

Los peligros que acechan en Internet

¿Qué es lo que puede infectar a un ordenador? (I)

Junto a los obvios beneficios de Internet, existen también ciertos riesgos que amenazan el bienestar de millones de usuarios de ordenadores.

Detallaremos aquí los riesgos más críticos asociados con la conexión en línea y propondremos ciertos pasos para poder controlar estas amenazas.

Debido al tamaño de la información a presentar, el documento es dividido en dos partes, mostrándose aquí la primera.

Amenaza Nº 1: Ataque externo

Este es uno de los peligros más comunes. La conexión a Internet permite el acceso del usuario a cualquier otra dirección de Internet alrededor del mundo, pero también le permite a cualquier persona acceder al sistema de este usuario.

Mientras la mayoría de los usuarios domésticos creen que no hay razón para ser atacados, en la práctica la mayoría de los ataques son exploraciones automáticas (donde un individuo malicioso explora una cantidad de direcciones en busca de sistemas con una vulnerabilidad específica) o pueden ser el resultado del accionar de un programa malicioso (principalmente gusanos, programas que buscan propagarse de sistema a sistema).

Aunque sigue siendo verdad que los negocios son objetivos más atractivos para los atacantes habilidosos, los sistemas de los usuarios domésticos si son secuestrados, pueden ser utilizados para una variedad de propósitos, incluyendo:

- *Envío de publicidad no deseada*
Corresponde al denominado *Spam* o correo basura.
- *Lanzar ataques a los sitios Web*
Generalmente se utiliza como una forma de chantaje a los dueños de los sitios Web atacados, buscando algún tipo de rédito.
- *Retransmitir información*
Normalmente se utiliza esta vía para ocultar la verdadera ubicación del sitio Web, especialmente si el objetivo es alojar contenido ilegal como pornografía infantil.
- *Alojar contenido ilegal directamente.*

Para tomar control de un sistema, el atacante necesita que el sistema ejecute un programa de su elección, siendo (lo más probable que sea por medio del aprovechamiento de una vulnerabilidad de Windows o de cualquier otro programa que utilice una conexión a Internet.

Si resulta exitoso, este programa permanecerá activo en segundo plano y aceptará las ordenes del atacante informándole sobre su estado.

No solo estos ataques han crecido notablemente en cuanto a su frecuencia, de acuerdo a Dshield.org (un sitio Web que recolecta información sobre ataques) sino que un sistema sin protección se verá comprometido aproximadamente a los 17 minutos de estar conectado a Internet, y también los programas utilizados para atacar han crecido en sofisticación, volviéndose mucho mas difícil detectarlos o quitarlos.

Otro tipo de ataque externo es el ataque de **Denegación de Servicio** (DoS, *Denial of Service*): el objetivo aquí no es controlar un sistema sino desactivarlo.

Esto puede ser ocasionado ya sea por medio del envío de información de red diseñada para causar el colapso de un sistema (por ejemplo, incluyendo parámetros ilegales) o por medio del envío de gran cantidad de información, saturando la conexión a Internet del usuario.

Un cortafuegos detectará y desechará cualquier información no solicitada (que no fuera enviada en respuesta a un pedido hecho por el ordenador del usuario) así como bloqueará todas las sondeos.

Sin embargo si el usuario ejecuta programas que necesitan aceptar conexiones entrantes (tales como los programas para compartir archivos, cualquier servidor, y voz sobre IP [VoIP] / video conferencias), será necesario configurar el cortafuegos para que permita esto.

En tales casos, se debe tener sumo cuidado y restringir el tráfico tanto como sea posible para reducir la posibilidad de irrupción de un ataque. Los cortafuegos más recientes también pueden detectar (y bloquear) ataques DoS.

Sin embargo, solo el proveedor de servicio de Internet (ISP) puede evitar que una línea sea saturada por exceso de información.

Si existe una red local (ya sea inalámbrica o no) entonces esto puede ocasionar otro método de ataque, el cual permite traspasar los cortafuegos físicos (como aquellos incluidos en muchos enrutadores de Internet).

Por eso es importante asegurarnos que todos los ordenadores en una red local estén protegidos y que las redes inalámbricas en particular sean seguras ante los accesos sin autorización.

Para evitar sondeos o ataques externos en el ordenador, el usuario debe seguir los siguientes pasos:

- Instalar un cortafuegos (ya sea uno físico o una aplicación cortafuegos) y asegurarse que esté configurado apropiadamente:
Debe considerarse la opción de utilizar un sitio de análisis como "Shield Up!" en <https://grc.com/x/ne.dll?bh0bkyd2> para examinar la visibilidad del ordenador en línea.
- Aplicar todas las actualizaciones de seguridad para Windows y cualquier otro programa que se utilice.
- Si el usuario tiene una red local inalámbrica, debe activar la codificación WEP (*Wired Equivalent Privacy*, Privacidad equivalente a las redes cableadas) para evitar que los intrusos la utilicen para acceder a la conexión de Internet del usuario o atacar al ordenador.
Mientras que la codificación WEP no es completamente segura, la versión 128-bit obligará a un atacante a pasar más tiempo en el radio de acción de una conexión inalámbrica antes de poder entrar a la red del usuario.
- Si el usuario tiene una red local de cualquier tipo, debe considerarse la opción de instalar un programa cortafuegos (como *Outpost Firewall*) en cada sistema para que en el caso que uno de los sistemas fuese secuestrado, este no podrá ser utilizado para controlar los otros ordenadores.

