Capítulo 2

Amenazas y vulnerabilidades de la seguridad informática

A finales de la década de los 80's las amenazas y vulnerabilidades a la seguridad informática eran objetos fáciles de identificar ya que las redes eran de uso exclusivo del ejercito militar de los Estados Unidos, pero poco a poco éstas fueron evolucionando hasta convertirse en una herramienta de uso común para las empresas, escuelas y hogares. Cabe destacar que los ataques que se llegaban a efectuar anteriormente eran muy peligrosos, lo que sucede en esta época, es que las nuevas amenazas ahora son más sofisticadas, ya que cuentan con una gran cantidad de variantes, un periodo de vida y distribución más corto, generalmente tienen un mayor alcance y provocan más daño, esto se ha ido dando de forma paralela con el crecimiento de la tecnología porque ahora hay mas personas dedicadas a burlar los sistemas de seguridad de las organizaciones o de cualquier usuario que tenga acceso a una red de computadoras.

Por lo tanto en este capítulo se explican los conceptos de "amenaza" y "vulnerabilidad", se dan a conocer las principales amenazas y vulnerabilidades que se han detectado desde sus inicios hasta el primer semestre del año 2009 así como su evolución y los daños que pueden causar si se llegan a efectuar.

2.1 Clasificación general de amenazas

En el campo de la seguridad informática se maneja mucho el término de "*amenaza*". El diccionario de la lengua española la define como el *"anuncio de un mal o peligro"*[13].
En términos generales, existen dos tipos de amenazas, las que provienen de sucesos naturales, como por ejemplo; terremotos, incendios forestales, huracanes, inundaciones, sequías, plagas, tsunamis y tornados y las amenazas provocadas por la actividad humana, como las explosiones, los incendios, los derrames de sustancias tóxicas, las guerras, el terrorismo, entre otros.

Dentro de las amenazas provocadas por la actividad humana relacionada con la seguridad informática, se puede decir que, *una amenaza representa la acción que tiende a causar un daño a los dispositivos o sistemas en donde se encuentra almacenada la información, atentando contra su confidencialidad, integridad y disponibilidad.*

Si una amenaza se llega a efectuar, ocurren diversos casos como por ejemplo; interrupción de un servicio o procesamiento de un sistema, modificación o eliminación de la información, daños físicos, robo del equipo y medios de almacenamiento de la información, entre otros. Las amenazas a la seguridad informática se clasifican en humanas, lógicas y físicas.

2.1.1 Humanas

Estos ataques provienen de individuos que de manera intencionada o no, causan enormes pérdidas aprovechando alguna de las vulnerabilidades que los sistemas puedan presentar. A estas personas se les bautizó de la siguiente manera, derivado del perfil que presenta cada individuo y para el presente trabajo únicamente se dan a conocer las más importantes las cuales se describen a continuación:

[13] http://diccionarios.elmundo.es/diccionarios/cgi/lee_diccionario.html?busca=amenaza&diccionario=1

- **Hacker:** Persona que vive para aprender y todo para él es un reto, es curioso y paciente, no se mete en el sistema para borrarlo o para vender lo que consiga, quiere aprender y satisfacer su curiosidad. Crea más no destruye.
- **Cracker:** Es un hacker cuyas intenciones van más allá de la investigación, es una persona que tiene fines maliciosos, demuestran sus habilidades de forma equivocada ó simplemente hacen daño sólo por diversión.
- **Phreakers:** Personas con un amplio conocimiento en telefonía, aprovechan los errores de seguridad de las compañías telefónicas para realizar llamadas gratuitas.

No se necesita ser un hacker para realizar alguna acción maliciosa a los sistemas de información, muchas veces un individuo puede realizar una acción indebida por diversión, por desconocimiento, entre otros. Hay que recordar que el talón de Aquiles de una empresa es su propio personal, es por ello que han surgido nuevos sistemas de ataque, los cuales se describen a continuación:

- **Ingeniería social:** Un atacante utiliza la interacción humana o habilidad social para obtener información comprometedora acerca de una organización, de una persona o de un sistema de cómputo. El atacante hace todo lo posible para hacerse pasar por una persona modesta y respetable, por ejemplo, pretende ser un nuevo empleado, un técnico de reparación, un investigador, etc.
- **Ingeniería social inversa:** El atacante demuestra de alguna manera que es capaz de brindar ayuda a los usuarios y estos lo llaman ante algún imprevisto, aprovechando la oportunidad para pedir la información necesaria y así solucionar el problema tanto del usuario como el propio.
- **Trashing (cartoneo):** Generalmente, un usuario anota su login y pasword en un papelito y luego, cuando lo recuerda, lo arroja a la basura. El trashing puede ser físico (como el que se describió) o lógico, como analizar buffers de impresora y memoria bloques de discos, entre otros.
- **Terroristas:** No se debe de entender a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.

- **Robo:** La información contenida en los equipos de cómputo puede copiarse fácilmente, al igual que los discos magnéticos y el software.
- **Intrusos remunerados:** Es el grupo de atacantes de un sistema más peligroso aunque es el menos habitual en las redes normales ya que suele afectar más a las grandes empresas u organismos de defensa. Se trata de personas con gran experiencia en problemas de seguridad y con un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos o simplemente dañar la imagen de la entidad afectada.
- **Personal interno:** Son las amenazas al sistema, provenientes del personal del propio sistema informático, rara vez es tomado en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Este tipo de de ataque puede ser causado de manera intencional o sin dolo.
- **Ex–Empleados:** Se trata de personas descontentas con la organización que aprovechan las debilidades de un sistema que conocen perfectamente, para dañarlo como venganza por algún hecho que consideran injusto.
- **Curiosos:** Personas con un alto interés en las nuevas tecnologías, pero no cuentan con la suficiente experiencia para ser considerados como hackers o crackers.
- **Personal interno:** Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta, porque se supone un ámbito de confianza muchas veces inexistente. Estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también son de tipo intencional. Por ejemplo: un electricista puede ser más dañino que el más peligroso de los delincuentes informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema.

2.1.2 Lógicas

En este tipo de amenazas se encuentran una gran variedad de programas que, de una u otra forma, dañan los sistemas creados de manera intencionada (software malicioso conocido como malware) o simplemente por error (bugs o agujeros).

Las amenazas más comunes son:

- **Adware:** Software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla.
- **Backdoors:** Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar 'atajos' en los sistemas de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.
- **Bombas Lógicas:** Son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.
- **Caballos de Troya:** Es aquel programa que se hace pasar por un programa válido cuando en realidad es un programa malicioso. Se llama troyano, caballo de Troya (trojan horse) por la semejanza con el caballo que los griegos utilizaron para disfrazar su identidad y ganar su guerra contra la ciudad de Troya. Así, un usuario podría descargar de un sitio Web de Internet un archivo de música que en realidad es un troyano que instala en su equipo un keylogger o programa que capture todo lo que escriba el usuario desde el teclado y después esta información sea enviada a un atacante remoto.
- **Exploits:** Programa o técnica (del ingles *to exploit*, explotar, aprovechar) que aprovecha una vulnerabilidad. Los exploits dependen de los sistemas operativos y sus configuraciones.
- **Gusanos (Worms):** Programas que se propagan por sí mismos a través de las redes, tomando ventaja de alguna falla o hueco de seguridad en los sistemas operativos o en el software instalado en los equipos de cómputo y que tiene como propósito realizar acciones maliciosas.
- **Malware:** Proviene de la agrupación de las palabras **"Mal**icious Soft**ware".** Este programa o archivo, está diseñado para insertar virus, gusanos, troyanos, spyware o

incluso bots (tipo de troyano que cumple una función específica), intentando conseguir información sobre el usuario o sobre la PC.

- **Pharming:** Consiste en suplantar el Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducir al usuario a una página Web falsa.
- **Phishing:** Es un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como *phisher* se hace parar por una persona o empresa de confianza en una aparente comunicación oficial electrónica.
- **Spam:** Mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. La más utilizada entre el público en general es la basada en el correo electrónico. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.
- **Spyware o programas espía:** Se refiere a las aplicaciones que recopilan información sobre una persona u organización, las cuales se instalan y se ejecutan sin el conocimiento del usuario. El objetivo principal del spyware es recolectar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.
- **Virus:** Programas que tienen como objetivo alterar el funcionamiento de la computadora y en ciertos casos alterar la información, se propagan sin el consentimiento y conocimiento del usuario. Algunos de los virus informáticos requieren de la intervención del usuario para comenzar a propagarse, es decir, no se activan por sí mismos, otros no la requieren y se activan solos.

En un principio, los virus se propagaban a través del intercambio de dispositivos de almacenamiento como disquetes y memorias de almacenamiento (USBs). Actualmente un equipo se puede infectar al abrir un archivo adjunto (ya sean documentos, imágenes, juegos, entre otros.) que llegue a través de un correo electrónico.

Los virus se distribuyen a través de mecanismos de intercambio de archivos, es decir, aquellos que se suelen utilizar para distribuir software, música y videos, están diseñados

para afectar a los sistemas operativos. La manera de erradicarlos y de protegerse contra éstos, es a través de un software antivirus, éste vendría siendo de poca ayuda si no se encuentra actualizado.

