RMTELCOM
RM TELECOMUNICACIONES MOMPOS S.A.S
Te conecta con el mundo

¿Qué es el malware?

Llevamos luchando contra la amenaza del malware desde el nacimiento de la informática. Pero ¿qué es exactamente el malware? En este artículo lo definimos, presentamos sus distintos tipos y explicamos cómo funciona. También describimos las señales que nos advierten de una posible infección y explicamos cómo prevenirlas mediante nuestra protección antimalware de talla mundial:

Malware es un término general para referirse a cualquier tipo de "**mal**icious soft**ware"** (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento. Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente. Sin embargo, todas las variantes comparten dos rasgos definitorios: son subrepticios y trabajan activamente en contra de los intereses de la persona atacada.

Adware, spyware, virus, redes de robots (botnets), troyanos, gusanos, rootkits y ransomware entran dentro de la definición de malware. Y es importante señalar que el malware no solo supone una amenaza para los PC: Mac y dispositivos móviles también pueden ser su objetivo.

Entonces, ¿el malware es solo un virus informático?

¿Un virus es malware? Sí y no. Mientras que todos los virus informáticos son malware, no todo el malware son virus. Los virus son solo un tipo de malware. Mucha gente emplea los dos términos como sinónimos, pero, desde un punto de vista técnico, virus y malware no son lo mismo. Mírelo de este modo: El malware es un código malicioso. Los virus informáticos son código malicioso que se extiende por equipos y redes.

¿Cómo funciona el malware?

Sea cual sea su tipo, todo malware sigue el mismo patrón básico: El usuario descarga o instala involuntariamente el malware, que infecta el dispositivo. La mayoría de las infecciones se producen cuando realiza sin saberlo una acción que provoca la descarga del malware. Esta acción podría ser un clic en el vínculo de un correo electrónico o la visita a un sitio web malicioso. En otros casos, los hackers extienden el malware mediante servicios peer-to-peer de compartición de archivos y paquetes de descarga de software gratuito. Incrustar malware en un torrent o una descarga popular es una manera efectiva de extenderlo por una base de usuarios más amplia. Los dispositivos móviles también pueden infectarse mediante mensajes de texto.

Otra técnica es cargar malware en el firmware de una unidad USB o flash. Como el malware está cargado en el hardware interno del dispositivo (y no en el almacenamiento de archivos), es improbable que el dispositivo lo detecte. Por eso nunca debe insertar en su equipo una unidad USB desconocida.

Una vez instalado, el malware infecta el dispositivo y comienza a trabajar para cumplir los objetivos del hacker. La forma de hacerlo es lo que distingue los distintos tipos de malware. Y entonces ¿cómo funciona el malware? ¿Qué es un ataque de malware? Vamos a averiguarlo.

Tipos comunes de malware

La inmensa mayoría del malware entra en las siguientes categorías básicas, dependiendo de su funcionamiento.

Ransomware

El ransomware es la versión malware de la nota de rescate de un secuestrador. Suele funcionar bloqueando o denegando el acceso a su dispositivo y sus archivos hasta que pague un rescate al hacker. Cualquier persona o grupo que guarde información esencial en sus dispositivos corre peligro frente a la amenaza del ransomware.

Spyware

El spyware recaba información sobre un dispositivo o red para luego enviársela al atacante. Los hackers suelen utilizar spyware para supervisar la actividad en Internet de una persona y recopilar datos personales, incluidas credenciales de inicio de sesión, números de tarjeta de crédito o información financiera, con el propósito de cometer fraude o robo de identidad.

Gusanos

Los gusanos están diseñados con un objetivo en mente: proliferar. Un gusano infecta un equipo y después se replica y se extiende a dispositivos adicionales, permaneciendo activo en todas las máquinas afectadas. Algunos gusanos actúan como mensajeros para instalar malware adicional. Otros están diseñados solo para extenderse y no causan daño intencionadamente a las máquinas anfitrionas, aunque siguen atestando las redes con sus demandas de ancho de banda.

Adware

El trabajo del adware es crear ingresos para el desarrollador sometiendo a la víctima a publicidad no deseada. Algunos tipos comunes de adware son los juegos gratuitos y las barras de herramientas para el navegador. Recaban datos personales acerca de la víctima y después los emplean para personalizar los anuncios que muestran. Aunque la mayoría del adware se instala de forma legal, no por ello es menos molesto que otros tipos de malware.

Troyanos

Los antiguos poetas griegos hablaban de unos guerreros atenienses que se escondieron en un gigantesco caballo de madera para luego salir del interior, una vez que los troyanos lo arrastraron tras las murallas de la ciudad. Por tanto, un caballo de Troya es un vehículo que oculta atacantes. El malware troyano se infiltra en el dispositivo de una víctima presentándose como software legítimo. Una vez instalado, el troyano se activa y, en ocasiones, llega incluso a descargar malware adicional.

