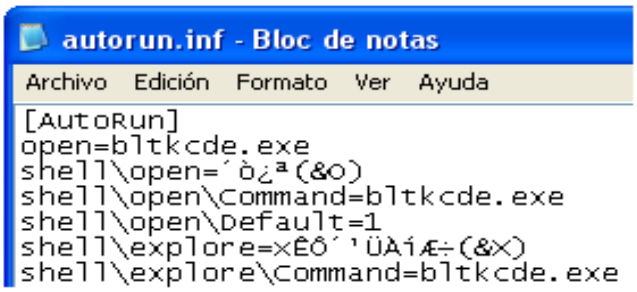


Fig. 4.2 Archivo autorun.inf

Cuando la computadora queda infectada, cualquier dispositivo que se inserte en está obtendrá una copia del código malicioso y así podrá infectar de forma sucesiva una gran cantidad de computadoras que no cuenten con una herramienta capaz de detectarlo.

Por este motivo, se debe de prevenir su ejecución. En la siguiente página web puede encontrar varias direcciones para descargar un parche que desactive la ejecución automática del archivo autorun.inf, dependiendo del tipo de sistema operativo que tenga, http://blogs.eset-la.com/laboratorio/2009/08/29/elimina-autorun-dispositivos-usb/.

4.3.1 Parches

Un parche es código que se desarrolla adicionalmente para resolver algunos problemas (comúnmente llamados “bugs”) en el software. Los parches son proporcionados por los fabricantes, en un intento de corregir errores en sus productos. Con frecuencia el parche cumple con sus objetivos, pero en ocasiones corrige un problema y genera otro.

Cuando a un programa se le realizan pruebas de seguridad y éste las resiste, se considera que es seguro. Sin embargo, existen casos donde no sólo se encuentra un problema de seguridad grave, sino varios. Esto origina un esfuerzo por generar los parches que reparen o restauren la seguridad del sistema, si no es que lo hacen más inseguro.

Los fabricantes publican cada día nuevos parches, y a menudo es muy difícil que los usuarios e incluso los administradores de las redes estén al corriente de todos ellos. Los atacantes aprovechan el momento en que se pública un nuevo parche, lo analizan e identifican la vulnerabilidad, así pueden desarrollar el código malicioso que podrá explotarla. Por lo tanto, en el momento que es lanzado un parche, se crea un intervalo vulnerable para la mayoría de las organizaciones que no implementan el parche.

Los atacantes se aprovechas de las vulnerabilidades sin importar donde estén, pueden explotarlas incluso si los parche están disponibles, ya que muchas maquinas siguen siendo vulnerables durante un largo periodo después de que un parche está disponible, y en ocasiones la computadora nunca cuenta con la actualización.

Para los usuarios domésticos, deben de darse tiempo de instalar las actualizaciones necesarias. La mayoría de los fabricantes proporcionan los parches gratis, envían un correo o a través de las actualizaciones automáticas (este es un sistema automatizado que notifica a un usuario de que hay una actualización disponible para un determinado programa, y los guiara por el proceso de descarga e instalación).

En caso de tener el sistema operativo de Microsoft Windows, el segundo martes de cada mes se liberan los parches necesarios para solucionar diferentes vulnerabilidades.

4.3.2 Privilegio mínimo

En el caso de Windows XP, cuando es instalado se crea un usuario por defecto conocido como Administrador, este usuario se encuentra habilitado para realizar cualquier tipo de tarea y acceder a cualquier lugar del sistema. El código malicioso aprovecha esta configuración, ya que dispone de los permisos necesarios para acceder a cualquier recurso crítico del sistema (por ejemplo, los registros, directorios del sistema operativo, archivos temporales, etc.).

Como buena práctica de seguridad se recomienda la creación de una cuenta con privilegios restringidos una vez que sea instalado el sistema. Si ocurre un incidente, los efectos causados por el código malicioso serán minimizados.

4.4 Mitigación de amenazas

Existen varios tipos de herramientas de seguridad que pueden ayudar a disminuir las amenazas por malware: los programas antivirus, anti-spam, sistemas de prevención de intrusos (IPS), cortafuegos y router.

Los programas antivirus son de los más utilizados, debido a su gran importancia se les dedicó el capitulo anterior. En esta sección se tratarán las herramientas restantes.

4.4.1 Anti-spam

Existen varias tecnologías conocidas como anti-spam, de las cuales sólo se revisaran las listas de confianza. Debido a que algunas de ellas únicamente son implementadas por grandes organizaciones como son: Proveedores de Servicios de Internet (ISPs), administradores de sistemas corporativos, etc.

