

NETBOOKS: LA MINIREVOLUCIÓN

IT NOW

www.revistaitnow.com TECNOLOGÍA & NEGOCIOS EN AMÉRICA CENTRAL Y EL CARIBE

ESTADO

GOBIERNO DIGITAL
E INICIATIVAS DE
INFORMATIZACIÓN ESTATAL
EN LA REGIÓN



LAS POLÍTICAS IT Y SUS PROBLEMÁTICAS.
OPINIONES SOBRE LAS LICITACIONES
PARA LA COMPRA DE TECNOLOGÍAS.
PROVEEDORES, FUNCIONARIOS Y CONSULTORAS
HABLAN SOBRE UNA CUESTIÓN QUE
TRASCIENDE A LOS GOBIERNOS DE TURNO.

 **cerca**
Revista de Ediciones digitales

MAYO 2009 - EDICIÓN 45



9 771659 173001

GUATEMALA Q. 50 - TL, SALVADOR US\$ 3.95
HONDURAS L. 210 - COSTA RICA C. 1790
NICARAGUA C. 80 - PANAMÁ B. 3.95
REP. DOMINICANA RD 130 - USA \$3.95

EL MAPA DE LA SEGURIDAD IT 2009



EL MAPA DE LA SEGURIDAD

Panorama de las herramientas para contrarrestar o prevenir el creciente número de amenazas IT. Un repaso sobre el entorno actual en el que debemos sobrevivir. Por JUAN M. TIRADO

| “MÁS DEL 97 POR CIENTO DE E-MAILS SON MENSAJES NO DESEADOS, TIENEN ADJUNTOS MALINTENCIONADOS O SON ATAQUES DE PHISHING”, |

Christian Linacre,
de Microsoft.

Cuando pensamos en la realidad tecnológica actual, la seguridad de la información juega un papel cada vez más preponderante en los aspectos de IT. Esto se debe a un número de factores diversos: un incremento constante de las amenazas informáticas, una mayor conciencia de los usuarios, más información disponible sobre el tema, entre otros.

A propósito de las amenazas informáticas, hace varios meses, en IT NOW llevamos a cabo un informe sobre los principales peligros a los que nos enfrentamos diariamente. Pero la otra cara de esta moneda es el brindar un panorama de cuáles son las herramientas con las que cuentan quienes están involucrados con las IT para contrarrestar o prevenir el creciente número de peligros que acechan a nuestras organiza-

ciones (Ver XXXX).

Antes de entrar de lleno en el contenido que debería tener nuestro kit de supervivencia de seguridad informática, hagamos un repaso sobre el entorno actual en el que debemos sobrevivir.

Informes de amenazas

Recientemente, **Microsoft** hizo público el volumen 6 del “Reporte de inteligencia de seguridad”, que ofrece una perspectiva acerca de las diferentes debilidades, así como de las tendencias del *software* malintencionado y el potencialmente no deseado que la marca ha observado en los últimos años, con un enfoque especial en la segunda mitad de 2008. El estudio también contiene nueva información acerca del *software* de seguridad falso, junto con las vulnerabili-

TENDENCIAS

Detalle de los incidentes relacionados con infracciones de seguridad en todo el mundo, a partir de la información obtenida de la base de datos de Open Security Foundation relacionada con la pérdida de datos.

- La categoría principal de pérdida de datos a raíz de una infracción de seguridad durante la segunda mitad de 2008 (2M08) continuó siendo el robo de equipos, como por ejemplo portátiles [consti-

tuye el 33,5% de todos los incidentes registrados relacionados con la pérdida de datos]. Junto con los equipos perdidos, estas dos categorías suponen el 50% de todos los incidentes registrados.

- Las infracciones de seguridad por incidentes de piratería o malware suponen menos de un 20% del total.
- Estos resultados refuerzan la necesidad de unas directivas y procedimientos apropiados para la administración de datos.



Fuente: "Informe de inteligencia sobre seguridad" de Microsoft, volumen 6.

dades de los exploradores y los formatos de documentos más habituales, además de información actualizada sobre las infracciones de seguridad y privacidad.

