MALWARE

ÍNDICE.

MALWARE

Introducción.

Aunque normalmente hablamos de virus informáticos, este término únicamente hace referencia a uno de los muchos tipos existentes de ataque mediante software a los sistemas informáticos. El término más genérico sería **MALWARE** (acrónimo de software malicioso en inglés: ***mal****icious soft****ware***).

Os sonarán diversos términos que podemos incluir en este concepto: virus, troyanos, gusanos, espías, software publicitario, etc. No me enrollaré aquí haciendo referencia a cada uno (para eso ya tenemos la Wikipedia), pero hemos de saber que entre estos virus los hay desde los que únicamente nos muestran una ventana de publicidad hasta los que capturan nuestros datos privados para uso fraudulento, pasando por los que pueden destruir nuestro sistema (nuestro sistema lógico, destruir físicamente la máquina sería mucho más complicado y además no tiene interés para los atacantes).

Si os interesa el tema, en la entrada de la Wikipedia sobre **MALWARE** tenéis información abundante.

Lo que pretendo con este artículo, es únicamente daros algunas pistas, que considero efectivas, para prevenir ataques de este tipo. Si aún así no conseguimos evitar la infección también veremos algunas posibles soluciones.

Lo primero que tenemos que hacer es **no quitarle importancia al tema**. Si se nos rompe el sistema, siempre podemos formatear el disco y listo. El mayor perjuicio de esta medida es la posible pérdida de datos, pero peor sería si mediante un software malicioso consiguen averiguar nuestros datos personales y con ellos vaciarnos la cuenta bancaria.

A pesar de esto, mi segundo consejo es **perderle el miedo a los virus**. Con unas pocas medidas de seguridad, podemos conseguir que la intrusión en nuestro pc sea mucho mas complicada.

Medidas preventivas.

Las principales medidas preventivas no pasan por gastarse un dineral en antivirus o por proteger el ordenador hasta el punto de que no podamos hacer operaciones habituales, como navegar por Internet con una cierta soltura. Las principales medidas hacen referencia al sentido común.

En primer lugar recomendaré una web en la que la información sobre este tema es abundante y de calidad:

http://www.alerta-antivirus.es

En este sitio web encontrarás recursos e información de gran utilidad del "Centro de Alerta Temprana sobre Virus y Seguridad Informática". Este Centro pertenece a la Sociedad Estatal "INTECO" promovido por el Ministerio de Industria Español. Desde mi punto de vista la información que da el INTECO a veces puede ser algo alarmante, pero, sin asustarse, es muy interesante ojear esta web. En particular te recomiendo el siguiente documento sobre consejos de seguridad:

http://alerta-antivirus.inteco.es/seguridad/ConsejosSeguridad-INTECO.pdf

(por si te falla este vínculo o lo cambian, tienes una versión guardada en mi web a la fecha de redacción de este documento. Haz clic en este texto para descargarla
http://www.teoweb.es/tecnolog/ConsejosSeguridad-INTECO.pdf
Fichero en formato pdf – 80 KB)

Hace referencia, entre otras, a las medidas de sentido común a las que me refería antes.

Para empezar, hablaremos de utilizar el menos común de los sentidos:

¿Que harías si recibes un e-mail con las siguientes caraterísticas?

> Remitente: **Vanessa "CUERPO PERFECTO"**
> Asunto: **La solución definitiva a todos tus problemas**
> Texto: **Tengo la solución definitiva a tu problema de obesidad. Haz clic en el siguiente vínculo y te mostraré cómo perder 25 kilos de peso en 15 minutos.**

¿De verdad harías clic en ese vínculo? Pero si ni siquiera eres obeso. ¡Ah pillín, te han picado la curiosidad con lo de Vanessa "CUERPO PERFECTO"!

Esto tal vez sea exagerado, pero así entran la mayoría de los virus.

Medidas de sentido común:

- No abras correos de desconocidos.
- No descargues ficheros sospechosos o que no te inspiren confianza, aunque sean ficheros adjuntos a correos de personas conocidas.

