Cómo eliminar malware del PC

Si tu equipo informático va más lento de lo normal; el sistema operativo muestra errores aleatorios; el navegador web se congela luchando para deshacerse de anuncios extraños o no puedes acceder a tus documentos, es probable que padezcas una infección digital que además de impedir el uso habitual del equipo **pone en riesgo tus datos, archivos y quizá algo más**, incluidas contraseñas y acceso a banca digital.

Y es que virus, gusanos, troyanos y demás especímenes maliciosos acechan a computadoras y redes informáticas. La introducción de malware de todo tipo y para todas las plataformas, el robo de datos, el ciberespionaje, la invasión a la privacidad o las campañas de desinformación que terminan suponiendo un riesgo en línea, cotizan al alza en la tecnología mundial y obligan a usuarios y empresas a tomar medidas pro-activas para su control.

Los grandes incidentes en ciberseguridad ponen de relieve que las amenazas digitales son cada vez más peligrosas, en número y en sofisticación de sus desarrollos. Y la situación no va a mejorar a medida que la industria sigue sumando miles de millones de equipos conectados y que fenómenos como el BYOD y el trabajo híbrido que ha llegado para quedarse tras la pandemia aumentan el número de dispositivos vulnerables.

Cómo eliminar malware del PC

Aunque **la prevención es la primera y principal línea de defensa**, no siempre es posible mantenerse a salvo de la infección y cualquier usuario habrá tenido problemas con el malware en alguna ocasión, incluso aunque no haya sido alertado por su solución de seguridad. Si tu ordenador personal tiene alguno de los síntomas toca ponerse en acción de inmediato con cuatro pasos concretos como los que te vamos a describir.

1. Intenta salvar archivos

Las copias de seguridad son el mayor "salvavidas" para contrarrestar cualquier tipo de virus informático y en ocasiones con algunos de ellos, como el Ransomware, son la única solución. Si no la habías realizado previamente, puedes intentar salvar documentos, fotos, vídeos y cualquier otro tipo de información personal o profesional que no puedas perder incluso aunque estén infectados, **para intentar recuperarlos después en un sistema limpio**.

Se incluyen en este grupo los más peliagudos que serán los infectados por los mencionados Ransomware (con archivos cifrados habitualmente), para poder recuperarlos cuando se publiquen herramientas para su descifrado. Por supuesto, el objetivo es solo copiar los archivos a una unidad externa controlada, ya que **no debemos ejecutar ninguno de estos archivos hasta su limpieza** porque pueden infectarnos otros equipos.

Para realizar estas copias podemos usar varios métodos. Si usas Windows, tiene un modo seguro, también llamado “a prueba de errores” o “arranque avanzado”, que solo carga controladores y servicios más básicos y es de **utilidad para encontrar y resolver problemas del sistema operativo** que no son posibles de solucionar en un arranque estándar donde suele cargarse el código malicioso.

Si no es posible realizar las copias de seguridad con la función anterior, debemos utilizar **otro método más avanzado** para acceder a los archivos de un equipo infectado, como es usar discos de rescate (auto arrancables desde unidades ópticas, pendrives o discos externos USB) tanto los nativos de Windows para recuperación del sistema, como soluciones especialmente preparadas especialmente para resolución de problemas como Hiren’s BootCD o Ultimate Boot CD.

2. Desinfecta el equipo

Una vez que hayamos intentado poner a salvo nuestros archivos esenciales es la hora de comenzar la desinfección, si bien conviene indicar que no siempre es posible dependiendo del malware en cuestión. Hay ocasiones en las que no quedará más remedio que realizar una instalación limpia del todo el sistema y las aplicaciones.

En casos de sospecha, la mejor opción para eliminar malware del PC es usar discos de rescate especializados contra virus. Un medio efectivo teniendo en cuenta que una gran mayoría de malware se **carga/oculta en la memoria** complicando su detección/eliminación una vez que arranca el sistema operativo.

Todos los grandes proveedores de seguridad ofrecen la posibilidad de crearlos y en este artículo tienes una decena de ellos. La mayoría son Linux en formato “Live CD” (creados y auto arrancables desde unidades ópticas, pendrives o discos externos USB), que podemos utilizar en el PC

independientemente del sistema y sin tener que instalar nada en él.

Su funcionamiento es sencillo, no sin antes arrancar el equipo con el medio de rescate creado. Todos actualizarán la firma de virus y el programa, comenzando a continuación el escaneo y la desinfección del malware en su caso. Desde el explorador de archivos del Live CD también podremos acceder a la unidad donde está instalado el sistema principal. Útil si queremos borrar algún archivo o directamente para hacer las copias de seguridad que vimos en el apartado anterior de los archivos esenciales.