"Vemos cifras proyectadas que demuestran que más del 97 por ciento de los mensajes de correo electrónico enviados a través de Internet son mensajes no deseados, tienen archivos adjuntos malintencionados (virus, troyanos) o son ataques de suplantación de identidad (*phishing*)", dijo Christian Linacre, gerente de Seguridad de Microsoft Latinoamérica.

Publicado dos veces al año, el informe utiliza datos reunidos de cientos de millones de computadoras de todo el mundo para ofrecer un análisis profundo del panorama. Con esta reciente edición, Microsoft proporciona información sobre las amenazas a través de datos nuevos sobre los ataques a los formatos de archivo de documentos, los diferentes tipos de *software* dañinos que afectan a las computadoras residenciales y empresariales y el *phishing*.

Los atacantes están usando cada vez con mayor frecuencia formatos de archivo comunes como instrumentos de transmisión de sus ataques. La mayoría de los programas actuales de correo electrónico y mensajería instantánea están configurados para bloquear la transmisión de archivos potencialmente peligrosos según su extensión. Sin embargo, estos programas permiten habitualmente la transmisión de los formatos de archivo habituales como

Office y *portable document format* (.pdf) de **Adobe**. Estos formatos son usados diariamente de manera legítima por multitud de usuarios, por lo que no se han bloqueado. Sin embargo, esto los ha convertido en un objetivo atractivo para los atacantes de las vulnerabilidades de seguridad.

Ahora bien, a pesar de la naturaleza internacional de Internet, hay diferencias significativas en los tipos de riesgos que afectan a los usuarios en diferentes partes del mundo. Conforme el ecosistema del *malware* se vuelve más dependiente de la ingeniería social, las amenazas de todo el mundo se han vuelto más dependientes de los factores lingüísticos y culturales. Por ejemplo, en China, prevalecen varios modificadores maliciosos de los exploradores; en Brasil, está muy extendido el *malware* dirigido a los usuarios de la banca electrónica; y, en Corea, son habituales los virus como **Win32/Virut** y **Win32/Parite**.

Por su parte, **Symantec** reveló los resultados de su "Informe sobre amenazas a la seguridad en Internet" correspondiente a abril de 2009 que, entre otras cosas, reflejó que América Latina representó 13 por ciento del total de computadoras infectadas por *bots* a nivel global.

En la región, Brasil registró el porcentaje más alto de computadoras infectadas por *bots*, con 42 por ciento del total, y a nivel global, el país tuvo 6 por ciento del total. Argentina ocupó el segundo lugar en 2008 en computadoras infectadas con este tipo