Dentro de este tipo de ataque (lógico), existen otro tipo de ataques los cuales tienen que ver con los sistemas y se han clasificado de la siguiente manera:

- **Ataques de Autenticación:** Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y Pasword. Algunos de estos ataques son: **Spoofing-Looping** (los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing), **IP Splicing-Hijacking, Spoofing (**Existen los IP Spoofing, DNS spoofing y Web Spoofing), **Net Flooding.**
- **Ataques de Monitorización:** Se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro. Se presentan como: **Shoulder Surfing, Decoy (Señuelos), Scanning (búsqueda), Snooping-Downloading, TCP Connect Scanning, TCP SYN Scanning.**
- **Uso de Diccionarios:** Son archivos con millones de palabras, las cuales pueden ser passwords utilizadas por los usuarios. El programa encargado de probar cada una de las palabras encripta cada una de ellas (mediante el algoritmos utilizado por el sistema atacado) y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema mediante el usuario correspondiente a la clave hallada.
- **Denial of Service (DoS):** Los ataques de denegación de servicio tienen como objetivo saturar los recursos de la víctima, de forma tal que se inhabilitan los servicios brindados por la misma. Ejemplos: **Jamming o Flooding, Syn Flood, Connection Flood, Net Flood, Land Attack, Smurf o Broadcast storm, Supernuke o Winnuke, Teardrop I y II, Newtear-Bonk-Boink, E-mail bombing-Spamming.**

- **Ataques de Modificación-Daño:** Se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Ejemplos de este tipo de Ataques: **Tampering o Data Diddling, Borrado de Huellas. Ataques mediante Java Applets, Ataques Mediante JavaScript y VBScript, Ataques Mediante Active X, Ataques por Vulnerabilidades en los Navegadores.**

2.1.3 Físicos

Este tipo de ataque está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en el cual se encuentran ubicados los centros de cómputo de cada organización o individuo. Las principales amenazas que se prevén en la seguridad física son:

1. **Incendios:** Generalmente son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad porque es considerado como el enemigo número uno de las computadoras debido a que puede destruir fácilmente los archivos de información y programas. Por ello es necesario proteger los equipos de cómputo, instalándolos en áreas que cuenten con los mecanismos de ventilación y detección adecuados contra incendios y que únicamente ingrese el personal autorizado.
2. **Inundaciones:** Se define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.
3. **Terremotos:** Fenómenos sísmicos que pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.
4. **Señales de Radar:** Las señales muy fuertes de radar infieren en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 volts/Metro o mayor. Ello podría ocurrir sólo si la

antena respectiva fuera visible dese una ventana del centro de procesamiento respectivo y en algún momento estuviera apuntando directamente hacia dicha ventana.

5. **Instalaciones eléctricas:** Trabajar con computadoras implica trabajar con electricidad. En las instalaciones eléctricas se debe considerar los siguientes aspectos: picos y ruidos electromagnéticos, buen cableado, pisos de placas extraíbles, un buen sistema de aire acondicionado, emisiones electromagnéticas.

Esta clasificación, de los principales ataques a la seguridad informática van muy ligadas, son aspectos que no deben pasar desapercibidas en ninguna organización ya que conforman la base para tener una buena estructura de seguridad, si alguna de éstas falla, no se podrá tener la certeza de mantener protegida la información, lo que puede provocar grandes daños tanto económicos.

2.2 Clasificación general de vulnerabilidades

En materia de seguridad informática los puntos débiles de los sistemas son comúnmente aprovechados por personas que buscan la manera de acceder y realizar alguna acción maliciosa para su propio beneficio, desgraciadamente todos los sistemas tecnológicos presentan alguna debilidad, por ejemplo, los sistemas requieren de energía eléctrica, sin ella simplemente no funcionan.

Es por ello que es muy importante conocer esos puntos débiles, una vez identificados, las empresas definen las medidas de seguridad adecuadas con la finalidad de reducir los riesgos a los que pueda estar sometida, evitando que se efectúe una amenaza.

Estos puntos débiles se conocen como *vulnerabilidades*, el diccionario de la real academia de la lengua española define la palabra vulnerable como: *"Que puede ser herido o recibir lesión física o moralmente"*. [14] En materia de seguridad informática las vulnerabilidades

[14] http://diccionarios.elmundo.es/diccionarios/cgi/lee_diccionario.html?busca=vulnerable&diccionario=1

son las debilidades de los activos de las organizaciones, las cuales podrían ser utilizadas por las amenazas para causar daño a los sistemas.

En la figura 2.1 se muestra una clasificación de las principales vulnerabilidades a las que las organizaciones están expuestas:

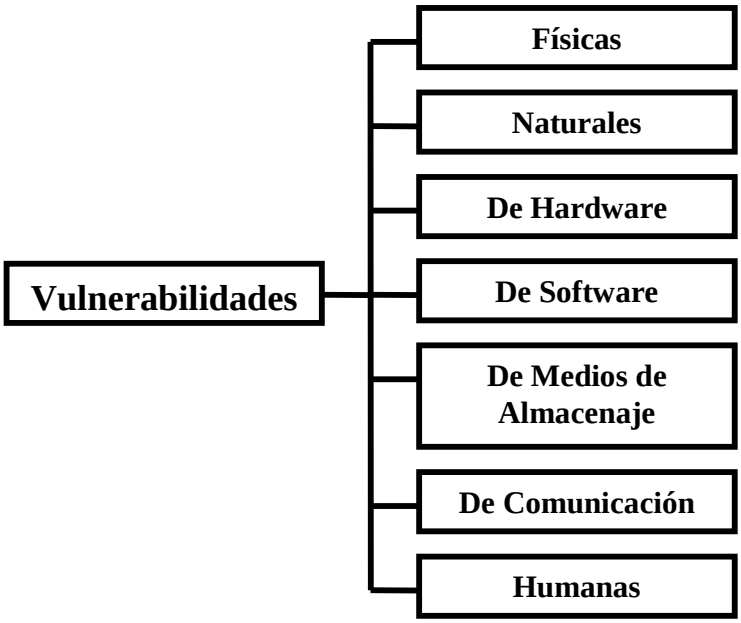


Figura 2.1 Principales Vulnerabilidades

A continuación se describirán de manera general cada uno de los diferentes tipos de vulnerabilidades:

- **Vulnerabilidad física**: Se refiere al lugar en donde se encuentra almacenada la información, cómo los centros de cómputo. Para un atacante le puede resultar más sencillo acceder a la información que se encuentra en los equipos que intentar acceder vía lógica a éstos o también se puede dar el caso de que al acceder a los centros de cómputo el atacante quite el suministro de energía eléctrica, desconecte cables y robe equipos. Si este tipo de vulnerabilidad se llega a efectuar, afecta a uno de los principios básicos de la seguridad informática que es la disponibilidad.
- **Vulnerabilidad natural:** Se refiere a todo lo relacionado con las condiciones de la naturaleza que ponen en riesgo la información. Por ejemplo, incendios, inundaciones, terremotos, huracanes, entre otros. Por ello es conveniente contar con

las medidas adecuadas, como tener respaldos, fuentes de energía alterna y buenos sistemas de ventilación, para garantizar el buen funcionamiento de los equipos.

- **Vulnerabilidad de hardware:** Hacen referencia a los posibles defectos de fábrica o a la mala configuración de los equipos de cómputo de la empresa que puedan permitir un ataque o alteración de éstos. Por ejemplo; la falta de actualización de los equipos que se utilizan o la mala conservación de los equipos son factores de riesgo para las empresas.
- **Vulnerabilidad de software:** Está relacionado con los accesos indebidos a los sistemas informáticos sin el conocimiento del usuario o del administrador de red. Por ejemplo; la mala configuración e instalación de los programas de computadora, pueden llevar a un uso abusivo de los recursos por parte de usuarios mal intencionados. Los sistemas operativos son vulnerables ya que ofrecen una interfaz para su configuración y organización en un ambiente tecnológico y se realizan alteraciones en la estructura de una computadora o de una red.
    - **Vulnerabilidad de medios de almacenaje:** Son los soportes físicos o magnéticos que se utilizan para almacenar la información. Por ejemplo; los disquetes, cd-roms, cintas magnéticas, discos duros, entre otros. Por lo tanto si estos soportes no se utilizan de manera adecuada, el contenido de los mismos podrá ser vulnerable a una serie de factores que afectan la integridad, disponibilidad y confidencialidad de la información.
    - **Vulnerabilidad de comunicación:** Es el trayecto de la información, es decir, donde sea que la información viaje, ya sea vía cable, satélite, fibra óptica u ondas de radio, debe existir seguridad. El éxito en el tránsito de los datos es un aspecto crucial en la implementación de la seguridad de la información por lo tanto se debe evitar:
        - Cualquier falla en la comunicación que provoque que la información no esté disponible para los usuarios, o por el contrario, que esté disponible para quien no tiene autorización.
        - Que la información sea alterada afectando la integridad de ésta.
        - Que la información sea capturada por usuarios no autorizados, afectando su confidencialidad.

- **Vulnerabilidad humana:** Se refiere a los daños que las personas puedan causar a la información y al ambiente tecnológico que la soporta sea de manera intencional o no. Muchas veces los errores y accidentes que amenazan a la seguridad de la información ocurren en ambientes institucionales, la principal vulnerabilidad es la falta de capacitación y la falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, etc. También existen las vulnerabilidades humanas de origen externo, como son; el vandalismo, estafas, invasiones, etc.

Las vulnerabilidades están ligadas a los hombres, a los equipos y al entorno. Por ejemplo, en cualquier organización de nada serviría tener herramientas de seguridad como (firewall's, IDS, antivirus, entre otros) si los centros de cómputo estuviesen en un lugar inadecuado y accesible a cualquier gente, ya que se está expuesto a que cualquier individuo realice un uso indebido a los equipos provocando grandes daños.

Existen otros tipos de vulnerabilidades que también afectan a las organizaciones a nivel mundial, pero que muy difícilmente se toman en cuenta, estas son:

1. **Vulnerabilidad de tipo Económico:** Se refiere a la escasez y un mal manejo de los recursos destinados a las organizaciones para el mejoramiento de las diversas áreas.
2. **Vulnerabilidad de tipo Socio-Educativa:** Se refiere a las relaciones, comportamientos, métodos y conductas de todas aquellas personas que tienen acceso a una red y lo que deseen de ésta.
3. **Vulnerabilidad de tipo Institucional/Política:** Se refiere a los procesos, organizaciones, burocracia, corrupción y autonomía que tienen todos los países del mundo. Desgraciadamente un atacante puede someter a ciertas personas a revelar información, realizando actos de corrupción.

Por lo anterior mencionado se puede decir que una vulnerabilidad es el paso previo a que se efectúe una amenaza, ésta se encuentra presente en todo momento, pero se reducen los riesgos teniendo en cuenta buenas medidas de seguridad.