4.4.1.1 Listas de confianza

Las listas de confianza son clasificadas en dos categorías: listas negras y blancas. Una lista blanca se defina cómo un conjunto de remitentes que el destinatario considera de confianza y de quien se desea recibir mensajes. Los usuarios pueden crear sus listas blancas, para asegurarse de que el correo remitente de confianza no sea bloqueado por las herramientas anti-spam.

Por otro lado, las listas negras ayudan a identificar los correos spam. El anti-spam es responsable de bloquear o enviar a una carpeta especial a los correos de un remitente que se encuentra en la lista negra. Organizaciones como Spamcop, Spamhous se encargan de mantener las listas negras.

Por ejemplo, *"usted tiene una cuenta de correo electrónico con un proveedor gratuito de cuantas (Hotmail, gmail, yahoo, etc.). Ahora imagine que el spammer spammer@malicioso.com envía un correo spam a su cuenta. El proveedor de servicios ha actualizado la lista negra, en donde se encuentra la dirección spammer@malicioso.com, debido a que éste ha enviado antes correos spam a otros usuarios y ha sido identificado. Cuando el mensaje llega al servidor de correo, la herramienta anti-spam de su proveedor busca la dirección del remitente en la lista negra y la encuentra, de manera que cataloga ese correo como spam y la redirige a la carpeta de correo no deseado*". [9]

Para administrar las listas en Hotmail deben de seguir los siguientes pasos:

- Dar click en el menú de opciones que se encuentra del lado derecho de la página web y seleccionar la opción de Desactivado (Fig. 4.3).

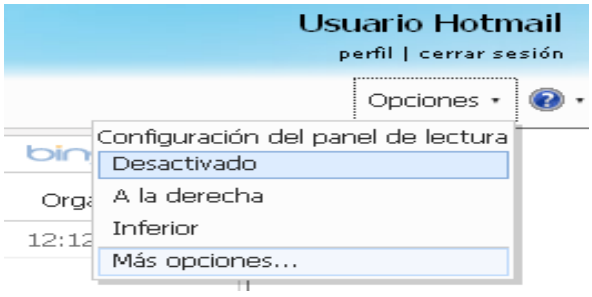


Fig. 4.3 Opciones

- En la opción de correo no deseado, seleccione remitentes seguros y bloqueados (Fig. 4.4).

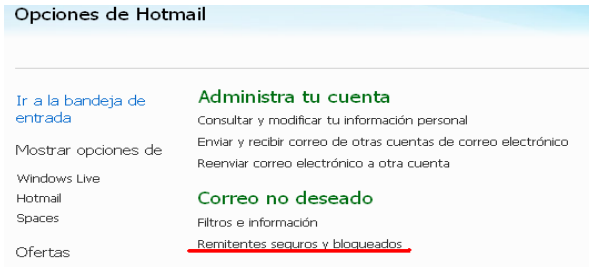


Fig. 4.4 Desactivado

- Aquí puede escoger correo seguro o contactos bloqueados (Fig. 4.5).

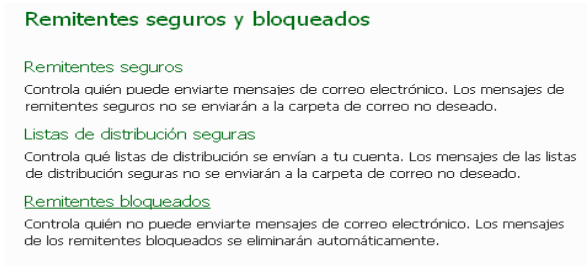


Fig. 4.5 Remitentes Seguros y bloqueados

- Si desea agregar contactos a la lista blanca escoja remitentes seguros. Escriba el correo en la sección de remitente y haga clic en agregar en la lista. Puede verificar que el correo sea agregado a la lista de remitentes seguros, en la parte derecha de la ventana (Fig. 4.6).

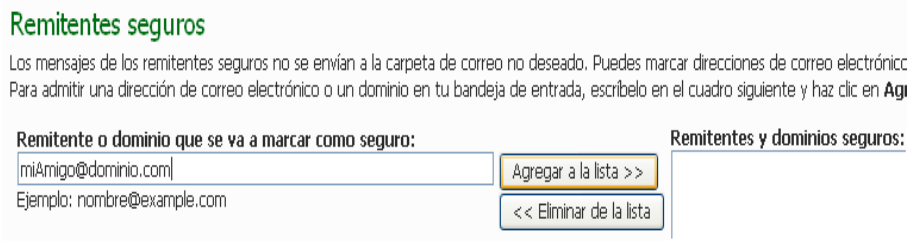


Fig. 4.6 Remitentes Seguros

- Para agregar un remitente a la lista negra, hacer clic en “Remitentes bloqueados” (Fig. 4.5), introduzca el correo y haga clic en agregar a la lista (Fig. 4.7).