- Si los descargas, revísalos con el antivirus antes de abrirlos.
- Es más seguro utilizar el correo web que un cliente de correo instalado en local.
- Si necesitas descargar software, hazlo desde la página oficial del fabricante.
- Utiliza software legal. No es necesario que sea de pago, hay software gratuito con una calidad inmejorable y para cubrir cualquier necesidad.
- Tu banco nunca te va a pedir a través del correo electrónico datos personales.
- Protege tus datos personales. No los facilites alegremente.
- Cambia con frecuencia tus contraseñas y que éstas sean lo más complicadas posible.
- Ten cuidado con el software shareware, a veces se les va la mano con la publicidad hasta que lo has pagado.
- Gran parte del malware utiliza agujeros de seguridad de tu sistema operativo. Mantén actualizado tu sistema operativo y todo tu software, especialmente con los parches de seguridad.
- Windows es el más vulnerable, pero esto no quiere decir que MAC o Linux no lo sean. Son más seguros pero también pueden ser atacados.
- No utilices PC's públicos, como los de los cibercafés, para operaciones comerciales o delicadas.
- Si utilizas un pc público o compartido, ten la precaución de borrar el historial, las cookies y los archivos temporales cuando termines y no olvides cerrar la sesión del navegador.
- Evita, si es posible, las descargas P2P.
- Linux mejor que Windows.
- Haz copias de seguridad periódicas de tus discos o al menos de tus datos.
- Etc.

En resumen, emplea la cabeza. Ya se que todos estamos muy atareados, pero hacer las cosas con prisa y sin pensarlas es muy arriesgado en este tema. Por ejemplo, cuando teclees una dirección en tu navegador, no es lo mismo:

http://www.cajamadrid.es

que

http://www.cajamdrid.es

así que teclea con cuidado (no te aconsejo que pruebes el ejemplo anterior).

No es mi caso, pero tengo algunos amigos que nunca han utilizado ningún tipo de antivirus o nada parecido. Simplemente han empleado el sentido común y nunca han tenido un virus en su ordenador. Esto tal vez sea un poco temerario, pero es indicativo de hasta qué punto es importante tener un poco de cuidado.

Si Todo esto te ha quedado claro, ya hemos recorrido más de la mitad del camino. Ahora veremos como protegernos con antivirus y otros programas de protección.

Software preventivo.

ANTIVIRUS:

Empezaremos por el antivirus.
Mi primer consejo es que **NO TE GASTES NI UN EURO EN ANTIVIRUS**, salvo que estemos hablando de una empresa, en la que la asistencia técnica del fabricante del antivirus puede ser importante.

Mentalízate de una cosa, ningún antivirus es capaz de limpiar todos los virus existentes. Conformate con tener uno que sea capaz, al menos, de detectar la mayoría de ellos a tiempo para evitar la infección. Y te aseguro que este problema no lo resuelves pagando una cifra astronómica por un antivirus.

Lo más importante a tener en cuenta es que el antivirus se actualice fácilmente para que sea capaz de detectar hasta las amenazas más recientes. Otro aspecto importante es que no sature demasiado el sistema. Algún antivirus de pago muy famoso, y en honor a la verdad bastante efectivo, tiene el problema de que te deja el ordenador tostado, se come todos los recursos. Esto es muy importante, pues normalmente en casa no disponemos del ordenador más potente del mundo.

Para tu ordenador personal, de uso doméstico, insisto **NO TE GASTES NI UN EURO EN ANTIVIRUS**. Existen en el mercado antivirus gratuitos con la misma calidad o incluso superior a los de pago. Normalmente son empresas que tienen una versión de pago para actividades comerciales y otra gratuita para uso doméstico o sin ánimo de lucro. La versión gratuita, si es buena, les da prestigio y les ayuda a vender la de pago, por tanto es tan fiable la una como la otra.

Hay muchos gratuitos en el mercado. Yo te recomiendo uno, no porque sea mejor, sino porque lo conozco más que a otros, porque está en castellano y porque los amigos a los que se lo he recomendado están encantados.

Se trata del **AVAST**. El fabricante es Alwil Software y puedes descargarte el paquete de instalación de su antivirus gratuito desde su página web en:

http://www.avast.com/esp/download-avast-home.html

Al pie de la página de descarga tienes la posibilidad de bajarte el fichero de instalación eligiendo el idioma deseado.