Es recomendable que las empresas realicen análisis de riesgos detallado de las vulnerabilidades a las que están expuestos, como las físicas, de software, humanas, entre otros, para evitar en la medida de lo posible ser puntos blancos de ataque.
Es muy importante ser consciente de que por más que las empresas sean las más seguras desde el punto de vista de ataques externos, Hackers, virus, entre otros, la seguridad de la misma sería nula si no se ha previsto como combatir un incendio.
Por ello se hace mucho hincapié sobre la importancia de la seguridad informática, ya que se está invirtiendo para proteger el objeto más valioso de cualquier empresa, que es *la información.*

2.3 Identificación de las principales amenazas y vulnerabilidades a nivel Nacional e Internacional

Conforme ha ido avanzando la tecnología en el mundo de la seguridad informática, las amenazas se han vuelto cada vez más sofisticadas y en ocasiones han sido difíciles de detectar, lo que implica estar al día y tener conocimiento de las nuevas amenazas que van surgiendo, buscando la manera de mantener los sistemas actualizados para evitar que alguna de estas amenazas se lleve a cabo con éxito.

Por este motivo, para el presente trabajo se realizó un análisis basado en estudios e informes presentados por las empresas PandaLabs, PandaSecurity, McAfee, Sophos y la UNAM-CERT, sobre las principales amenazas y vulnerabilidades que se han presentado hasta el año 2009 y algunos comparativos con años anteriores.

En primera instancia es necesario conocer las principales amenazas de mayor peligro que se han efectuado en los últimos 20 años, esta recopilación la realizó la empresa PandaSecurity y se basó en la capacidad de distribución epidémica y daño causado tanto a usuarios domésticos como a las diversas organizaciones. A continuación en la tabla 2.1 se muestran estos acontecimientos.

Tabla 2.1. Las amenazas más peligrosas en los últimos 20 años

Año	Amenaza	Característica
1988	Viernes 13 ó Jerusalén	Creada en Israel y detectada por primera vez en la ciudad de Jerusalén. La creación de esta amenaza estaba relacionada con el aniversario de la fundación del Estado de Israel, aunque coincidió que apareció un viernes 13. Este virus infectaba archivos .COM y .EXE.
1993	Barrotes	Se trata del primer virus en español. El virus se hospedaba en la PC para activarse en enero 5, cuando desplegaría unas barras tipo barrotes en la pantalla.
1997	Cascada o letras cayendo	Creado en Alemania, provocaba que las letras proyectadas en la pantalla cayeran en cascada una vez que la PC fuera infectada.
1998	CIH o Chernobyl	Producido en Taiwán, tan solo le tomó una semana distribuirse para infectar miles y miles de PC's. El virus infecta los archivos ejecutables de 32 bits de Windows 95/98.
1996	Melissa	Detectado en EU. Fue uno de los primeros en utilizar con gran éxito las tácticas de ingeniería social para su distribución masiva, llegaba al buzón de los correos con el texto "Aquí está el documento que me pediste… no se lo muestres a nadie más".
2000	I love you o Love letter	El muy popular virus salió de Filipinas y fue distribuido con el asunto "ILoveYou". Millones de PC's fueron infectadas en todo el mundo en solo unas semanas y su alcance fue tan amplio que golpeó al mismo Pentágono.
2001	Klez	Fue creado en Alemania y solo infectaba computadoras los días 13 de cada mes non. Nimda: Es 'admin' escrito al revés. Su poder consistió en conseguir privilegios de administrador al infectar PC's. Apareció en China.
2003	SQLSlammer Blaster Sobig	-Fue un gran dolor de cabeza para las empresas pues en sólo unos días afecto a más de 500,000 servidores. -Contenía dos mensajes escondidos en su código, uno decía "I just want tos ay love you, San!" y "Billy gates, why do you make this posible? Stop making money and fix your software". -Este virus fue muy famoso y vino acompañado de numerosas variantes, de las cuales la F fue la más dañina, generando millones de copias de sí mismo.
2004	Bagle Netsky	-Este ejemplar y sus variantes rondan e infectan las PC's lo que lo convierte en uno de los virus más prolíficos. -Se cree que este gusano provino de Alemania. Su función era explotar vulnerabilidades de Internet Explorer.
2008	Conficker	Se cree que la finalidad de este gusano que ha infectado decenas de millones de PC's junto con sus variantes, ha sido armar una gran red de computadoras zombie.

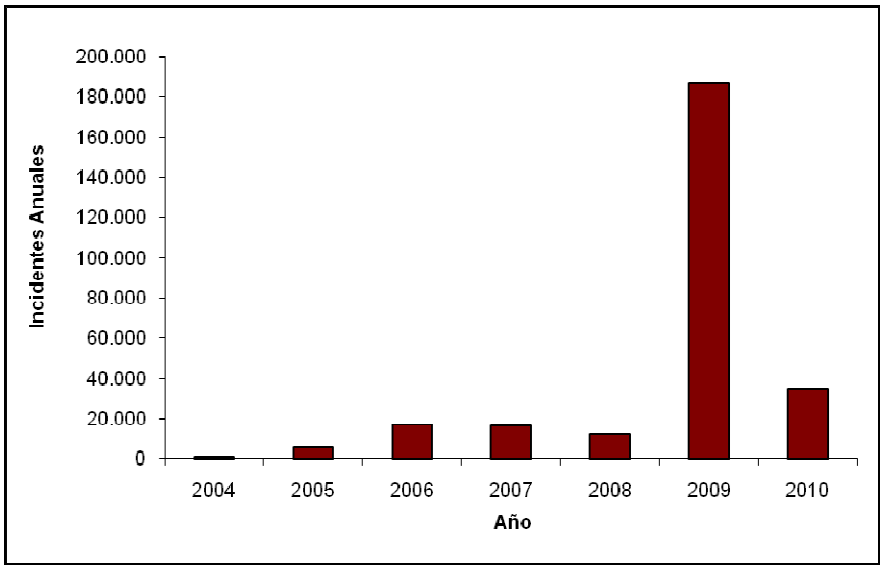
A través de los años, las amenazas a los sistemas de información se han vuelto más sofisticadas llegando a causar un mayor daño a las empresas o a los usuarios comunes, por ello es necesario hacer conciencia sobre la peligrosidad que se puede tener cuando se logre con éxito una amenaza.

En nuestro país la Universidad Nacional Autónoma de México (UNAM) y el Equipo de Respuesta a Incidentes de Seguridad en Cómputo (CERT) el cual, se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo ayudando a mejorar la seguridad de los sitios. Dieron a conocer los principales incidentes que se han producido en los últimos años (2004 - 2010).

En la gráfica 2.1 se aprecia que en el año 2004 se reportaron 1,060 incidentes, para el año 2005 y 2006 hubo un incremento de 6,742 y 17,016 incidentes respectivamente, así mismo del 2007 al 2008 disminuyeron de 16,778 a 12,595 incidentes. Se puede observar que para el año 2009 se incrementaron drásticamente el número de incidentes hasta llegar a los 187,393 y finalmente se logró disminuirlos en el año 2010 a 34,908.

Incidentes Anuales

Año	Incidentes
2004	1,060
2005	6,472
2006	17,016
2007	16,778
2008	12,595
2009	187,393
2010	34,908

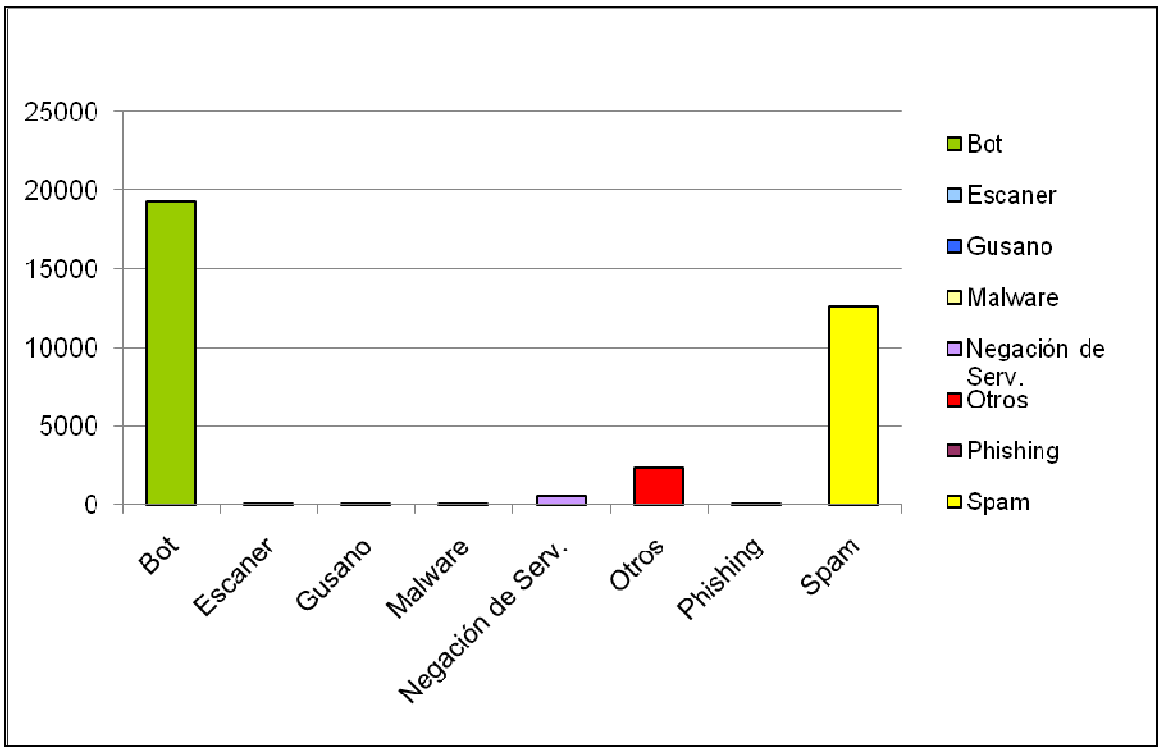


Gráfica 2.1 Incidentes Anuales

Los principales incidentes que se reportaron en el año 2010 fueron los bots y el spam. En la gráfica 2.2 se observa que los bots alcanzaron un total de 19,318 incidentes durante el 2010, así mismo el spam obtuvo 12,626 incidentes y en último lugar lo ocupan los gusanos con tan sólo un incidente anual.