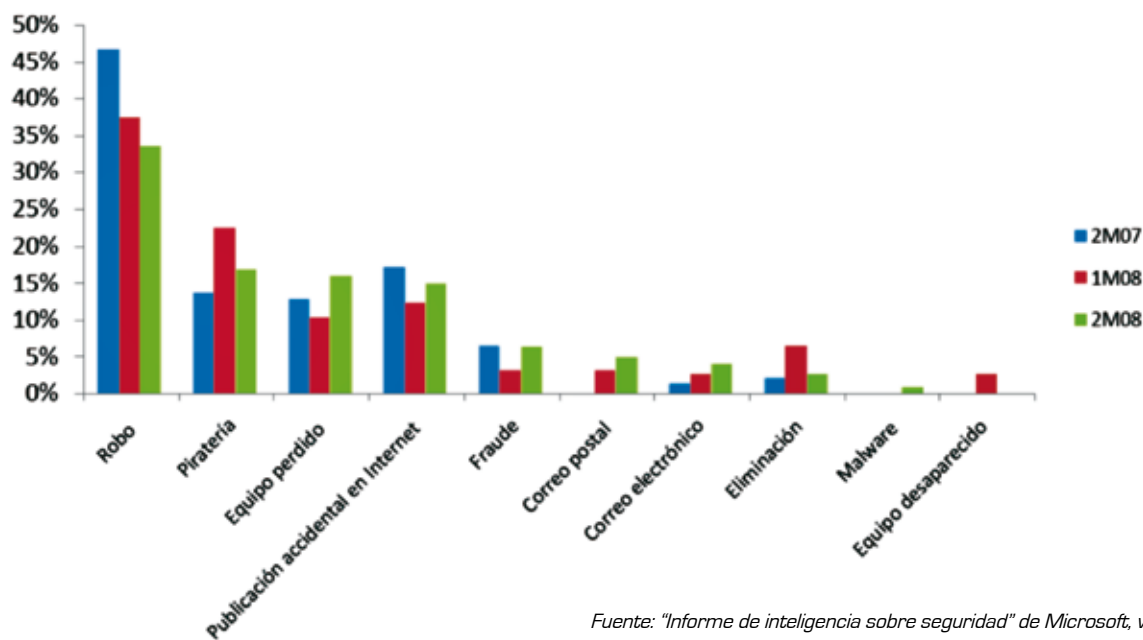
ALTO RIESGO

Aspectos destacados del "Informe sobre amenazas a la seguridad en Internet" correspondiente al mes de abril 2009.

- Brasil fue el país número uno con actividad maliciosa en América Latina durante 2008, representando el 34 por ciento del total. A nivel global, se clasificó en el quinto lugar, con el cuatro por ciento del total de la actividad maliciosa por país.
- Estados Unidos ocupó el lugar número uno de origen de ataques detectado por los sensores ubicados en América Latina en 2008, representando 58 por ciento de todos los ataques detectados. El país también mantuvo su clasificación en el primer lugar por originar ataques contra blancos globales en 2008, con 25 por ciento.
- Brasil ocupó el primer lugar en computadoras infectadas por *bots* en la región de América Latina en 2008, con 42 por ciento del total. También tuvo el seis por ciento del total de computadoras infectadas con esta amenaza a nivel global.
- En 2008, 29 por ciento del spam detectado en América Latina se originó en Brasil. El país representó el cuatro por ciento del correo basura que se detectó a nivel mundial.

INCIDENTES RELACIONADOS CON INFRACCIONES DE SEGURIDAD

Clasificados según el tipo y expresados como porcentajes del total, entre la segunda mitad de 2007 (2M07) y el mismo período de 2008 (2M08).



Fuente: "Informe de inteligencia sobre seguridad" de Microsoft, volumen 6.

| SEGÚN SYMANTEC, EN 2008 EL 29 POR CIENTO DEL SPAM DETECTADO EN AMÉRICA LATINA SE ORIGINÓ EN BRASIL. EL PAÍS REPRESENTÓ CUATRO POR CIENTO DEL CORREO BASURA QUE SE DETECTÓ A NIVEL MUNDIAL. |

de amenazas en América Latina, con 17 por ciento, y Perú se clasificó en el número tres, con 10 por ciento.

Junto con la alta clasificación de estos países, que puede deberse a su alto número de suscriptores de banda ancha en la región, los datos de Symantec también muestran que el porcentaje global de *spam* originado en América Latina se duplicó en 2008, de dos a cuatro por ciento.

Las computadoras infectadas con *bots* con frecuencia se asocian con *spam*, ya que pueden programarse para que envíen en forma automática una gran cantidad de mensajes de correo electrónico

Muestras de código malicioso

De acuerdo con el informe de Symantec, la muestra más común de código malicioso por número de infecciones potenciales registradas en América Latina fue el gusano **Gammima.AG**, que fue clasificado en el séptimo lugar a nivel global. Este *worm* se propaga copiándose en dispositivos de almacenamiento removibles de medios removibles, como unidades USB y reproduc-

tores de sonido portátiles.

El **Gammima.AG** también roba credenciales de cuentas de juegos en línea populares y ocupa uno de los tres primeros lugares dentro de las diez muestras de código malicioso en América Latina en este tipo de robos.

La muestra que ocupó el segundo lugar fue el **SillyFDC**. Al igual que el mencionado anteriormente, este gusano se propaga copiándose en dispositivos de almacenamiento de medios removibles anexos a la computadora comprometida. Una vez que este código malicioso se instala en una computadora, también intenta descargar e instalar amenazas adicionales en el equipo.

La tercera muestra de código malicioso que se reportó con más frecuencia como causante de infecciones potenciales en Latinoamérica durante este período fue el gusano **Rontokbro**, que había ocupado el primer lugar durante 2007 y también fue una de las diez primeras muestras de código malicioso a nivel global tanto en 2007 como en 2008.