Antes de ejecutar el programa de instalación asegúrate de que no tienes ningún otro antivirus instalado. Normalmente cuando en un mismo pc se instalan varios antivirus, éstos suelen colisionar y dar problemas.

Una vez instalado, tienes 60 días para evaluarlo. Pasado ese tiempo, lo único que te piden a cambio del uso de su software es que te registres en su web facilitando únicamente un nombre y una dirección de e-mail. Una vez que lo has hecho, te

enviarán por e-mail un número de serie que te dará derecho al uso del antivirus durante un año.

Comprobarás que este antivirus se actualiza con mucha frecuencia (incluso varias veces al día) y él solito, sin necesidad de que tengas que hacer nada para actualizarlo (lógicamente tendremos que tener activa la conexión a Internet). Cuando falte poco para que venza el año de licencia, te avisará y te dará la opción de renovar por otro periodo de un año. Además apenas notarás que está vigilando tu sistema pues consume muy pocos recursos. Funciona con todas las versiones de Windows.

Si localiza algún virus nos avisará con una ventana en pantalla y con una llamativa señal acústica. Una vez detectado el virus y si no es capaz de eliminarlo, lo aislará en una zona segura a la que denomina “Baúl de virus” a la espera de poder eliminarlo posteriormente con próximas actualizaciones. Para analizar manualmente un archivo, carpeta o unidad de disco, bastará con abrir el menú contextual con el botón derecho del ratón sobre ése objeto y elegir la opción de “Escanear”.

ANTI-SPYWARE:

Casi con un buen antivirus sería suficiente, no obstante muchos aconsejan la utilización de un anti-espías para mejorar la seguridad.

Yo os recomendaré uno que, igual que decíamos con el antivirus, no tiene por qué ser el mejor, pero lo conozco y me consta que es muy efectivo. Es gratuito y fácil de utilizar aunque no está totalmente traducido al castellano.

Se trata de **Spybot Search & Destroy.** El paquete de instalación se puede descargar de:

http://www.spybot.info/es/spybotsd/index.html

Una vez instalado se puede dejar residente en memoria con lo que nos avisará cada vez que un programa intente modificar el registro de Windows, pidiéndonos confirmación de cada una de las modificaciones en el registro.

No actúa como un antivirus que se mantiene alerta revisando el sistema constantemente. En este caso hay que ejecutarlo periódicamente y comprobar si existen actualizaciones con la opción correspondiente (buscar actualizaciones) para lo que necesitaremos que esté activa la conexión a Internet. Una vez actualizado podremos analizar el sistema con la opción Search & Destroy y finalizado el análisis nos mostrará todo el malware encontrado dándonos la opción de repararlo y a continuación de inmunizar el sistema para evitar nuevas infecciones. Es recomendable inmunizar el sistema aun cuando no se haya encontrado ningún malware en la revisión.

Tiene el inconveniente de que hemos de habituarnos a revisar manualmente el sistema periódicamente, pero es muy efectivo y no consume recursos. El proceso de

análisis de sistema es largo y se alarga más si al mismo tiempo seguimos trabajando con el pc, por lo que es conveniente lanzar este proceso en un momento en que no tengamos otra cosa que hacer y dejarlo trabajar.

CORTAFUEGOS:

Con lo que hemos visto hasta ahora, es más que suficiente para tener una protección adecuada. No obstante si te preocupa mucho el tema y quieres seguir todos los consejos de los más ortodoxos, te puedes plantear la opción de instalar un cortafuegos.

Estos programas controlan las conexiones tanto de salida como de entrada de un ordenador. Generalmente son programas difíciles de configurar adecuadamente. Si nos pasamos en el nivel de seguridad es probable que evitemos, sin quererlo, comunicaciones que no quisiéramos restringir y si nos quedamos cortos reducimos considerablemente su efectividad.

Si disponemos de Windows XP o Windows Vista estos sistemas operativos ya tienen su propio cortafuegos, que está activado por defecto y con una configuración bastante equilibrada.

No creo necesario abundar más en este tema, pues como he dicho considero suficiente, al menos para uso doméstico, la protección que aportan el antivirus y el antispy.

Cuanto todo ha fallado.

Si sigues los consejos que hemos dado en los relativo a las medidas de prudencia y sentido común y tienes al menos un buen antivirus instalado, es muy difícil que todo falle y que te encuentres con una situación irreparable.