Incidentes Anuales

Reporte	Incidente	%
Bot	19,318	35.5
Escaner	24	.04
Gusano	1	.001
Malware	2	.003
Negación de Servicio	572	1.05
Otros	2,357	4.34
Phishing	8	0.014
Spam	12,626	23.26

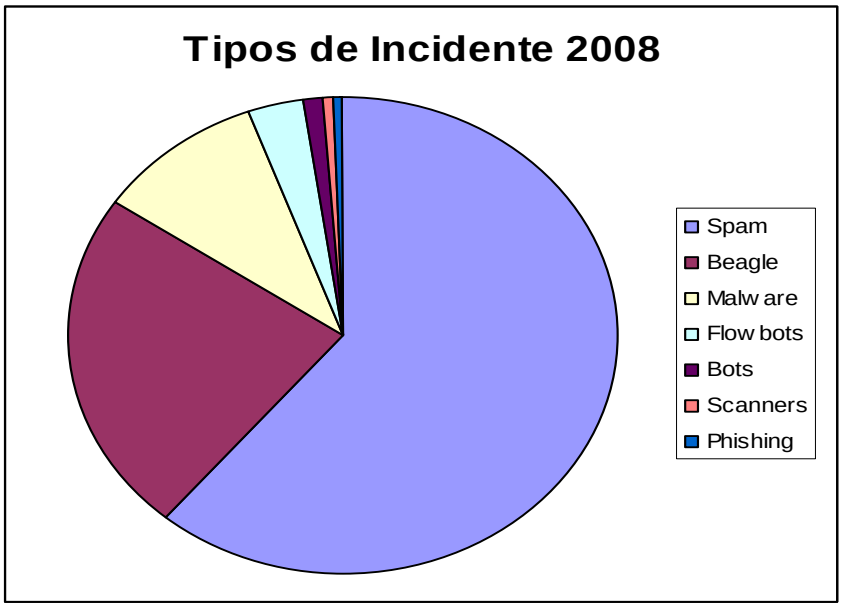


Gráfica 2.2 Tipos de incidentes en el 2010

Los principales incidentes que se reportaron en el año 2008 fueron el spam, beagle (gusano), malware, flowbots (virus), bots (virus), scanners y phishing. En la gráfica 2.3 se observa que el Spam ocupa el 60.56% de todos los incidentes generados en ese año, después le sigue el Beagle con un 23% y en último lugar se encuentra el phishing ocupando el 0.5%.

Principales Problemas

Reporte	%
Spam	60.56
Beagle	23.28
Malware	9.75
Flowbots	3.23
Bots	1.19
Scanners	0.63
Phishing	0.5

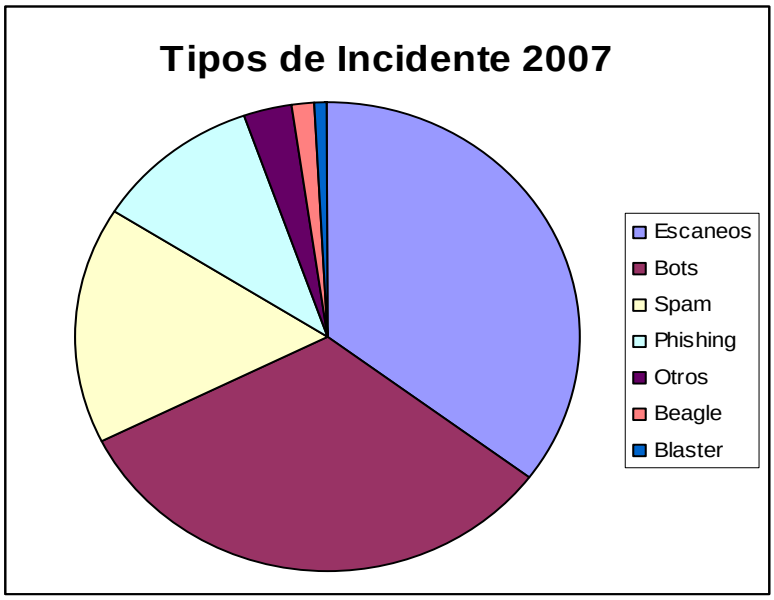


Gráfica 2.3 Tipos de Incidente en el 2008

Para el año 2007 se puede observar en la gráfica 2.4 que el principal incidente fueron los escaneos, ocupando el 35.4% muy a la par de los bots con el 32.16%, el spam se encontraba en tercer lugar con el 16.28% y en último lugar se encontró el blaster (virus) representando el 0.85%

Principales problemas

Reporte	%
Escaneos	35.40
Bots	32.16
Spam	16.28
Phishing	10.91
Otros	3.01
Beagle	1.39
Blaster	0.85

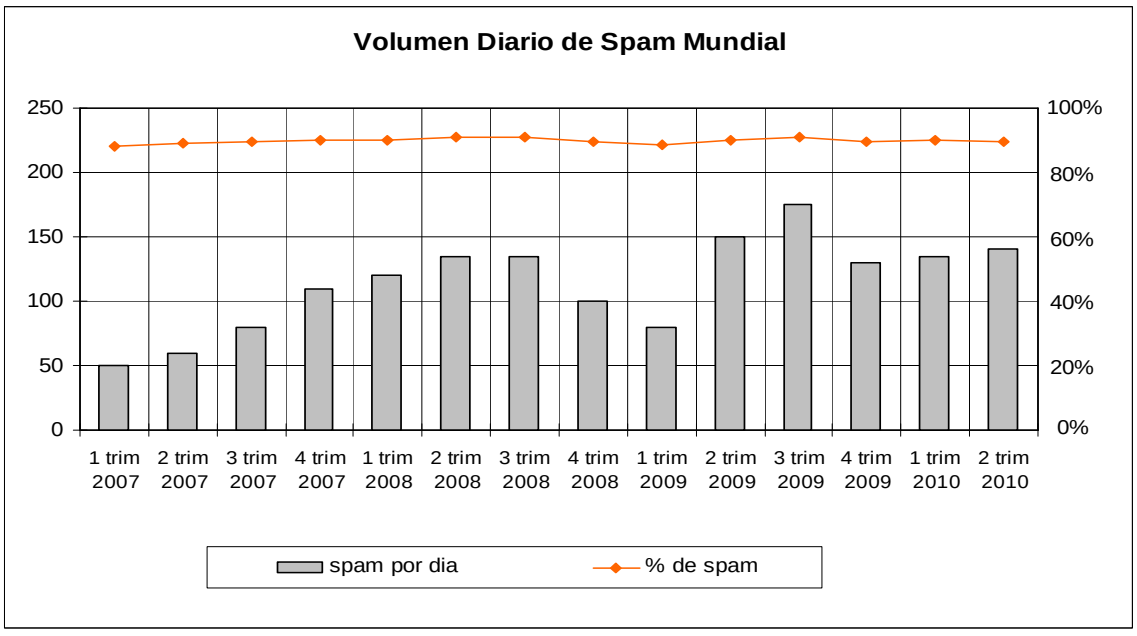


Gráfica 2.4 Tipos de incidente en el 2007

Analizando ambas gráficas se puede observar que, los principales problemas que se presentaron en el año 2007 y 2008 fueron el spam, el beagle, el malware, los flowbots, los bots, scanners, el phishing entre otros. Por otra parte en el año 2007 fueron los escaneos con un 37% pero para el año 2008 disminuyó al 0.63%, en ese mismo año el spam representaba el 16.28% pero en el 2008 éste se incrementó, representando el 60.56%, ocupando el primer lugar en incidentes detectados. En estos años hubo una notable diferencia con respecto a los tipos de ataques que se detectaron, algunos de éstos se incrementaron de manera considerable y otros disminuyeron drásticamente.

Análisis del informe trimestral comprendido del periodo (Abril - Junio) del 2009 realizado por la empresa McAfee sobre amenazas de seguridad informática

En este informe se presentan las últimas estadísticas y análisis acerca de las amenazas que llegan a través del correo electrónico y la web. En la gráfica 2.5 se muestra el porcentaje de spam desde el último trimestre del 2007 al segundo trimestre del 2010.



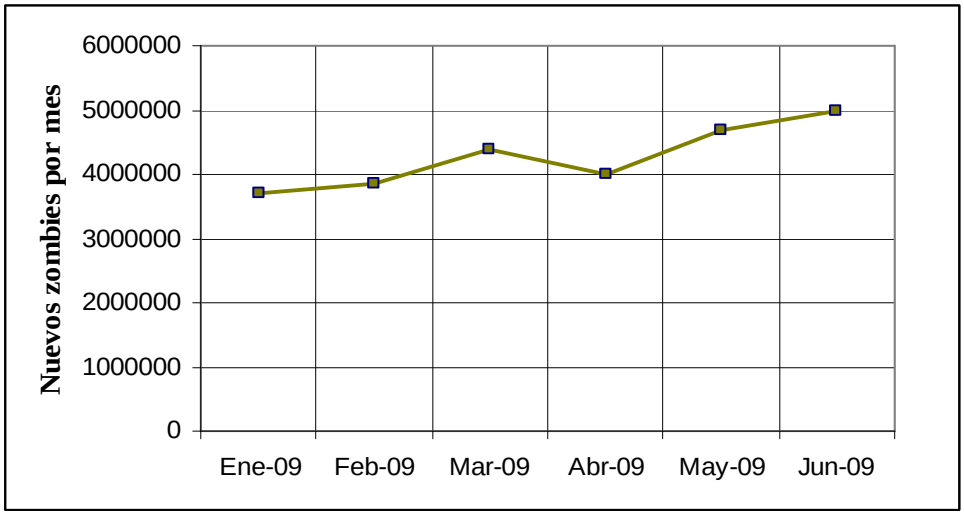
Gráfica 2.5 Volúmenes de spam mundiales y el spam como un porcentaje de todo el correo

Durante el 2do trimestre del año 2010 el tráfico de spam representó el 88% de todo el tráfico de correo electrónico en Internet, un porcentaje ligeramente inferior que en el trimestre anterior.