Amenaza Nº 2: Virus, gusanos o infecciones de programas espía

Este problema también ha escalado enormemente en los últimos dos años y puede dividirse en varias categorías:

- **Publicidad no deseada**
(*Adware*)
Cualquier programa que muestra publicidad.
Además de ser irritante, la publicidad no deseada puede reducir la velocidad de un sistema o causar conflictos con otros programas.
Ejemplos: *Gator*, *WhenU*.
- **Secuestrador del explorador**
(*Browser hijacker*)
Este altera las configuraciones del explorador (agregando una barra de herramientas extra, o cambiando la página de inicio y la página de búsqueda en Internet Explorer) generalmente para redirigir a los usuarios a los motores de búsqueda "Pulse y pague" (*Pay-per-Click*) o sitios Web específicos.
Puede también modificar los Favoritos/Marcadores para agregar sitios extras, generalmente relacionados con la pornografía.
Ejemplos: *CoolWebSearch*, *ISTBar*.
- **Programa espía**
(*Spyware*)
Recolecta información personal o privada ya sea de forma abierta o furtivamente.
Puede incluir sitios Web visitados, programas utilizados, detalles de los correos electrónicos y otros mensajes y hasta (en los peores casos) contraseñas y detalles de tarjetas de crédito.
Ejemplo: *MarketScore*.
- **Discadores**
(*Dialer*)
Utiliza el módem para comunicarse con un número de teléfono con coste adicional.
Esto solía ser común con los sitios de pornografía como un método alternativo de cobrarles a los visitantes (dónde el número de teléfono sólo podía ser utilizado por un corto período mientras se descargaba contenido) pero algunos discadores causaron que todos los posteriores accesos a Internet fueran con tarifa adicional.
Este tipo de programa no afecta a los usuarios con otro tipo de conexión (DSL, por satélite, cable, entre otros)
Ejemplos: *Haldex*, *SiteCon*.

- **Gusanos y Virus**

Programas que se propagan de ordenador a ordenador y que incluyen una carga que a su vez puede incluir una o más de las categorías antes mencionadas.

Pueden destruir o alterar información.

Ejemplos: *MyTob, Netsky, Zafi*.

- **Trojanos**

Programas maliciosos ocultos dentro de aplicaciones que aparecen como útiles.

A menudo son utilizados para controlar otros sistemas (trojanos de acceso remoto) pero también pueden incluir un capturador de pulsaciones del teclado (*Keylogger*) que permite controlar las teclas presionadas para capturar contraseñas y detalles de tarjetas de crédito).

Ejemplos: *Optix, Bionet, Formglieder*.

- **Rootkit**

Programa que se oculta a sí mismo y a otros códigos maliciosos asociados (alguna de las categorías mencionadas anteriormente) por medio de la modificación de las funciones del Kernel de Windows.

Esto hace de la detección y eliminación de los mismos una tarea mucho más difícil y puede exigir darle formato al disco duro y reinstalar Windows.

Ejemplos: *HackerDefender, FU*.

Las formas más probables de ser infectado por una de las categorías antes mencionadas son:

- Visitando un sitio Web que utilice las vulnerabilidades del navegador (en mayor medida al utilizar Internet Explorer) para descargar programas maliciosos.
Técnica conocida como "descargas automáticas" o *drive-by downloads*.
- Descargando y ejecutando un programa que parece inofensivo (un protector de pantalla, juegos, o programas de utilidades) pero el cual también contiene programas maliciosos.
La publicidad no deseada (*Adware*) siempre se menciona en el Acuerdo de licencia del usuario final y por eso se recomienda verificar cuidadosamente antes de permitir que el programa se instale (o utilizar programas como [EULAlyzer](#) para verificarlos).
- Recibiendo y abriendo un archivo infectado en un fichero adjunto de correo.

Para reducir el riesgo y las infecciones de programas maliciosos:

- Nunca deben ejecutarse los archivos que el usuario considere no confiables o cuya fuente no pueden ser verificada (redes para compartir archivos, Usenet y las descargas en IRC son especialmente peligrosas).
- Desactivar ActiveX, Java y Javascript del navegador de Internet (Internet Explorer, Mozilla, Opera) o utilizar una herramienta predefinida hecha por terceros (como el filtro de Contenido activo de Outpost Firewall) y solamente habilitarlos para los sitios de confianza.
- Utilizar Opera o Firefox para explorar la Web en lugar de Internet Explorer.
Además de mejorar la seguridad, estos navegadores ofrecen muchas mejoras en lo referido a la practicidad (explorador por pestañas, funciones del ratón, acceso rápido al motor de búsqueda) y los dos son gratuitos.
- Instalar un antivirus y siempre mantenerlo actualizado con la mayor frecuencia que sea posible.
Un antivirus que tenga un sistema avanzado de detección heurística es aconsejable.
- Si el usuario recibe un archivo por correo electrónico, siempre debe analizarlo con un programa antivirus, aún si proviene de fuentes conocidas (amigos, familia, colegas) es posible que esa dirección sea burlada, o que se comprometan los sistemas.
- Es necesario ser muy cuidadoso cuando se visitan sitios Web mencionados en los correos no solicitados (*Spam*).
Muchos tratan de descargarse automáticamente como una forma de propagar códigos maliciosos que benefician al que envía este tipo de mensajes (ya sea dándole control sobre miles de ordenadores o propagando publicidad no deseada, con las cuales puede obtener algún tipo de ventaja o beneficio) y algunos pueden utilizar *exploits* (utilización de vulnerabilidades) que todavía no fueron detectados por los programas antivirus.

Aquí concluye la primera parte, en la siguiente edición trataremos sobre más amenazas.