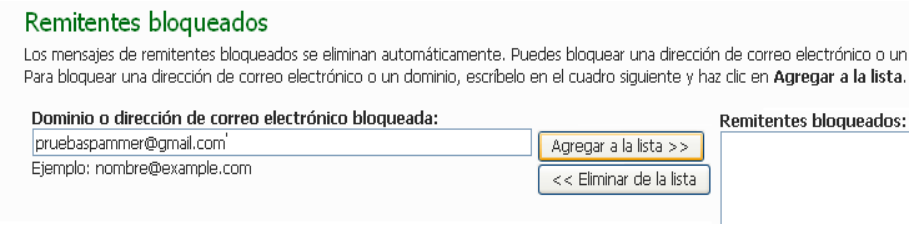


Fig. 4.7 Remitentes bloqueados

4.4.2 Herramientas de detección de Spyware

Prevenir los incidentes de spyware es importante, no sólo porque esté puede violar la privacidad del usuario, sino que además causa problemas frecuentes en los sistemas, entre los cuales podemos encontrar una disminución en el rendimiento o causar la inestabilidad en algunas aplicaciones.
Se pueden encontrar herramientas de detección de spyware especializadas en una forma determinada de código malicioso, pero la mayoría cuenta con algunas de las siguientes capacidades [2]:

- *Supervisar el comportamiento de las aplicaciones más susceptibles a ser utilizadas para colocar spyware, como pueden ser los navegadores web y los clientes de correo electrónico.*
- *Realizar exploraciones periódicas de los archivos, la memoria y los archivos de configuración conocidos por spyware.*
- *La identificación de varios tipos de spyware, incluyendo códigos maliciosos como troyanos y cookies de seguimiento.*
- *Poner en cuarentena o eliminar archivos del spyware (porque a la mayoría de los archivos del spyware no se les aplica la desinfección).*
- *Controladores para monitorear la red y la configuración del Shell de Windows.*
- *Monitoreo de los procesos y programas que se cargan automáticamente en el arranque del equipo.*
- *Prevención de varios métodos de instalación del spyware, incluidos los anuncios en ventanas emergentes, cookies de rastreo, instalación de plug-in, y secuestro del navegador.*

Los programas de detección y eliminación de spyware suelen depender de firmas, al igual que los programas antivirus, y que son similares a estos. Las herramientas son eficaces en el reconocimiento de las amenazas conocidas y las variantes de estas, pero tiene capacidades diferentes para detectar amenazas desconocidas.

Así que es necesario que el software de detección de spyware sea mantenido al día con la última firma y que esté actualizado.

4.4.3 Sistemas de prevención de intrusos (IPS)

Un sistema de prevención de intrusos realiza la detención de paquetes, analiza el tráfico de red para identificar y detener cualquier actividad sospechosa. Los IPS reciben los paquetes, los analizan, deciden si el paquete es aceptable y en caso de serlo permiten su paso.

Una gran parte de productos IPS basados en red utilizan la combinación de firmas y análisis de protocolos de red, llevan a cabo una comparación entre las actividades realizadas en aplicaciones de uso frecuente (por ejemplo, servidores de correo electrónico, servidores web) y el comportamiento que se espera de las actividades potencialmente maliciosas.

Existen IPS especiales, comúnmente conocido como software de mitigación de ataques DDoS, son un intento de detener los ataques mediante la identificación del flujo inusual en la red. Éstos productos son diseñados principalmente para detener los ataques DDoS dirigidos a una organización, también se pueden implementar en la identificación de gusanos.

Si un usuario desea proteger su computadora pude utilizar un sistema IPS basado en anfitrión. Este software supervisa las características de una sola computadora y los acontecimientos que ocurren dentro de ésta, en otras palabras, realiza un seguimiento de todas las llamadas realizadas en el sistema y las compara con políticas basadas en comportamientos “normales”.

Como ejemplos de las actividades que pueden ser controladas por los sistemas IPS tenemos al tráfico de red, los registros del sistema, procesos en ejecución, el

acceso y modificación de archivos, los intentos para aumentar los privilegios en el sistema y los cambios de configuración de la aplicación.

Cuando los IPS monitorean los cambios realizados a los archivos, suelen detectar un virus que intente infectarlos o a un caballo de Troya que busque reemplazarlos, además detectan el uso de herramientas de ataque entregadas por el código malicioso, como son los rootkits.

Así como el software antivirus o el de detención de spyware pueden causar falsos positivos o falsos negativos, un sistema IPS basado en anfitrión no se salva de cometer estas fallas.