En general, el spam parece que recupera la tendencia ascendente, aunque de forma lenta, tras la caída del 20% sufrida entre el tercer y cuarto trimestre del año 2009, precisamente en ese trimestre se registró el mayor volumen de spam con casi 175,000 millones de mensajes diarios.

Zombies

En este informe se analizaron lo que hoy en día se conocen como "zombis". Un **zombie** es la denominación que se asigna a computadoras tras haber sido infectadas por algún tipo de malware (el nombre procede de los zombis o muertos vivientes esclavizados). Existen grupos organizados que llegan a controlar decenas de miles de computadoras infectadas (zombis), que usan para generar grandes cantidades de tráfico proveniente de una multitud de diversas fuentes en Internet, dirigido a una sola red o servidor. Otro uso frecuente de los zombis es el envío de spam. En la gráfica 2.6 se muestra el incremento de zombis durante el año 2009, llegando a producir aproximadamente 5 millones de éstos.



Gráfica 2.6 Nuevos zombis que envían spam, por mes

Este problema va acompañado del envío de spam, por lo tanto, el spam sigue representando la principal preocupación que tienen las organizaciones en el mundo.

Nuevos zombies

En la tabla 2.2 se muestra una lista de los 10 principales países que producen nuevos zombis comprendido en el periodo de abril a junio del año 2009. Se aprecia que Estados Unidos ocupa el primer lugar con el 15.7%, seguido de China (9.3%) y en último lugar se encuentra España con el 2.6%. Estos países representan el 60.7% de producción de zombies a nivel mundial, lo que significa que el problema depende en gran medida de estos lugares, por lo tanto deben de prestar mas atención para ayudar a mitigar el problema al que están siendo víctimas.

Tabla 2.2 Países productores de nuevos zombis por trimestre

País	%	País	%
Estados Unidos	15.7	Italia	4
China	9.3	República de Corea	3.8
Brasil	8.2	India	3.2
Rusia	5.6	Reino Unido	3
Alemania	5.3	España	2.6

Spam por país

En la tabla 2.3 se muestra una relación de los países que producen mayor porcentaje de spam a nivel mundial. Estos datos se obtuvieron del periodo comprendido entre el primer semestre del año 2009 y cuarto trimestre del 2008.

Tabla 2.3 Países con mayor producción de spam

País	2º trim. 2009 % total	País	1er trim 2009 % total	País	4 º trim 2008 % total
Estados Unidos	25.5	Estados Unidos	35	Estados Unidos	34.3
Brasil	9.8	Brasil	7.3	Brasil	6.5
Turquía	5.8	India	6.9	China	4.8
India	5.6	Rep. de Corea	4.7	India	4.2
Polonia	4.9	China	3.6	Rusia	4.2
Rep. de Corea	4.6	Rusia	3.5	Turquía	3.8
Rusia	2.4	Turquía	3.2	Rep. de Corea	3.7
Rumania	2.3	Tailandia	2.1	España	2.4
España	2.1	Rumania	2	Reino Unido	2.3
Rep. Checa	1.9	Polonia	1.8	Colombia	2
% total del spam mundial	64.9		70		68.3

Del porcentaje total de estos países se puede notar que hubo un descenso del 5% en el segundo trimestre del año 2009 con respecto al primer trimestre de ese mismo año, lo que indica que la disminución de spam aún es lento, falta mucho por hacer, los países tienen que trabajar en ello para evitar seguir siendo puntos blancos de ataque. Sin embargo, el 65% de la producción de spam sigue procediendo de estas diez naciones.

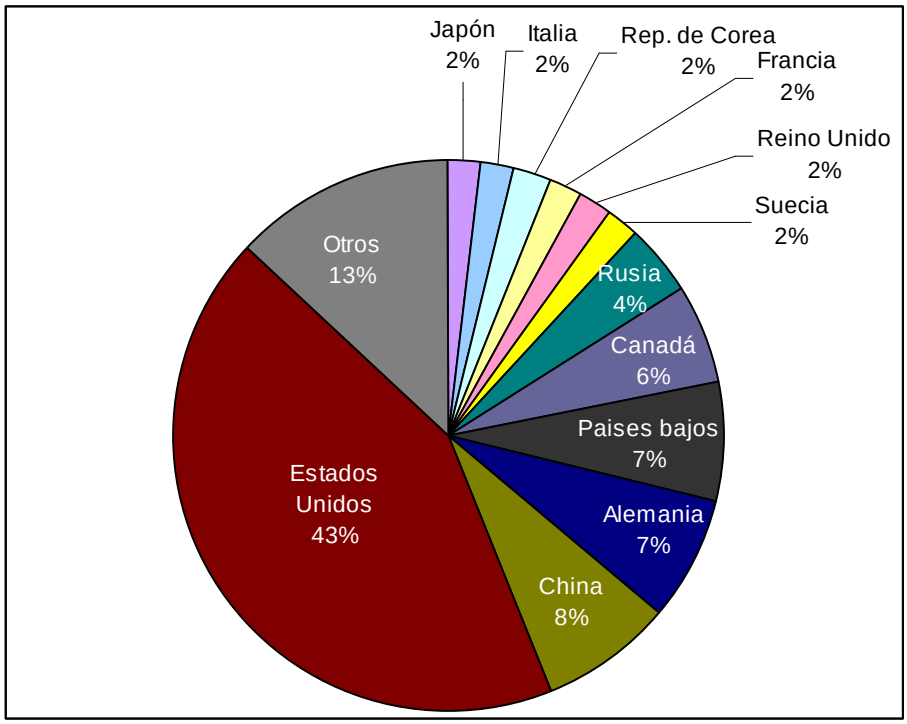
En el último trimestre del 2008 Estados Unidos tenía el 34.3% de spam y para el segundo trimestre del 2009 ocupa el 25.5%, lo que significa que disminuyó aproximadamente un 10% en este periodo. Con lo que respecta a Brasil, sigue manteniendo el segundo lugar con el 9.8% (2trim2009), Turquía se encuentra en el tercer lugar con el 5.8% (2trim2009), a inicios de año estaba en el séptimo lugar, lo que indica que se incrementó el spam en ese país.

Resulta interesante cómo estos países van cambiando su posición en periodos de tiempo muy cortos, se puede decir que, día a día se está en constante lucha contra los ciberdelincuentes, esperando a que estos índices disminuyan considerablemente sin afectar a las organizaciones.

Phishing

Otro problema común en la mayoría de los países es la distribución de sitios web de Phishing, en este caso Estados Unidos abarca el 43%, significa que, ocupa casi el 50% con respecto a los países del mundo, esta cifra es alarmante, puesto que como se ha visto, el mayor problema radica en este país que es una de las principales potencias, por lo tanto, es vulnerable a cualquier tipo de ataque.

En la gráfica 2.7 se observan los países con menor porcentaje de phishing son Japón, Italia, República de Corea, Francia, Reino Unido y Suecia con el 2% respectivamente.

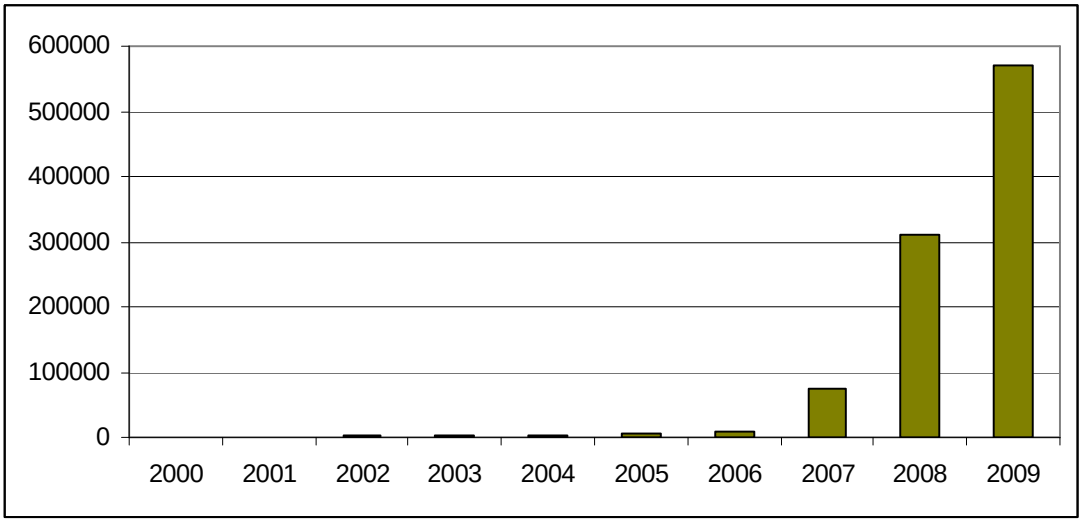


Gráfica 2.7 Distribución de los sitios Web de Phishing

Malware

McAfee señala que el malware y la ciber-delincuencia existen desde los inicios de la informática e Internet. Los virus atacaban el sector de arranque, eran parasitarios y se distribuían principalmente a través de discos flexibles. Aparece el spam y su objetivo era el mismo que tienen hoy día: vender algo. Cuando se produjo la aparición del uso de Internet, el malware y la ciber-delincuencia, evolucionaron para adaptarse a los cambios en el comportamiento de los usuarios. En la actualidad, la vida de muchas personas está completamente ligada al uso de las computadoras, ya sea para pagar facturas online, utilizar blogs o comunicarse con otros en Facebook y Twitter, la realidad es que ahora las personas y sus identidades son digitales. Los creadores de malware y los ciber-delincuentes conocen bien esta dinámica y no se quedan atrás ante esta.