TOMAR LAS ARMAS

Cuáles son las metodologías y herramientas para la protección IT en todos los frentes de ataque. Antivirus, firewalls, programas anti-spam, y recursos contra el malware y los spywares. JUAN M. TIRADO

Una vez revisado el panorama de las amenazas más recientes, debemos saber que no estamos desarmados a la hora de hacerles frente. La intención con este informe es cubrir en forma general los aspectos principales de esta eterna lucha por asegurar nuestras organizaciones desde cinco puntos distintos: el antivirus, el *firewall*, los programas *anti-spam* y la protección contra *malware* y *spyware*.

Un viejo conocido

Es relativamente común que muchos asocien seguridad con antivirus, pero en el mundo actual esta simplificación puede ser muy costosa.

“Hay más en la seguridad que los virus y *software* maliciosos. Aunque son un importante riesgo y necesitan ser abordados, hay muchas más amenazas de las que las pequeñas empresas deben ser conscientes. Cada acción llevada a cabo por un empleado puede ser un peligro para la seguridad. Hoy una preocupación creciente es la cantidad de información perdida por las organizaciones. El uso no monitorizado de Internet es otra

seria amenaza. Todo lo que se necesita es pulsar un *link* para que un *software* malicioso se descargue discretamente en segundo plano. Los empleados que utilizan sus dispositivos personales tales como *pen-drives*, iPods, *smartphones*, por nombrar algunos, pueden introducir virus y *soft* maliciosos en la empresa sin saberlo, o pueden copiar información que sea confidencial”, explicó David Kelleher, gerente de Relaciones Públicas de **GFI Software**.

Un antivirus tiene como propósito prevenir o erradicar una infección causada por un virus informático y su origen data desde la década del ochenta. Claro que, para que pueda ser efectivo debemos mantenerlo lo más actualizado posible.

El funcionamiento de los antivirus varía de uno a otro, aunque su comportamiento generalmente se basa en contar con una lista de virus conocidos y la forma de reconocerlos —las llamadas firmas o vacunas— y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador.

“Un antivirus puede asemejarse al uso de un filtro del agua potable: el agua es algo que

REPERCUSIONES

Por Nicolás Severino, gerente de Ingeniería de Symantec para el Norte de América Latina (NOLA).

Con la proliferación de la banda ancha, aumentaron los potenciales ataques ya que contar con una mayor velocidad implica que más datos pueden ser inspeccionados y potencialmente robados del equipo. Adicionalmente, muchos usuarios están optando por dejar sus computadoras conectadas todo el tiempo, con lo cual facilitan la invasión de los equipos por parte de estos intrusos. Los hackers profesionales se infiltran en el equipo (o la red) de la víctima en busca de cualquier tipo de información que puedan utilizar en su propio beneficio, desde números de cuentas bancarias hasta direcciones postales físicas o núme-

ros de identificación.

Todo un mercado negro ha crecido alrededor de los hackers y de los ladrones de identidad: tan solo el año pasado, el valor del mercado de la economía clandestina alcanzó cerca de 276 millones de dólares y una cuenta de correo electrónico se podía adquirir por solo diez centavos de dólar.

Por su parte, los intrusos también secuestran equipos domésticos y los utilizan para encubrir futuros delitos. Cuando un hacker usa la máquina de un usuario como base de ataque, este usuario pasa a ser sospechoso de los delitos que él está cometiendo de manera inadvertida.



todos necesitamos y usamos constantemente, pero puede tener impurezas, microbios o virus que pueden hacerle daño a la persona. El uso del filtro es una protección indispensable, pero no es lo único necesario para la seguridad de la persona. Si uno no usa un antivirus, es posible que se enferme. Pero el hecho de usar un filtro no implica que nunca se enfermará”, agregó Eli Faskha, gerente general de **Soluciones Seguras**.

Para Cristian Borghello, gerente técnico y educativo de **ESET** Latinoamérica, contar con una solución antivirus actualmente implica ser consciente de la importancia de estar protegido contra millones de programas dañinos que buscan infectar nuestros equipos y que generalmente persiguen algún rédito económico.