Para terminar, un sistema IPS puede ser útil en la identificación de las amenazas que utilizan los servicios de red que no son controlados por el software antivirus, como son los DNS. Recordando que los DNS son atacados por el pharming.

4.4.4 Cortafuegos (Firewall)

Los cortafuegos son como una barrera entre los usuarios finales, corporaciones o individuos, y los sistemas informáticos externos. Permiten controlar el tráfico de la red, es decir, los datos que son enviados y recibidos a través de la red por aplicaciones ejecutadas en el ordenador.

Los cortafuegos son el mecanismo encargado de proteger una red confiable de una que no lo es, por ejemplo Internet (Fig. 4.8). Estos no ayudan a defenderse de ataques o errores provenientes del interior de la red “segura”, así como tampoco ofrecen protección una vez que el atacante lo traspasa.

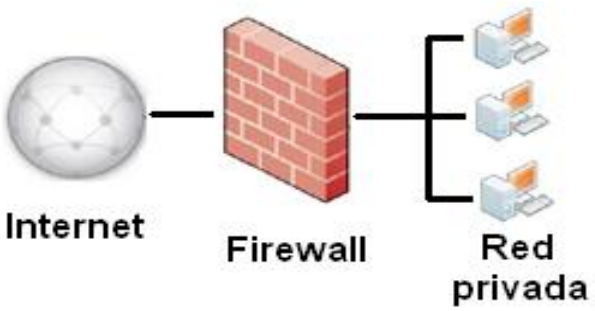


Fig. 4.8 Ejemplo de Cortafuegos

Las funciones que realizan unos cortafuegos pueden ser implementadas por una computadora o un conjunto de dos o más sistemas de cómputo que cooperan entre sí.

Los cortafuegos aplican políticas de seguridad diseñadas para hacer frente a las cosas malas que pudieran suceder. Como ejemplo de políticas tenemos: evitar cualquier acceso a la red desde el exterior (permitiendo el paso del tráfico del interior hacia el exterior), permitir el acceso sólo desde lugares específicos y de ciertos usuarios, etc. La política implementada depende de las necesidades que se deseen satisfacer.

Para lograr implementar las políticas, los cortafuegos utilizan cuatro técnicas que les permiten controlar el acceso al sitio:

- Control de Servicio: especificar que servicios de Internet pueden ser usados desde adentro y desde afuera (por ejemplo servicios web, mail, etc.).

- Control de Dirección: determina la dirección en la que los servicios particulares pueden ser iniciados y que se les permitirá fluir a través de los cortafuegos.

- Control de Usuarios: controla el acceso a los servicios que intenta acceder cada usuario.

- Control de Conducta: aquí se pude controlar la forma en que son utilizados los servicios. Por ejemplo, los cortafuegos puede filtrar los correos electrónicos para eliminar el spam.

4.4.4.1 Tipos de Cortafuegos

En esta sección se presentara la información básica sobre las capacidades con las que cuentan los cortafuegos y que a menudo se combinan con las tecnologías de los encaminadores (routers).

Encaminador filtrador de paquetes

Por lo general, son configurados para filtrar paquetes en ambas direcciones (desde y hacia la red). La configuración es como una lista de reglas basadas en coincidencias en los campos de los encabezados de IP o TCP.
Los campos pueden incluir alguno o todos los siguientes: Dirección IP origen (de donde salió), dirección IP destino (a donde se dirige), puerto origen (lugar de salida), puerto destino (lugar de entrada).

Cuando existen coincidencias con alguna de las reglas se invoca esa regla para determinar si el paquete es reenviado o descartado. Se pueden tener casos donde no se encuentren coincidencias con alguna regla, entonces se realiza una acción por omisión. Hay dos posibles políticas de default:

- Default = discard: lo que no está expresamente permitido, está prohibido.
- Default = forward: lo que no está expresadamente prohibido, está permitido.

La primera política es más conservadora, en un inicio todo es bloqueado y los servicios son agregados sobre la marcha. Esta política es más visible a los usuarios, quienes son más propensos a ver a los cortafuegos como un obstáculo.

En el segundo caso el usuario tiene más libertad, pero se proporciona una seguridad más limitada. Los administradores de seguridad deben de reaccionar a cada nueva amenaza, conforme se presenten.

Como ventajas de los filtradores de paquetes tenemos que: son de los cortafuegos más comunes, simples y fácil de emplear, para sitios pequeños y sencillos. Normalmente son transparentes para los usuarios y muy rápidos.

Los cortafuegos filtradores de paquetes cuentan con desventajas como: la capacidad de registro de actividades es pequeña, o no tiene, no soportan políticas de seguridad complejas como la autentificación de usuarios y control de acceso con horarios predefinidos.