Los troyanos, ladrones de contraseñas, crecen rápidamente y siguen siendo una de las herramientas favoritas de los ciber-delincuentes. Las herramientas para crear estos troyanos están disponibles de forma generalizada en Internet y hay muchos sitios dedicados a venderlas como un servicio, su función es bien sencilla: robar contraseñas, el secreto de su éxito radica en la complejidad del propio troyano. En la gráfica 2.8 se muestra el crecimiento del malware de robo de contraseñas en el periodo comprendido del año 2000-2009.



Gráfica 2.8 Crecimiento del Malware de robo de contraseñas

Claramente se observa que este incremento se disparó a partir del año 2008 registrando más de 300,000 robos de contraseñas y para el 2009 casi se llegaba a cubrir los 600,000 robos de contraseñas en todo el mundo.

En la mayoría de los casos, los troyanos ladrones de contraseñas infectan a usuarios que abren un adjunto de correo electrónico que descarga malware de un sitio Web malicioso, una vez que se encuentran instalados, los troyanos recopilan nombres de usuarios y contraseñas de una gran variedad de programas, como Internet Explorer, sesiones FTP y muchos juegos online.

Los datos de identidades recogidos, se envían a un servidor controlado por los ciber-delincuentes, que los venden a un comprador utilizando distintos medios, como por ejemplo, sitios de subastas o ventas masivas.

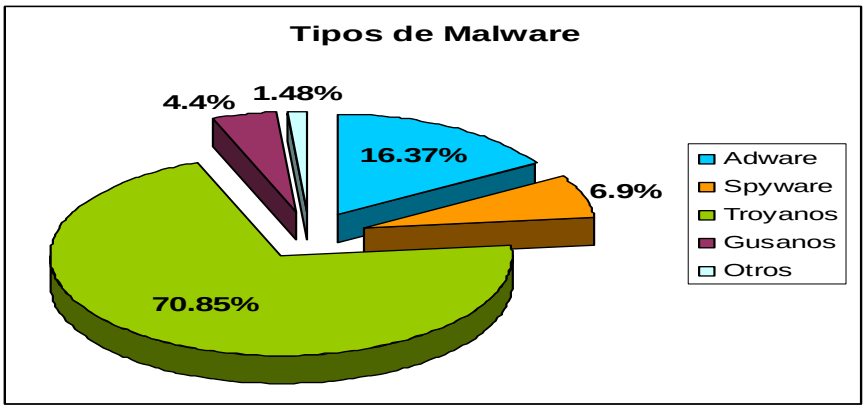
McAfee AvertLabs ha observado que estos programas maliciosos son cada vez más complejos, son más sigilosos que nunca y con frecuencia disponen de mecanismos de autoprotección para garantizar su supervivencia en una PC infectada. Asimismo, cada vez son de índole más general. Antes, los troyanos se creaban específicamente para atacar a una institución concreta. Sin embargo, últimamente han estado recopilando cada vez más datos de una mayor variedad de objetivos, maximizando así su eficacia.

Análisis del informe trimestral comprendido del periodo (Abril – Junio) del 2009 realizado por la empresa PandaLabs.

En este informe se dan a conocer las principales amenazas que afectan a los sistemas de comunicación, así como los principales países que sufren algún tipo de Malware.

Distribución de las nuevas amenazas detectadas

En la gráfica 2.9 se muestran los diferentes tipos de malware detectados durante este periodo. Según los datos presentados por PandaLabs se puede observar que en la categoría de malware predominan los troyanos ocupando el 70.85% seguido del Adware con el 16.37% mientras que los gusanos únicamente ocupan el 4.40%.

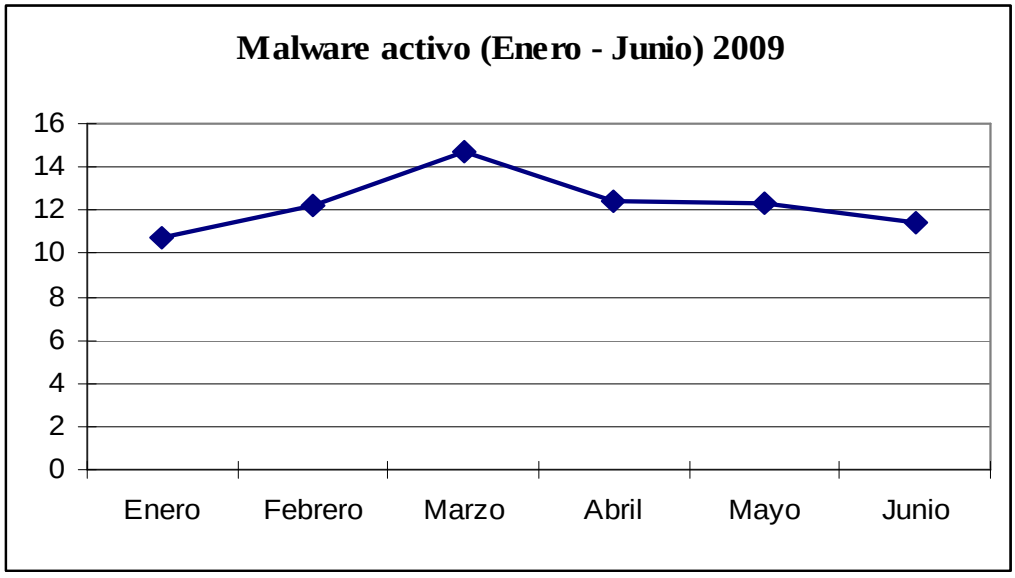


Gráfica 2.9 Tipos de Malware

Malware Activo

PandaLabs define al Malware en dos posibles estados que es el latente y el activo. El malware latente es aquel que está alojado en una máquina pero sin realizar ninguna acción, es decir, está a la espera de ser ejecutado directamente por el usuario o bien de forma remota por el cieberdelincuente, una vez que es ejecutado comienza a realizar las acciones dañinas para las que está programado, por lo tanto, el estado de este malware cambia y pasaría de estar latente a activo.

En la gráfica 2.10 se puede observar la evolución de malware activo durante el primer semestre del 2009. Estos datos se obtuvieron gracias a la herramienta ActiveScan 2.0 proporcionada de manera gratuita a cualquier usuario que ingresaban a la página web de pandalabs: (www.pandasecurity.com/infected_or_not/). De esta manera se comprueba si los equipos están infectados. Los resultados que se recopilaron fueron los siguientes:

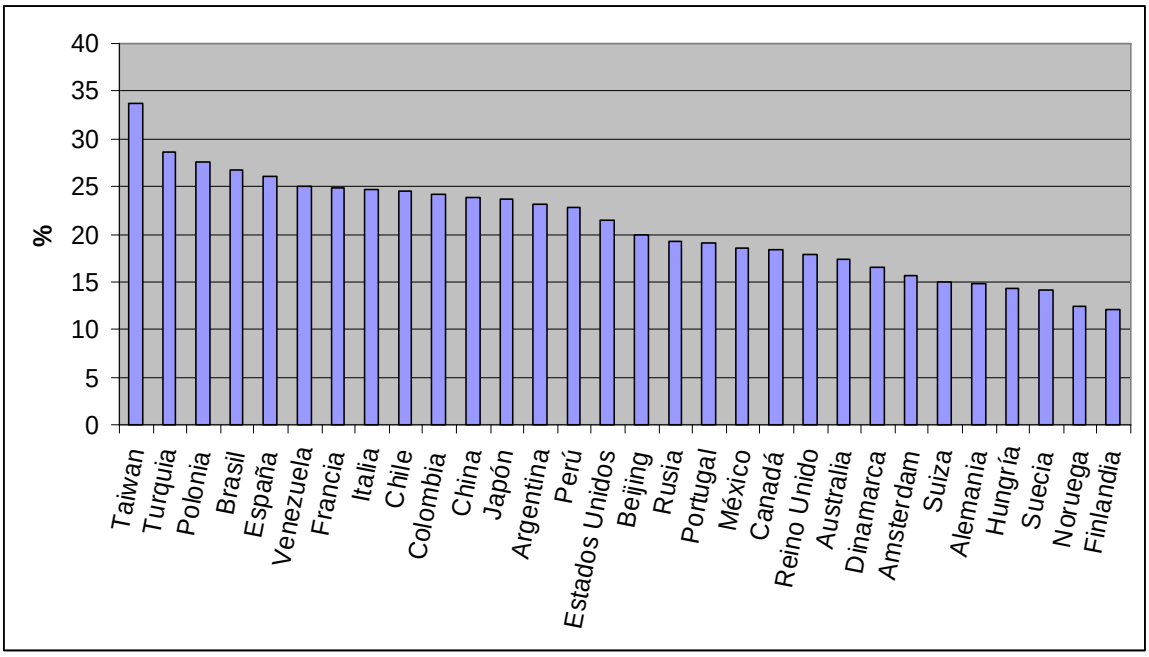


Gráfica 2.10 Evolución de malware activo durante el primer semestre del 2009

Enero mostró un comienzo bajo con el 10.78% de PC's Infectados. Los siguientes dos meses fueron en aumento llegando al 14.68% en marzo, a partir de ahí empezó a disminuir paulatinamente hasta el mes de junio con un 11.39%.

Aunque aún se considera un porcentaje relativamente bajo, es muy importante mantener el control del Malware, de tal manera que se evite en la medida de lo posible que se éste se incremente y para ello se tienen que proporcionar tanto las herramientas adecuadas para solucionar este tipo de amenaza, así como, crear buenos hábitos en los usuarios quienes son los más vulnerables a padecer algún tipo de malware.

En la siguiente gráfica 2.11 se muestra la evolución de máquinas infectadas por país registradas en el primer semestre del año 2009.



Gráfica 2.11 Países con mayor porcentaje de malware (Enero – Junio 2009)

Se puede observar que Taiwan es el país con mayor índice de malware activo, con el 33.63%, por debajo del 30% se encuentra Turquía (28.6%) y Polonia (27.54%). México se encuentra por debajo del 20% seguido de Canadá y del Reino Unido. Los países nórdicos como Suecia (14.2%), Noruega (12.48%) y Finlandia (12.17%) se encuentran con el menor número de PC's infectados de malware activo durante este periodo.