“Aunque la mayoría de las empresas tienen instalada una solución antivirus, varias encuestas sobre seguridad de IT muestran que entre el dos y tres por ciento de los encuestados no utilizan productos de este tipo en su organización. Esto podría significar que estas empresas ni siquiera consideran que la seguridad sea un problema, lo cual es muy preocupante. Los negocios necesitan entender que tener *software* de seguridad no representa que sus redes sean seguras o que no haya riesgo de infección. Simplemen-

te significa que han cerrado una puerta”, señaló Kelleher, de GFI.

Adicionalmente a sus labores de protección, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de infecciones conocidas, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinos para el ordenador con técnicas como la heurística, que reconoce comportamientos de archivos que aún no están registrados.

“La evolución de los antivirus ha ido acompañada del progreso de los archivos dañinos y el cambio de paradigma en su existencia: hoy un ataque ya no es una demostración ostentosa de las habilidades técnicas de su creador, sino que persigue fines delictivos y de beneficio económico. Originalmente, los antivirus eran simples programas capaces de eliminar unos pocos archivos dañinos. En la actualidad, y dado el complejo panorama de amenazas informáticas, son complejas herramientas perfeccionadas para detectar cualquier tipo de infecciones”, añadió Borghello, de ESET.

Detección y prevención

Debido a la sofisticación de los virus, hoy es difícil percatarse de su presencia por cau-



sas de pérdida de desempeño, pero hay que destacar que la mayoría de estos provocan:

- que el sistema realice las operaciones de procesamiento más lentas;
- que los programas tarden más en cargarse en memoria;
- que los programas comiencen a acceder por momentos a la unidad de discos flexibles y discos duros sin necesidad alguna;
- la disminución sin motivos del espacio en disco duro y memoria de la computadora en forma constante y repentina; y
- la aparición de programas desconocidos en la memoria.

La mayoría de los especialistas consultados concuerdan en que, generalmente, las infecciones informáticas pueden ser prevenibles por el usuario con una combinación de un sistema antivirus instalado y con las firmas al día sumado con la implementación de políticas de seguridad que incluyan la conscientización de los usuarios en cuanto al uso de los recursos de la empresa, como el correo electrónico e Internet.

El espía

En números pasados, IT NOW publicó un artículo sobre lo que representa hoy el *spyware* y sus características. En este apartado, veremos con qué contamos para contrarrestar este tipo de ataque informático.

"Ahora los problemas relacionados con la defensa de la intimidad y la protección de la información ya no son una preocupación meramente militar. El frente ha llegado hasta nuestros propios equipos informáticos y el combate se libra en el campo de batalla de la *web*", aportó Andrea Ostrowiak, gerenta de Mercadeo y Comunicaciones de McAfee en Centroamérica.

Para Borghello, de ESET, el *spyware* es actualmente tanto o más importante que detectar que cualquier otro tipo de *malware*, porque las consecuencias son las mismas que en cualquier otro caso de archivo dañino y, a veces, aun peor, debido a que están diseñados para robar información sensible del usuario. Si los datos obtenidos son críticos, los secretos comerciales de la compañía pueden estar en peligro.

"Este tipo de programas normalmente se ejecuta en segundo plano, recopila infor-

mación o monitorea la actividad y puede transmitir dicha información a alguna otra ubicación en Internet. Una gran cantidad de *spyware* recopila información relacionada con el equipo y con la forma en que se usa. Por ejemplo, puede monitorear su patrón de exploración en la *web* o las clases de *software* que está ejecutando. Se sabe que otras clases más sofisticadas capturan y transmiten información altamente personal, desde contraseñas y nombres de usuario, hasta números de tarjetas de crédito y mensajes instantáneos", añadió Nicolás Severino, gerente de Ingeniería de Symantec para el Norte de América Latina (NOLA).

De acuerdo con Fabián Flores, gerente de Ventas de AEC Electrónica, dado que el *spyware* usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otros equipos conectados a Internet. Además, se puede apreciar un uso intenso por ejemplo de la conexión a Internet o del disco duro, aun cuando la computadora no está siendo utilizada.

"Hay que establecer una política en la que se defina lo que los usuarios pueden instalar. Bloquear las configuraciones del sistema y reducir los privilegios de administrador. De este modo, los empleados no pueden instalar ningún *software* sin el permiso explícito de los responsables de IT. Además. Hay que proteger los sistemas con fuertes defensas, tanto para equipos como para la red. Con las descargas inadvertidas y otros ataques, los ordenadores sin protección contra programas espía se pueden contaminar rápidamente. Si trabaja desde casa o está de viaje, su ordenador necesita protección contra programas espía", concluyó Ostrowiak, de McAfee.