Proxy – Compuerta de aplicación

Para contrarrestar las debilidades asociadas a los filtradores de paquetes, se crearon aplicaciones encargadas de filtrar las conexiones, se conocen como Servidores proxy y la máquina donde se ejecutan reciben el nombre de Compuerta (gateway) de Aplicación o Bastión Host.

Estos programas actúan como intermediarios para cada sesión de comunicación, proveen una barrera segura entre los usuarios internos e internet. Cuando el usuario interno intenta conectarse a internet por medio de su navegador, lo que en realidad consigue es conectarse a la compuerta de aplicación, quien establece la conexión con el servicio web en internet, actuando como intermediario en el intercambio de datos (Fig. 4.9).

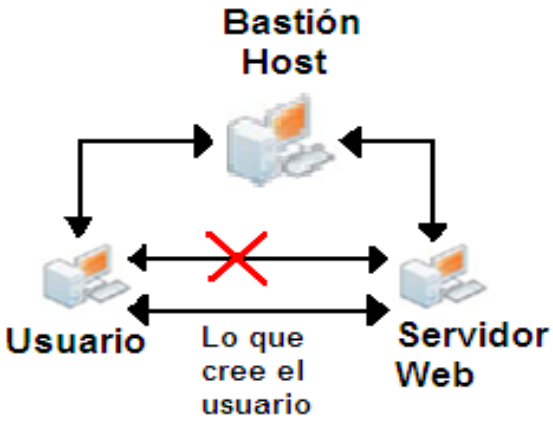


Fig. 4.9 Bastión host.

Un servidor proxy es capaz de examinar el contenido de cada paquete (tanto de entrada como de salida) y por lo tanto capaz de controlar la sesión del usuario basado en las operaciones que son solicitadas.
Unas de las principales ventajas de una compuerta de aplicación es la capacidad de controlar la sesión y proporcionar un registro detallado de los sucesos.

Las compuertas de aplicación implementan una política de rechazar todo a menos que sea explícitamente permitido. El hecho de que efectúen un análisis detallado de los paquetes, los convierte en los filtros más costosos en términos de tiempo y capacidad de cómputo.

A continuación se presentan dos ejemplos que pueden ayudar a comprender mejor el verdadero propósito de una compuerta de aplicación [6]:

- *Una empresa desea establecer una lista de precios en línea para que los extranjeros puedan ver los productos y los precios ofrecidos. Se necesita estar seguro de que: a) ningún extraño pueda cambiar los precios o la lista de los productos, b) que los extranjeros sólo puedan acceder a la lista, no a cualquiera de los archivos más sensibles almacenados en su interior.*

- *Una escuela quiere permitir a sus alumnos, que desean recabar información, ocupar los recursos que ofrece Internet. Para ayudar a proporcionar un servicio eficiente, la escuela quiere saber qué sitios han sido visitados y qué archivos de esos sitios han sido obtenidos, particularmente los archivos más solicitados son almacenados localmente.*

Estos requisitos pueden ser cumplidos con un proxy. En el primer ejemplo, el proxy podría supervisar la transferencia de datos para garantizar que sólo el archivo de la lista de precios sea accedido, y que este sólo se pueda leer, no modificar. Los requisitos de la escuela se podrían alcanzar con un procedimiento de registro como parte del navegador web.

Compuerta a nivel de circuito

Las compuertas a nivel de circuitos también implementan aplicaciones proxy, pero a diferencia de las compuertas de aplicación que interpretan el contenido de los protocolos de aplicación, estos determinan si una conexión entre dos puntos es permitida, de acuerdo a un determinado conjunto de reglas y agrupa los paquetes que pertenecen a la misma conexión.

Cuando la compuerta a nivel de circuitos acepta la comunicación, el proxy abrirá una sesión, permitirá el tráfico sólo para la fuente permitida y posiblemente por un tiempo limitado para dicha conexión.

Las compuertas a nivel de aplicación pueden implementar mecanismos de control de acceso elaborados, incluyendo la autenticación e intercambio de mensajes entre el proxy y el cliente.

La compuerta define dos conexiones, una entre sí misma y un usuario TCP de un anfitrión interno, y otra entre sí misma y un usuario TCP de un anfitrión externo. Una vez que se estableció la conexión, la compuerta simplemente envía los datos

entre las dos conexiones, sin examinar los contenidos. La función de seguridad consiste en determinar cuáles conexiones se permiten.

Cortafuegos personales

Un cortafuego personal es un programa que se ejecuta en una computadora. Funciona como un “controlador de tráfico”, verifica el tráfico entrante y saliente de la computadora, permitiendo o neutralizando conexiones en base a políticas predeterminadas.