3. Recupera el sistema

Si la limpieza del malware fue efectiva, retira el disco de rescate e **intenta arrancar el equipo de la forma habitual**. Si es posible, instala la mejor solución de seguridad que tengas disponible y revísalo de nuevo en la búsqueda de virus. Aquí también hay una buena colección de soluciones gratuitas o comerciales muy completas. Si el sistema arranca normalmente hay que comprobar si todas las aplicaciones que teníamos instaladas funcionan correctamente. También controladores y drivers. Incluso si el sistema operativo está limpio y funcionando, puede ser que existan daños.

Si a pesar de los esfuerzos anteriores no hemos sido capaces de acabar con la infección, **solo nos queda la reinstalación del sistema operativo**. Si tenemos una partición de recuperación o discos del sistema como los que ofrecen algunos fabricantes en sus equipos nuevos, será lo primero a utilizar para revertir el equipo a su estado de fábrica.

Restablecer el sistema operativo a una configuración de fábrica utilizando la misma herramienta del sistema operativo o usar puntos de restauración son otra alternativas sencilla al uso de copias de seguridad o a una instalación desde cero. Si no funciona nada de los anterior, toca realizar una

instalación limpia de todo el sistema, formateando la partición para asegurarse de la eliminación de virus en el equipo.

Por último, puedes recuperar tus datos y aplicaciones no sin antes **escanear y desinfectar a fondo** los archivos de datos que habías guardado previamente en la copia de seguridad. Asegúrate bien de su limpieza antes de volverlos a copiar en el equipo porque podrían ser la causa de la infección y tener que repetir de nuevo todo el proceso. Incluye la revisión de unidades externas USB, otra vía frecuente de camuflaje de virus.

4. Impide nuevos daños

La partición del sistema está limpia pero también **debemos comprobar el resto de particiones y toda la red local** porque el virus ha podido llegar por esa vía e infectar de nuevo el equipo. Puedes comprobarlo con los discos de rescate creados anteriormente y también con una solución de seguridad instalada en el equipo, porque hoy por hoy, por mucha precaución que tengamos, es complicado mantener limpio un ordenador personal sin ninguna protección adicional. Si usas Windows, es recomendable al menos utilizar el Defender de Microsoft que se instala por defecto.

También es recomendable el cambio de contraseñas. Una buena parte del malware actual infecta los equipos con el objetivo de obtener las contraseñas de acceso. No es improbable que estén en manos de terceros a pesar que tu sistema esté limpio. Por ello y después de una infección, es altamente recomendable cambiarlas, las locales para autenticación en el sistema operativo a las utilizadas en los servicios de Internet, especialmente las destinadas a servicios financieros o de comercio electrónico.

Y cuida tu ciberseguridad

Insistir en la **prevención como la primera y principal línea de defensa**, observando la precaución debida en los sitios web por los que navegamos; las aplicaciones que instalamos; la recepción de correos electrónicos y adjuntos; las descargas o el uso de redes sociales; la imprescindible actualización de sistema operativo y aplicaciones o el uso de una buena solución de seguridad. Hace poco publicamos un especial con consejos generales de seguridad para ordenadores Windows o Linux que te recomendamos revisar.

Y **extremo cuidado con el Ransomware y el Phising**. Son sin duda los dos tipos de ataque más usados y peligros a nivel de computadoras cliente. La mayoría de infecciones se producen porque el usuario abre una aplicación o un programa malintencionado que puede llegar desde cualquier fuente, especialmente las habituales como un navegador web (despliegue de adware, direccionamiento a un sitio web malicioso…), el correo electrónico que en lugar de ir adjuntado incluye un enlace hacia Mega, Google Drive o Dropbox que lleva al malware o los servicios de mensajería en el caso de los ataques a móviles, cada vez más extendidos.

Una característica común a todos los Ransomware es que bloquean el funcionamiento de los equipos apoderándose de los archivos con un cifrado fuerte y exigen a la organización, empresa o usuario una cantidad de dinero **como "rescate" para liberarlos**. El gran problema es que una vez infectado no hay solución salvo que se hayan descifrado ese tipo en particular algo que suele tardar años en suceder y la recuperación de archivos es complejo. Es habitual verlo combinado con ataques de Phishing, la segunda gran amenaza y para la que también conviene extremar la precaución.

Fuente: muycomputer.