Asentando barreras

Como en cualquier otro conflicto bélico, en la seguridad informática es de suma importancia establecer una línea de defensa del perímetro, y es aquí donde el *firewall*, o cortafuegos, juega un papel importante para proteger nuestro ambiente de IT.

Un *firewall* es un elemento de *hardware* o *software* que se utiliza para controlar las comunicaciones, permitiéndolas o prohi-

| SEGÚN UN ESTUDIO DE F-SECURE SOLO EL DIEZ POR CIENTO DE LOS USUARIOS AFIRMÓ QUE PODÍAN ABRIR LOS ARCHIVOS ADJUNTOS A UN CORREO ELECTRÓNICO CON LA SEGURIDAD DE QUE SU ORDENADOR NO SE INFECTARÍA CON ALGÚN VIRUS. |



DOBLE IDENTIDAD

Es importante destacar un ítem que rescata el más reciente "Informe de inteligencia sobre seguridad" de Microsoft, y tiene que ver con la creciente presencia del software de seguridad falso. Este relativamente nuevo factor se ha incrementado significativamente a lo largo de los tres últimos períodos y su propagación emplea técnicas basadas en la ingeniería social, el miedo y la insistencia para

convencer a las víctimas de pagar por "versiones completas" del software para evitar y eliminar una infección, detener las alertas y advertencias continuas, o ambas cosas.

En estos casos, lo ideal es que, antes de descargar o aceptar cualquier actualización sospechosa o descarga no autorizada, consulte con su proveedor de seguridad sobre la legitimidad de la notificación.



biéndolas según las políticas de la red que se hayan definido. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet. De este modo, se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

Como lo define Ari Supperi, director general de **Consortio Fincosta**, "Además de implementar un cortafuegos perimetral, existe el modo de dividir departamentos internos de la empresa con *firewalls* internos, cuya ventaja es poder mediante reglas evitar la fuga de información y esparcimiento de una contaminación desde un departamento al otro".

Por su parte, Severino, de Symantec planteó que "tradicionalmente, la función del *firewall* estaba encasillada dentro de la necesidad de controlar y proteger la red de potenciales ataques que pudieran vulnerar el perímetro de la organización. Hoy en día, el nivel de protección requerido por las empresas no solo contempla la necesidad de proteger la red del tráfico entrante, sino también

de la alternativa que tráfico saliente no autorizado trascienda el perímetro. Adicionalmente, los *firewalls* permiten proteger la red de una serie de ataques y técnicas utilizadas para intentar penetrar a la organización. Para brindar este nivel de control, estos programas controlan todo el tráfico de entrada y salida. Verifican toda información o paquete de información que se intenta intercambiar entre Internet y el equipo o la red interna".

Ahora bien, existen principalmente dos tipos de *firewalls*: está la protección de *hardware* y la de *software*. Para Borghello, de ESET, las ventajas de la implementación de esta herramienta de tipo físico es que, al ser dispositivos desarrollados para este fin, pueden ser mucho más potentes en el filtrado de las conexiones y, además, permiten una mayor especialización de la herramienta, pudiendo realizar un análisis eficiente de cada una de las capas de la comunicación. Suelen tener la contra de tener un costo más elevado.

Según Supperi, de Consortio Fincosta, generalmente el *firewall* perimetral es un equipo y los interdepartamentales suelen ser de *software*.

Ataque masivo

Si hay algo que caracteriza los ataques a través de correo basura es que, en el mundo actual, es lo más parecido a un bombardeo militar incesante sobre territorio enemigo, solo que esta vez los atacados somos todos.

Dependiendo de las cifras consultadas, el promedio de *spam* que recibimos en nuestras



cuentas de correo comprende entre el 85 y el 95 por ciento diariamente y, de acuerdo con todos los especialistas, estos números van a seguir aumentando.