No obstante no es imposible y cabe la posibilidad de que un día te encuentres un virus en tu pc. Incluso es posible que el antivirus no pueda con él y en el peor de los casos que ni siquiera sea posible arrancar el pc.

En este último caso lo mejor y más barato es que no te compliques la vida. Si has seguido el consejo de hacer copias periódicas de seguridad, no pierdas tiempo y formatea el disco duro, luego recuperas la copia de tus datos, reinstalas el software y listo. Como mucho en un día de trabajo tienes otra vez el sistema como nuevo. Si no te sientes capaz de hacer esto, tal vez tendrás que recurrir a un profesional y o un amigo generoso que te ayude a hacerlo, o a recuperar los datos que puedan salvarse del disco infectado, si no hiciste copia de seguridad.

Pero lo normal será, como mucho, que el antivirus detecte un virus y no pueda eliminarlo. Puede ocurrir también que ni siquiera lo detecte, pero tu notes que el ordenador no funciona como debiera y sospeches que tal vez un virus no detectado esté incordiando más de lo debido. Asegurate de esto haciendo una segunda revisión con otro antivirus (pueden servirte los que hacen análisis gratuitos on-line sin necesidad de instalarlo). Una vez confirmada la existencia de virus y que este no puede ser eliminado con un antivirus, tendrás que realizar la desinfección de forma manual. Para ello te cuento como suelo hacerlo yo en estos casos.

- Primero identifica el virus. Para ello tendrás que ver en el antivirus el nombre, lo más exacto posible, del virus detectado
- Segundo. Entra en http://www.alerta-antivirus.es y en el buscador que hay en la cabecera de la página teclea el nombre del virus. Te mostrará una lista de los virus que coinciden con la búsqueda. Una vez identificado el tuyo encontrarás información suficiente para, paso a paso, eliminar el virus de tu sistema.

Enlaces recomendados (y otros documentos).

- http://es.wikipedia.org/wiki/Malware (información en la Wikipedia sobre el malware)
- http://www.alerta-antivirus.es (Centro de Alerta Temprana sobre Virus y Seguridad Informática". Ministerio de Industria Español)
- http://alerta-antivirus.inteco.es/seguridad/ConsejosSeguridad-INTECO.pdf (Consejos sobre seguridad informática)
- http://alerta-antivirus.inteco.es/utiles/ver.php?tema=U (Recopilación de herramientas gratuitas de protección informática)
- https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/index-ides-idphp.php (Publicaciones sobre la protección de datos personales de la Agencia Española de protección de datos)
- http://www.avast.com/index_esp.html (Página web de Alwil Software, fabricante de AVAST antivirus)
- http://www.avast.com/esp/download-avast-home.html (Página de descarga de AVAST)
- http://www.spybot.info/es/index.html (Página del fabricante de Spybot Search & Destroy)
- http://www.spybot.info/es/spybotsd/index.html (Página de descarga de Spybot Search & Destroy)

Para terminar.

Yo creo que los que se dedican a diseñar los virus y Microsoft tienen mucho en común:

- Los dos fabrican software.
- Los dos consiguen que nuestros ordenadores no funcionen como deberían, haciendo que dediquemos mas tiempo a repararlos, protegerlos, configurarlos, actualizarlos, hacer copias de seguridad, etc... que a utilizarlos normalmente.

Para finalizar, el último consejo: El ordenador está a nuestro servicio y no al revés. Es una maquina que debería estar diseñada para facilitarnos la vida, no para complicárnosla. Tu tiempo es muy valioso y no merece la pena dedicar al PC ni un minuto que no sea para obtener de él la prestación esperada. Ten esto presente y baraja siempre si merece la pena dedicarle un tiempo que puede ser mucho más interesante dedicárselo a los amigos o a lo que te salga de ahí mismo. Si las cosas se complican seguramente es preferible buscar un buen profesional y pagarle para que te arregle el desaguisado, antes que acabar de los nervios después de dedicar varios días a intentar arreglar el problema, y terminar con la sensación de que has perdido un tiempo precioso para finalmente no conseguir nada.

Teo (octubre 2008)

http://www.teoweb.es

info@teoweb.es