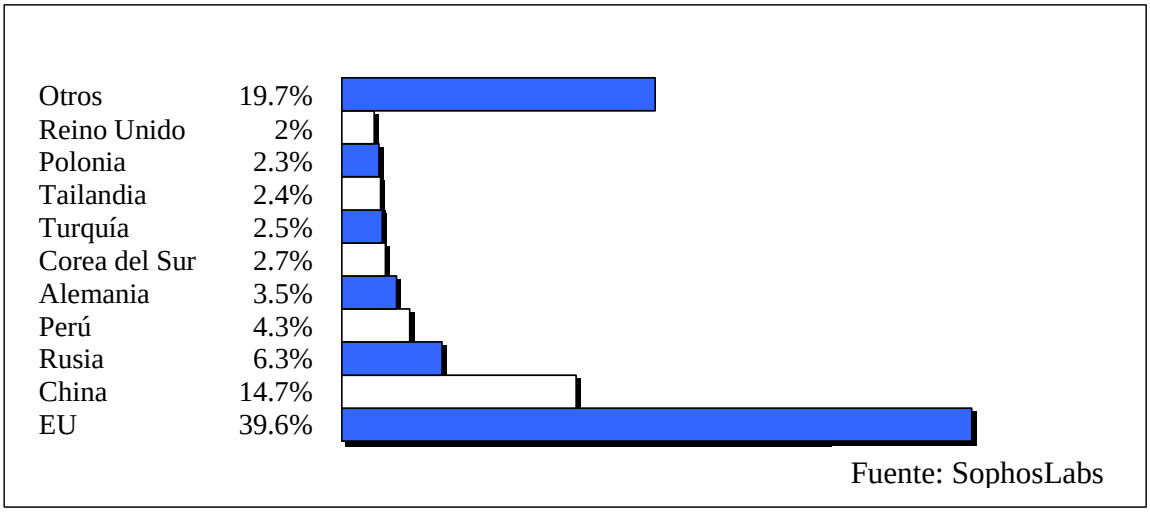
PandaLabs enfatiza que el malware activo a través de los troyanos es el mayor problema que se ha detectado a nivel mundial. México se encuentra en el lugar 19 de 30 países que se

consideraron con el mayor índice de computadoras infectadas, lo que significa que se deben de incrementar las medidas de seguridad para mitigar estos ataques e ir reduciendo este índice, para ello se deben de considerar algunos aspectos como la inversión en materia de seguridad informática y hacer conciencia sobre la situación que se vive a nivel nacional e internacional ya que siempre se está expuesto a sufrir cualquier tipo de incidente.

Análisis realizado por la empresa Sophos durante el primer semestre del 2009

El análisis presentado por la empresa Sophos da a conocer los principales países con mayor cantidad de malware en las páginas web, así como la reproducción de spam por país y por continente.

En la gráfica 2.12 se muestran los países que contienen malware en las páginas web, se observa que Estados Unidos encabeza la lista representado el 39.6%, seguido de China con el 14.7% y en último lugar se encuentra el Reino Unido con el 2%. El resto de los países del mundo representa el 19.7%.

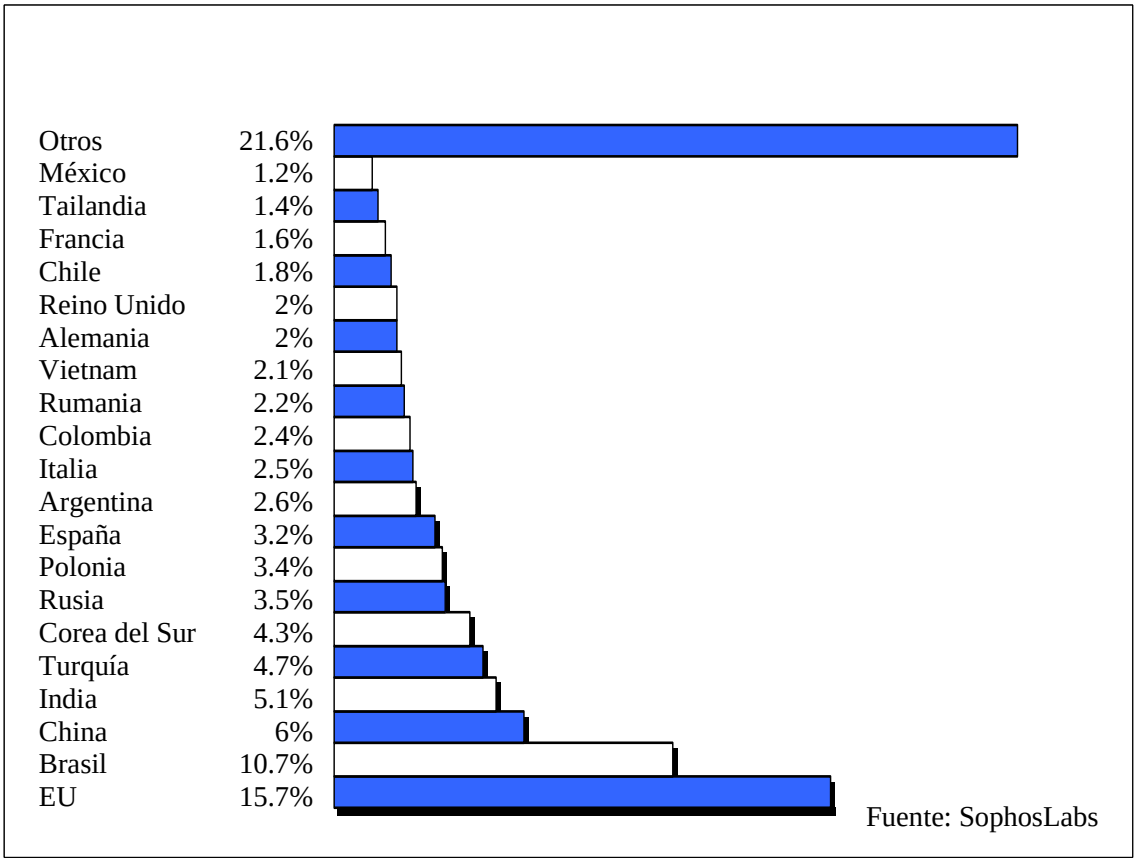


Gráfica 2.12 Países con mayor porcentaje de malware en la web

Prácticamente más de la tercera parte de malware que existe en el mundo, lo padece Estados Unidos, por lo que es necesario prestar mayor atención, incrementar el nivel de seguridad y estar alertas para evitar ser víctimas de cualquier tipo de amenaza.

Reproducción de spam por país

En la gráfica 2.13 se observan los principales países productores de spam, esta lista está conformada por 20 países los cuales representan el 78.4% del total de spam a nivel mundial, el resto representa el 21.6%.

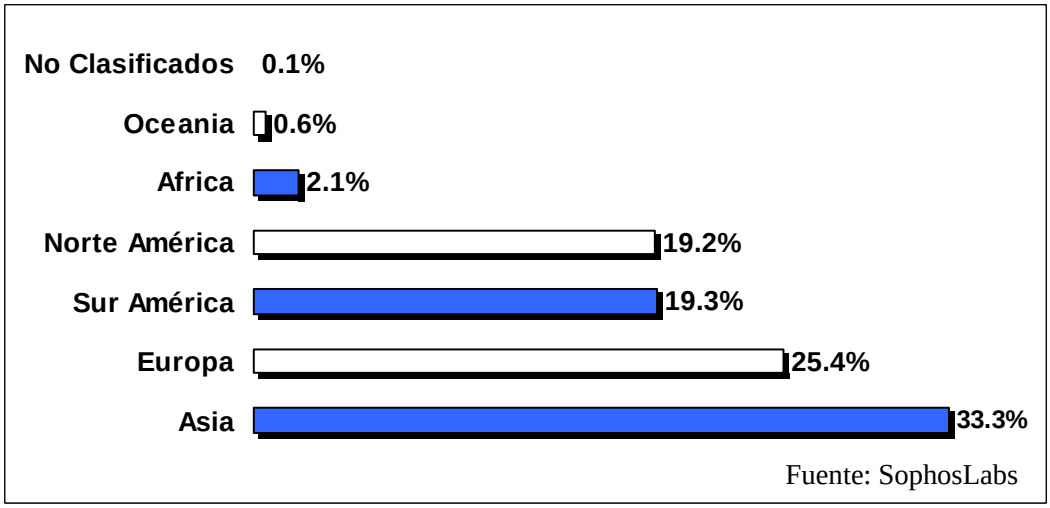


Gráfica 2.13 Reproducción de Spam por país

ShophosLabs señala que Estados Unidos aumentó la cantidad total de spam representando el 15.7% en comparación con el 14.9% en el mismo período del año 2008. Rusia ha caído de su postura anterior en segundo lugar en la tabla (7.5%) hasta el 3.5%. México únicamente representa el 1.2% de spam con respecto a los países en el mundo, por lo tanto se tiene que seguir trabajando para evitar en la medida de lo posible incrementar la reproducción de spam.

Spam por continente

En la gráfica 2.14 se aprecia la cantidad de spam generada por continente en el periodo comprendido de Enero a Junio del año 2009, se puede observar que Asia abarca el 33.3% del total a nivel mundial seguido de Europa. El continente Americano abarca el 19.3% en la parte sur y en la zona norte el 19.2%. Oceanía es el continente que representa tan solo el 0.6% de spam a nivel mundial. Todo se centra en los países desarrollados, derivado del avance de la tecnología.



Gráfica 2.14 Spam por continente

En este informe también se tomaron en cuenta las principales amenazas de seguridad informática que han estado presentes en la primera mitad del 2009, las cuales son:

- **Redes sociales:** Debido al auge que están teniendo estas redes, también se han manifestado sus debilidades, como la falta de privacidad que puede haber si no se configuran adecuadamente, programas maliciosos orientados a estas redes o, como sucede en muchas empresas, pérdida de tiempo por parte de los usuarios y fugas de información.
- **Fuga de información:** Generalmente producida por no tener la información importante cifrada.