Para Kelleher, de GFI, la principal causa para tomar medidas preventivas frente a estos ataques es que los buzones de los empleados se inundarán con correo basura, lo que exigirá que cada uno navegue entre cientos de correos para encontrar los que son importantes. También existe el riesgo de que mensajes legítimos se pierdan en el proceso y esto podría tener serias repercusiones sobre el negocio —eliminar la confirmación de pedido de un cliente, por ejemplo. Aun más, el correo que contenga algún tipo de *phishing* es una amenaza y los usuarios podrían ser engañados para dar información que no debieran, de naturaleza personal o empresarial.

“Los recursos de una empresa y de una persona son finitos. Uno tiene que poder filtrar las solicitudes que uno tiene o si no nunca encontrará el tiempo para hacer las cosas importantes. El filtro *anti-spam* puede ser como el timbre de la puerta, que se usa para saber quién es y filtrar rápidamente si la persona es de interés o no”, agregó Faskha, de Soluciones Seguras.

De acuerdo con el especialista de Symantec, “ocuparse del *spam* es una pérdida de valioso tiempo de los empleados e impacta en el funcionamiento de la red. De acuerdo con un estudio realizado por **Nucleus Research**, los usuarios desperdician 16 segundos en identificar y eliminar cada correo electrónico basura. Esto genera un costo de 712 dólares por empleado en concepto de pérdida de productividad, lo que implica un costo anual de 70.000 millones de dólares en todas las empresas de los Estados Unidos”.

Desde el código

Por último, y sin que sea menos importante, abordaremos el ataque por código malicioso, o *malware*, y cómo prevenirlo. Este tipo de amenaza busca explotar en silencio las vulnerabilidades existentes en sistemas. En el caso de su variante *adware*, estos programas pueden recopilar, de forma secreta, información personal a través de Internet y transmitirla a otro equipo. Además, puede realizar un seguimiento de los hábitos de navegación del usuario con fines publicitarios.

Este tipo de aplicaciones también puede enviar contenido publicitario.

Ahora bien, el *adware* se puede descargar sin saberlo desde los sitios *web*, por lo general en *software* compartido (*shareware*) o en gratuito (*freeware*), correos electrónicos y mensajes instantáneos. En muchos casos, es posible que esté descargando inadvertidamente aplicaciones *adware* al aceptar la licencia para el usuario final de un programa.

“Contar con herramientas de prevención contra código malicioso remueve gusanos y trojanos de los archivos descargados, e impide que amenazas desconocidas se introduzcan en su equipo. Al igual que con el *spyware*, cualquier programa que circule, opere y transmita información desde la red sin control ni conocimiento de la gerencia de IT es potencialmente dañino y algo que debe controlarse o, de ser necesario, eliminarse”, comentó Severino, de Symantec.

De acuerdo con Borghello, de ESET, hoy el *malware* es uno de los principales problemas de seguridad para cualquier compañía y no contar con herramientas de prevención deja expuesto al usuario a miles de amenazas nuevas cada día, que tienen el objetivo robar información o beneficiar de otra forma a quienes las crean.

“Es importante destacar que el *malware* actual tiene objetivos comerciales y financieros, y evitar infectarse reduce directamente en la capacidad de producción, los costos y la imagen de la compañía; es decir que instalar una herramienta que detecte amenazas conocidas y desconocidas a través de técnicas proactivas es fundamental para proteger todos los activos de la compañía”, concluyó el especialista.

Todo un mercado negro ha crecido alrededor de los *hackers* y de los ladrones de identidad: tan solo el año pasado, el valor del mercado de la economía clandestina alcanzó cerca de 276 millones de dólares y una cuenta de correo electrónico se podía adquirir por solo diez centavos de dólar.

Por su parte, los intrusos también secuestran equipos domésticos y los utilizan para encubrir futuros delitos. Cuando un *hacker* usa la máquina de un usuario como base de ataque, este usuario pasa a ser sospechoso de los delitos que él está cometiendo de manera inadvertida.

| “AUNQUE LA MAYORÍA DE LAS EMPRESAS TIENEN INSTALADO UN ANTIVIRUS, VARIOS ESTUDIOS MUESTRAN QUE ENTRE EL DOS Y TRES POR CIENTO DE LOS ENCUESTADOS NO UTILIZAN PRODUCTOS DE ESTE TIPO EN SU ORGANIZACIÓN”. |

David Kelleher,
de GFI Software.