Podemos encontrar dos características sobresalientes en los cortafuegos personales: por una parte, permiten el filtrado de aplicaciones. Es decir, permiten fijar reglas para las aplicaciones más usadas como los navegadores de Internet, programas de mensajería instantánea, etc. Los cortafuegos personales también permiten el filtrado de paquetes: analizan las transferencias de datos (encabezados, protocolos utilizados, direcciones IP, etc.) y filtran paquetes siguiendo políticas predeterminadas.

Cuando se combinan los cortafuegos personales con un antivirus, los cortafuegos pueden dirigir los correos entrantes del correo electrónico a los antivirus, el cual examina cada archivo adjunto en el momento que éste llega a la computadora de destino antes de que sea abierto.

Los cortafuegos personales pueden evitar que las computadoras sean infectadas por gusanos, puertas traseras o ataques de spyware. En ocasiones los gusanos pueden traspasar los cortafuegos, logrando ejecutarse en el equipo e incluso puede tener la oportunidad de eliminar el software del cortafuego personal.

Otro de los riesgos que podemos encontrar es la instalación de una puerta trasera que se ejecuta en el sistema por medio de un kit de descarga que aprovecha una vulnerabilidad del navegador web.

Como operaciones normales en los cortafuegos personales tenemos que son capaces de alertar sobre el acceso a la red, por lo que cada vez que se ejecute el navegador web, usted consigue una alerta de los cortafuegos. Ésta es una opción común, permite que una aplicación en particular pueda ser controlada por el usuario.

Los cortafuegos personales están disponibles como parte de los sistemas operativos para servidores tales como Linux, Windows, Solaris. También se pueden instalar versiones comerciales.

Limitar el tráfico de salida desde un servidor también puede ser útil en la prevención de determinados programa de malware que intenten propagarse a otras computadoras. Muchos cortafuegos personales también pueden actuar como sistemas de prevención de intrusos (IPS) que, después de detectar un ataque en curso, tomen medidas para impedir que el atacante cause daño al equipo destino.

Algunos cortafuegos personales permiten la creación de diferentes perfiles basados en cierta ubicación, por ejemplo la utilización de un perfil para su uso dentro de la red de la organización y otro diferente para usarlo en una conexión remota. Esto es particularmente importante cuando se utiliza una computadora en una red externa, ya que tener un perfil diferente para su uso en dichas redes puede ayudar a restringir la actividad de la red con más fuerza y proporcionar una mayor protección a la que ofrece un único perfil.

Al igual que todas las soluciones de seguridad, los cortafuegos personales vienen con una reducción del rendimiento. Normalmente los cortafuegos tienen un mejor rendimiento, pero a pesar de esto no cuenta con la capacidad para hacer frente a todas las preocupaciones de seguridad.

En la versión de Windows XP con Service Pack 2 (SP2), se encuentra un firewall, llamado Servidor de conexión a Internet o ICF, el cual esta activado de forma predeterminada. Desafortunadamente, esté solamente puede filtrar las comunicaciones entrantes y no las salientes, es decir, que la mayor parte de los programas no aceptan comunicaciones de Internet que no hayan solicitado a menos que el usuario decida catalogarlas como excepciones.

Básicamente, el firewall de Windows se dedica a bloquear las solicitudes no deseadas (cuando alguien en Internet o de una red intenta conectarse a un equipo). Por ejemplo, si utiliza un programa de mensajería instantánea o un video juego de red con varios jugadores, que tienen que recibir información desde Internet o de una red, el servidor de seguridad le preguntara si desea bloquear o desbloquear (permitir) la conexión. En el caso de que elija desbloquearla la conexión, el firewall de Windows creara una excepción de modo que el servidor de seguridad no se interpondrá cuando ese programa tenga que recibir información en un futuro.

Si bien el firewall de Windows representa un avance importante, pero se debe de tener en cuenta que no es suficiente cuando se trata de malware que está enviando información al exterior. Por otro lado, Windows Vista si filtra las comunicaciones entrantes y salientes.

4.5 Manejo de incidentes

Como podrán darse cuenta las técnicas de prevención no garantizan al 100% la seguridad de un equipo, mucho menos la de una red. La combinación de estás pueden ofrecer cierto grado de seguridad, pero siempre existirá la posibilidad de que sus equipos sean infectados. Por esta razón, se presenta una descripción breve del manejo de incidentes.