Redes de robots (botnets)

Una red de robots no es un tipo de malware, sino una red de equipos o de código informático que puede desarrollar o ejecutar malware. Los atacantes infectan un grupo de equipos con software malicioso conocido como “robots” (o “bots”), capaz de recibir órdenes desde su controlador. A continuación, estos equipos forman una red que proporciona al controlador acceso a una capacidad de procesamiento sustancial. Dicha capacidad puede emplearse para coordinar ataques, enviar spam, robar datos y crear anuncios falsos en su navegador.

¿Qué hace el malware?

El ransomware es la forma de malware más hostil y directa. Mientras que los demás tipos operan invisibles, el ransomware anuncia su presencia de inmediato y exige un pago a cambio de devolver el acceso a sus dispositivos o archivos.

En la mayoría de los casos, el malware es mucho más difícil de observar y trabaja con discreción en segundo plano. Hay malware que opera por simple malevolencia y borra datos importantes en las máquinas afectadas. No busca ni cometer fraude ni robar nada, y la única recompensa del hacker es la frustración y los contratiempos que sufren las víctimas.

Otras instancias de malware provocan consecuencias más graves. Las máquinas infectadas con este software captan la información personal o financiera del usuario y se la envían al atacante, que la utiliza para cometer fraude o robo de identidad. Llegados a este punto, la simple eliminación del malware es insuficiente para remediar el problema.

Como el malware depende de la capacidad de procesamiento del dispositivo infectado, las víctimas suelen sufrir problemas de rendimiento significativos. Una ralentización repentina puede ser síntoma de infección de malware.

¿Qué dispositivos pueden verse afectados?

Ningún dispositivo es inmune al malware. Los dispositivos Android y Mac pueden sufrirlo igual que los PC. Y, aunque el malware es poco frecuente en iOS, los iPhone y iPad son susceptibles a las amenazas para la seguridad.

Una instancia reciente de malware para Mac es lo bastante sofisticada como para evadir activamente las contramedidas de seguridad. Se denomina CrescentCore y comprueba el dispositivo de la víctima en busca de programas antivirus comunes. Si los encuentra, detiene de inmediato su propia ejecución para evitar ser detectado.

Los dispositivos móviles iOS y Android pueden infectarse con malware. Muchos tipos de malware específico para teléfonos móviles se extienden mediante SMS, aparte de los ataques estándar por correo electrónico. Si se pregunta cómo puede infectarse con malware su teléfono, estas son dos de las técnicas más comunes.

¿Cómo sabré si mi dispositivo está infectado?

Aquí indicamos algunos síntomas universales que pueden indicar la presencia de malware en su dispositivo:

1. El dispositivo empieza a funcionar más lento de lo normal. Si ha notado una ralentización repentina sin causa aparente, puede deberse a una infección de malware. Como el malware se adueña de los recursos de procesamiento del dispositivo, queda menos capacidad para todo lo demás.

2. Nota que le falta espacio de almacenamiento. Muchos tipos de malware descargan e instalan archivos y contenido adicional en el dispositivo. Una reducción repentina en la cantidad de almacenamiento libre podría indicar que está infectado con algún malware.

3. En su dispositivo aparecen ventanas emergentes y programas no deseados. Esta es una de las señales más claras de que sufre una infección de malware. Si le bombardean los anuncios emergentes o encuentra nuevos y extraños programas en el dispositivo, es probable que sea cosa del malware.

El funcionamiento lento y la reducción en el espacio de almacenamiento no siempre significan que haya malware. Con el tiempo, los dispositivos se van cargando de forma natural con archivos innecesarios. Siempre es buena idea limpiar de vez en cuando, y si al hacerlo el funcionamiento vuelve a ser el normal, es probable que no sufra una infección de malware.

Avast Cleanup puede eliminar automáticamente contenido innecesario del dispositivo, de modo que funcione a niveles óptimos. También tenemos consejos para acelerar su PC.

¿Es posible librarse del malware?

En la mayoría de los casos, es posible eliminar el malware y devolver el dispositivo a su estado normal.

Si tiene un PC y le gusta meterse en faena, puede seguir los pasos que se indican en nuestra guía para eliminar malware en PC. Tenemos guías similares para eliminar malware y otras amenazas en Mac, iPhone y dispositivos Android.

Sin embargo, algún malware es muy difícil de eliminar una vez que se engancha al sistema. Una herramienta de eliminación de malware es el modo más sencillo y fiable de garantizar la erradicación de este software malicioso. Están especialmente diseñadas para detectar el malware de forma automática y eliminarlo de su dispositivo.

Mantenga sus dispositivos a salvo del malware

La mejor protección contra el malware es un potente programa antivirus de un proveedor de confianza. Por ejemplo, Avast Free Antivirus. Nuestro antivirus gratuito recibe constantemente la calificación de «excelente» por parte de expertos del sector y es el «antivirus con el menor impacto en el rendimiento del PC», según AV Comparatives. Estamos orgullosos de proteger a los más de 400 millones de personas que confían a Avast su seguridad y privacidad.

RMTELCOM

RM TELECOMUNICACIONES MOMPOS S.A.S

Te conecta con el mundo