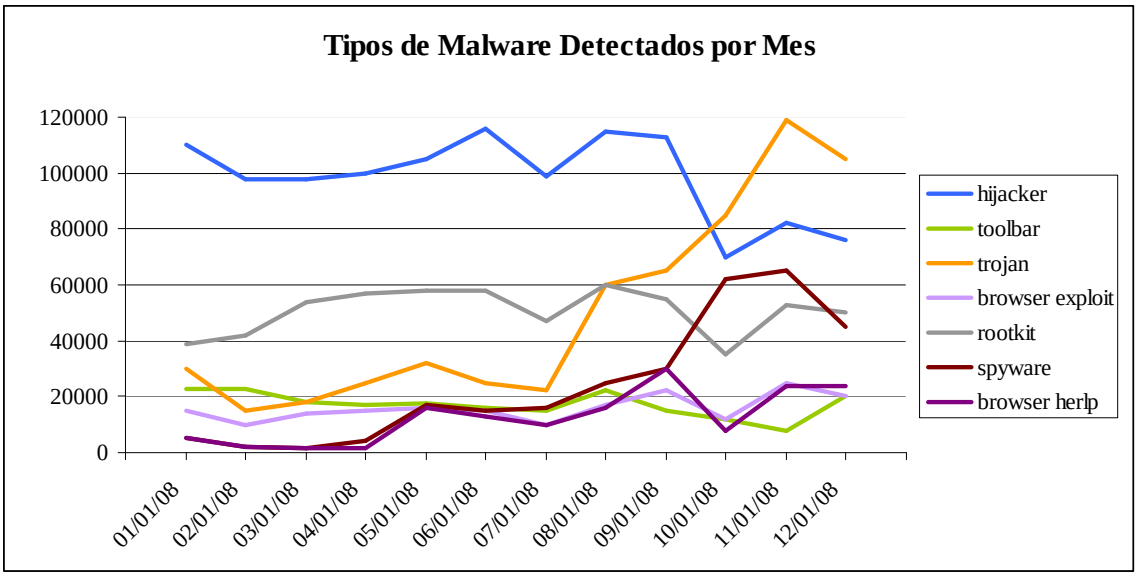
- **Amenazas Web:** Fallos en los navegadores o alguno de sus componentes, enlaces a páginas maliciosas o páginas legítimas que han sido modificadas sin el conocimiento de su creador, son las principales formas de infección.
- **Amenazas de Correo Electrónico:** Los usuarios son vulnerables a quedarse infectados al recibir correos electrónicos que contienen un adjunto malicioso como en correos con enlaces a páginas Web maliciosas.
- **Spam:** Sigue siendo una de las principales molestias a nivel de seguridad informática.
- **Malware:** Este semestre han predominado los falsos antivirus y la infección del gusano Conficker.
- **Apple MACs:** Aunque en menor cantidad que para otras plataformas, este semestre han surgido varios programas maliciosos para MAC.
- **Teléfonos móviles y dispositivos Wi-Fi:** Todas las aplicaciones son susceptibles de ser vulnerables y últimamente se han detectado algunas vulnerabilidades en terminales de gran aceptación entre los usuarios y las empresas como BlackBerry e iPhone.
- **Cibercrimen y delitos informáticos:** Aumenta el ciber espionaje a la par de que en muchos gobiernos empiezan a arrestar a ciberdelincuentes. Como dato positivo cabe destacar que muchos gobiernos se empiezan a preocupar seriamente por la seguridad informática para prevenir y evitar ciber ataques.

Análisis del informe sobre seguridad informática realizado por la empresa CISCO en el año 2008

En este informe se señalan las principales **vulnerabilidades** que tienen los equipos de comunicación, por ello, los ciber-delincuentes se aprovechan de estas debilidades para instalar malware en los dispositivos y así obtener el control de las computadoras y las redes.

En la gráfica 2.15 se muestra el uso del malware, como troyanos, objetos de ayuda del navegador y software espía. Estos datos reflejan una tendencia muy peligrosa en la

recopilación de datos de malware, así como cada vez más sofisticado el ataque de ingeniería social.



Gráfica 2.15 Tipos de Malware detectados por mes

CISCO presentó de manera general las principales **amenazas** producidas en el primer semestre del año 2009 las cuales se describen a continuación:

- **Botnets:** Estas redes de computadoras sirven como un medio para lanzar un ataque. Los propietarios de los botnets están alquilando estas redes a otros criminales, ofreciendo eficaces y sólidos recursos para suministrar spam y malware.
- **Spam:** El spam sigue siendo un vehículo principal a la hora de expandir gusanos y malware, así como de saturar el tráfico de Internet. Cada día se envían 180,000 millones de mensajes de spam, lo que representa un promedio del 90% de todo el tráfico de correo electrónico del mundo.
- **Gusanos:** El aumento de las redes sociales ha facilitado el lanzamiento de gusanos. La gente que entra en estas comunidades de Internet son más propensos a hacer clic en vínculos y descargar contenido que creen que han enviado personas que conocen y en quienes confían.
- **Indexación de spam:** Muchos tipos de empresas utilizan la optimización de motores de búsqueda para aparecer en listas destacadas en búsquedas realizadas en

Google y otros sitios. La táctica, que implica empaquetar un sitio Web con palabras clave o términos de búsqueda relevantes, se utiliza cada vez más entre los ciber-delincuentes que tratan de disfrazar el malware como software legal, puesto que los usuarios tienden a confiar y no sospechan de las clasificaciones en los principales motores de búsqueda por lo que fácilmente podrían descargar uno de los paquetes de software básicos creyendo que es legal.

- **Fraudes de mensajes de texto:** Desde principios del año 2009 han aparecido al menos, dos o tres campañas semanales, cuyo objetivo son los dispositivos móviles de mano. Cisco describe el creciente mercado de los dispositivos móviles como una *"nueva frontera de fraude irresistible para los criminales"*.
- Con casi 4, 100,000 millones de abonados a teléfonos móviles en todo el mundo, un delincuente podría lanzar una red extraordinariamente amplia y obtener un suculento beneficio, incluso si el ataque se produjera sólo sobre una pequeña parte de los usuarios.
- **Insiders:** La recesión global ha provocado que muchos individuos pierdan su trabajo, como resultado de ello ahora las amenazas provienen de personas que tienen acceso a información confidencial (conocidos como *insiders*), por lo tanto son ya una preocupación para las organizaciones. Estas personas que cometen fraude no sólo podrían ser empleados actuales o ex-empleados, sino contratistas o terceras partes.

Estos análisis ayudan a conocer la problemática que se vive a nivel mundial, en la tabla 2.4 se muestra un resumen sobre los análisis realizados por las diversas organizaciones, y se observa que las principales amenazas a las que se enfrentan los países en el mundo son los escaneos, spam, malware, phishing y bots, lo que ha ocasionado grandes problemas a las empresas e incluso en menor grado a usuarios domésticos derivado del desconocimiento sobre la importancia de mantener protegida la información que manejan.

Tabla 2.4 Resumen de los informes analizados por las diferentes empresas

Año	Organización	País	Tipo de Amenaza	%
2007	UNAM-CERT	México	Escaneos	35.40
			Bot	32.16
2008	UNAM-CERT	México	Spam	60.56
			Beagle	23.28
	Cisco	Todos	Spam	90
2009	McAfee	Todos	Spam	88
		Estados Unidos	Phishing	43
			Spam	25.5
			Zombis	15.7
		Todos	Malware	60
		Brasil	Spam	9.8
		China	Phishing	8
	PandaLabs	Taiwan	Malware	34
		México	Malware	18
	Sophos	Estados Unidos	Malware	39.6
			Spam	25.7
		Brasil	Spam	10.7
		China	Malware	14.7
			Spam	6
2010	UNAM-CERT	México	Bot	35.5
			Spam	23.26

Los resultados presentados por las diversas empresas en materia de seguridad informática colocan a Estados Unidos en el primer lugar con los mayores índices registrados de spam, malware, y phishing principalmente; le siguen Brasil, China, Taiwán, entre otros y en último lugar se encuentran los países con los menores registros de estas amenazas, entre los que se encuentran Rumanía, República Checa, Francia, Italia, México, y Tailandia.

Por lo tanto, para el caso particular de México, los registros presentados indican que está por debajo de los principales países. Esto se debe a muchos factores, como por ejemplo; el tipo de economía, la tecnología que se emplea, el nivel de conocimiento que existe en los usuarios, la educación, entre otros.

Conforme México crece en tecnología, será más vulnerable a sufrir ataques de cualquier índole provenientes de cualquier parte del mundo. Por ese motivo surgió la necesidad de contar con instituciones en materia de seguridad informática las cuales se encargan de mantenerse al día sobre las nuevas amenazas, encontrando soluciones para mitigarlas y así ofrecer un buen sistema de seguridad enfocado a las necesidades de cada empresa o usuario.

Es importante que las empresas inviertan en nuevas metodologías de seguridad para combatir la problemática que se vive en el mundo ya que nadie está exento de sufrir algún ataque y padecer daños que en la mayoría de los casos resultan ser muy costosos.

Por ello, se hace hincapié en que las organizaciones realicen periódicamente un análisis de riesgos para determinar las posibles amenazas y vulnerabilidades a las que se enfrentan, realizando planes de contingencia en los diversos sistemas de seguridad con los que cuenta cada organización. Una vez conocidos los problemas a los que se enfrentan las empresas en el mundo, es recomendable hacer conciencia y proporcionar una adecuada solución a éstos.
Desafortunadamente como se ha mencionado a lo largo de este capítulo, las amenazas y vulnerabilidades van siendo más sofisticadas y difíciles de detectar, se puede decir que existe ahora una guerra cibernética entre aquellos individuos que buscan la manera de llevar a cabo con éxito un ataque de cualquier índole, contra los que se protegen de éstos.