De acuerdo a la "Computer Security Incident Handling Guide" del NIST [6] un incidente puede ser considerado como una violación o la amenaza de violación de las políticas de seguridad informática, las políticas de uso aceptable, o la práctica estándar de seguridad. Como ejemplo de incidentes tenemos:

- Negación de servicios (DoS). Es cuando el atacante envía paquetes especialmente diseñados a un servidor web, provocando que se bloquee.
- Código malicioso. Gusanos, puertas traseras, troyanos, etc.
- Acceso no autorizado. Cuando un atacante logra tener acceso a los archivos o contraseñas de un servidor.
- Uso inapropiado. Se produce cuando un usuario efectúa acciones que violan las políticas aceptadas y establecidas por la organización respecto al uso de recursos.

4.5.1 Ciclo de vida para el manejo de incidentes

La fig. 4.10 representa las 4 fases que constituyen el ciclo de vida para el manejo de incidentes. A continuación se procede a describir brevemente cada una de ellas.

Fig. 4.10 Ciclo de vida para la respuesta a incidentes

- Preparación. Para poder responder satisfactoriamente a los incidentes por malware las organizaciones realizan medidas preparatorias. Por ejemplo, facilitar la comunicación y coordinación mediante la conformación de un pequeño equipo de personas que puedan responder a los incidentes, adquirir el hardware y las herramientas de software necesarias para ayudar en el manejo de incidentes por malware.

- Detención y análisis. La detención y validación rápida de incidentes puede evitar la propagación de código malicioso a través de una organización que por lo general suelen dar se en cuestión de minutos, esté tipo de medidas suelen disminuir la magnitud de los esfuerzos de recuperación y la cantidad de daño a la organización.

  Como se menciono anteriormente, el malware puede tomar diferentes formas y distribuirse a través de varios medios, causando que existan muchos signos de incidentes y lugares dentro de una organización en la que los signos pueden ser registrados u observados. Cuando se ha logrado la detención del malware, los controladores del incidente deben de determinar el tipo, extensión y magnitud del problema los más rápidamente posible para que la respuesta al incidente se pueda dar la prioridad adecuada. Monitorear los avisos de malware y las alertas de seguridad (por ejemplo, el software antivirus, IPS) para la detención de los precursores de malware, que le pueden dar a la organización la oportunidad de prevenir los incidentes.

- Contención. En esta fase podemos encontrar dos componentes principales: detener la propagación del código malicioso y prevenir mayores daños a los sistemas. Es importante comprender que la detención de la propagación de malware no necesariamente evitará todos los daños a los sistemas. Incluso después de que la organización ha logrado su detención, el malware puede continuar infectando o eliminado los datos, aplicaciones y archivos del sistema operativo. Además, podemos encontrara algunos casos en donde el malware está diseñado para causar daño adicional cuando se pierde la conexión con la red. Los métodos de contención pueden ser divididos en: participación de los usuarios, detención automática, deshabilitar los servicios, deshabilitar la conectividad.

- Erradicación. Su principal objetivo el eliminar el malware de los sistemas infectados. Puede tomas varios días o semanas llevar a cabo la erradicación de la gran mayoría de los sistemas infectados, debido al gran número de sistemas involucrados, y a la naturaleza dinámica de los sistemas.

  Diferentes situaciones requieren diferentes combinaciones de técnicas de erradicación. Las herramientas más comunes para la erradicación de software antivirus, detención de spyware y utilidades de eliminación, y el software de administración de parches.

- Recuperación. Cuanta con dos principales aspectos de recuperación de incidentes: la restauración de la funcionalidad y los datos de los sistemas infectados, y la eliminación de las medidas temporales de contención.

- Actividades post incidentes. Aquí se engloban conjuntos de acciones que permiten mejorar los procesos relacionados con el manejo de incidentes. Su principal objetivo es generar reportes que ayuden a una organización a mejorar su capacidad de administración sus recursos para defenderse del código malicioso, incluyendo los cambios necesarios en las políticas de seguridad, configuración del software y la implementación de programas de prevención.

Referencias capítulo 4

[1] "Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad". España, 2004. Disponible en: http://www.oecd.org/dataoecd/15/29/34912912.pdf

[2] Peter Mell, Karen Kent, Joseph Nusbaum. "Guide to Malware Incident Prevention and Handling". NIST.800-30, 2005. Disponible en: http://csrc.nist.gov/publications/nistpubs/

[3] Tim Grance, Karen Kent, Brian Kim. "Computer Security Incident Handling Guide". NIST.800-61, 2004.

[4] AMIPCI. "Estudio Sobres los Hábitos de los Usuarios de Internet en México". Mayo del 2010

[5] Hispasec Sistemas. "¿Cuánto tardan los grandes fabricantes de software en arreglar una vulnerabilidad?. Disponible en: http://www.hispasec.com/laboratorio/Hispasec_Estudio_Vulnerabilidades.pdf

[6] Tim Grance, Karen Kent, Brian Kim. "Computer Security Incident Handling Guide" NIST.800-61, 2004.

[7] Charles P. Pfleeger. "Security in Computing". 4at, edición. Ed. Prentice Hall ISBN 978-0-13-239077-4

[8] Raúl Siles Peláez. "Análisis de seguridad de la familia de protocolos TCP/IP y servicios asociados". Junio del 2002.

[9] Microsoft, "Proteja su equipo: conceptos avanzadas". Disponible en: http://www.microsoft.com/latam/protect/computer/viruses/default.mspx

[10] CERT® Coordination Center, "Home Network Security". Disponible en: http://www.cert.org/tech_tips/home_networks.html

[11] ESET, "Creando un entorno seguro en Windows XP". Disponible en: http://www.eset-la.com/centro-amenazas/2038-proteccion-windows-xp

[12] David Emm, "Arreglando las vulnerabilidades humanas". Disponible en: http://www.viruslist.com/sp/analysis?pubid=207271063

[13] Nikolay Grebennikov, "Las pruebas de fugas como método para evaluar la efectividad de un cortafuegos". Disponible en: http://www.viruslist.com/sp/analysis?pubid=207270960

[14] Sego-Info, "Firewall". Disponible en: www.segu-info.com.ar/firewall/firewall.htm

[15] La Heuristica. Disponible en: spi1.nisu.org/recop/al01/joss/heuristica.html

Conclusiones

La falta de información sobre el código malicioso, no sólo se puede observar en las personas que se encuentran en sus casas, sino también en los alumnos de las universidades, empleados de grandes corporaciones, etc. El que no sean capaces de darse cuenta con qué facilidad pueden ser víctimas de algún tipo de malware, los hace una presa fácil.

Saber los métodos en que el código malicioso afecta los sistemas de cómputo, nos da la oportunidad de tomar medidas adecuadas para prevenir el robo de información, el daño a las computadoras, el espionaje, etc. Recordando siempre que la implementación de estas medidas no nos garantiza que el sistema de cómputo este protegido al %100, siempre abra la posibilidad de sufrir alguna infección.

Los servicios que ofrece Internet son cada vez más, los usuarios pueden realizar transferencias bancarias, chatear con personas de otros países, descargar videos o música, etc. Los atacantes siempre buscarán la forma de sacar ventaja de los usuarios que no manejen adecuadamente estos servicios, es por esto y muchas razones más que el usuario es considerado el eslabón más débil de la cadena de seguridad.

Utilizar y mantener actualizadas las herramientas de detención de spyware y el antivirus forma parte fundamental en cualquier estrategia en contra del malware, a pesar de las desventajas mencionadas anteriormente.

Cada una de las técnicas de prevención presentadas en este trabajo son capaces de ofrecer un cierto nivel de seguridad en contra del malware, el usuario podrá implementar las que mejor se adecuen a sus necesidades.

Bibliografía

Peter Szor. “The art of computer virus research and defense”. Ed. Addison Wesley Professional, 2005. ISBN 0-321-30454-3

Daltabuit Godás Enrique, Hernández Hernández Leobardo. “La Seguridad de la Información”. Ed. LIMUSA. ISBN-13: 978-968-18-6935-9, 2007.

John Aycock. “Computer Viruses and Malware”. Ed. Advances in Information Security. ISBN 978-0-387-30236-2, 2006.

Charles P. Pfleeger. “Security in Computing”. 4at, edición. Ed. Prentice Hall ISBN 978-0-13-239077-4

Peter Mell, Karen Kent, Joseph Nusbaum. “Guide to Malware Incident Prevention and Handling”. NIST.800-30, 2005.

Tim Grance, Karen Kent, Brian Kim. “Computer Security Incident Handling Guide” NIST.800-61, 2004.

OECD. “Malicious Software (Malware) A Security Threat to the Internet Economy” Junio del 2008.

AMIPCI. “Estudio Sobres los Hábitos de los Usuarios de Internet en México” Mayo del 2010

Proyecto malware. Disponible en: http://proyecto-malware.webnode.es/nomenclatura-de-los-nombres-de-virus/

NTEK, “Symantec informa sobre las amenazas más comunes a las que están expuestos los usuarios de Internet y las razones de su incremento”. Disponible en: http://ntek.com.mx/2010/04/23/symantec-informa-sobre-las-amenazas-mas-comunes-a-las-que-estan-expuestos-los-usuarios-de-internet-y-las-razones-de-su-incremento/

AntiVir, “Estudio sobre virus informáticos”. Disponible en: http://www.seguridad-profesional.com/cms/content/view/41/2/

ITSECURITY, “The Nastiest Malware Trends”. Disponible en: http://www.itsecurity.com/features/nastiest-malware-trends-011207/