**¿QUÉ ES EL MALWARE?**

[Malware](https://blog.malwarebytes.com/glossary/malware/) o “software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

El malware hostil, intrusivo e intencionadamente desagradable intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo. Al igual que la gripe, interfiere en el funcionamiento normal.

La intención del malware es sacarle dinero al usuario ilícitamente. Aunque el malware no puede dañar el hardware de los sistemas o el equipo de red —con una excepción que se conozca (vea la sección Android de Google)—, sí puede robar, cifrar o borrar sus datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en el ordenador sin su conocimiento o permiso.

El malware, es cualquier código de software o programa informático escrito de manera intencionada para dañar un sistema informático o a sus usuarios. Casi todos los [ciberataques](https://www.ibm.com/es-es/topics/cyber-attack) modernos implican algún tipo de malware. Estos programas maliciosos pueden adoptar muchas formas, desde el costos y muy dañino [ransomware](https://www.ibm.com/es-es/topics/ransomware) hasta adware meramente molesto, dependiendo de lo que pretendan hacer los ciberdelincuentes.

***Tipos De Malware***

La ciberdelincuencia es una industria enorme. Según [una estimación](https://www.zdnet.com/article/cybercrime-can-be-the-biggest-threat-to-business-growth/) (enlace externo a ibm.com), sería la tercera economía más grande del mundo por detrás de EE. UU. y China, y se prevé que costará 10.500 millones de USD en 2025.

Dentro de este sector, los piratas informáticos desarrollan constantemente nuevas cepas de malware con nuevas características y funcionalidades. Estas cepas individuales de malware generan nuevas variantes con el tiempo para evadir mejor el software de seguridad. [Se estima](https://www.av-test.org/en/statistics/malware/) (enlace externo a ibm.com) que se han creado más de 1 mil millones de cepas y variantes de malware diferentes desde la década de 1980, lo que dificulta que los profesionales de la ciberseguridad sigan el ritmo.

Los piratas informáticos suelen compartir su malware haciendo que el código sea de código abierto o vendiéndolo a otros delincuentes. Los acuerdos de [malware como servicio](https://www.ibm.com/es-es/topics/malware) son frecuentes entre los desarrolladores de ransomware, por lo que incluso los delincuentes con poca experiencia técnica pueden cosechar los frutos de la ciberdelincuencia.

***¿CUÁLES SON LOS TIPOS MÁS COMUNES DE MALWARE?***

Estos son los malhechores más comunes en la galería de la deshonestidad del malware:

* El *[adware](https://es.malwarebytes.com/adware/" \t "_blank)* es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador. Suele recurrir a un método subrepticio: bien se hace pasar por legítimo, o bien se adosa a otro programa para engañar al usuario e instalarse en su PC, tableta o dispositivo móvil.
* El [*spyware*](https://es.malwarebytes.com/spyware/) es malware que observa las actividades del usuario en el ordenador en secreto y sin permiso, y se las comunica al autor del software.
* Un [*virus*](https://blog.malwarebytes.com/glossary/virus/) es malware que se adjunta a otro programa y, cuando se ejecuta —normalmente sin que lo advierta el usuario—, se replica modificando otros programas del ordenador e infectándolos con sus propios bits de código.
* Los [*gusanos*](https://blog.malwarebytes.com/glossary/worm/) son un tipo de malware similar a los virus, que se replica por sí solo con el fin de diseminarse por otros ordenadores en una red, normalmente provocando daños y destruyendo datos y archivos.
* Un [*troyano*](https://blog.malwarebytes.com/glossary/trojan/), o caballo de Troya, es uno de los tipos de malware más peligrosos. Normalmente se presenta como algo útil para engañar al usuario. Una vez que está en el sistema, los atacantes que se ocultan tras el troyano obtienen acceso no autorizado al ordenador infectado. Desde allí, los troyanos se pueden utilizar para robar información financiera o instalar amenazas como virus y ransomware.
* El [*ransomware*](https://es.malwarebytes.com/ransomware/) es un tipo de malware que bloquea el acceso del usuario al dispositivo o cifra sus archivos y después lo fuerza a pagar un rescate para devolvérselos. El ransomware se ha reconocido como el arma preferida de los delincuentes informáticos porque exige un pago rápido y provechoso en [criptomoneda](https://blog.malwarebytes.com/101/2017/11/cryptocurrency-works-cybercriminals-love/" \t "_blank) de difícil seguimiento. El código que subyace en el ransomware es fácil de obtener a través de mercados ilegales en línea y defenderse contra él es muy difícil.
* El *[rootkit](https://blog.malwarebytes.com/glossary/rootkit/" \t "_blank)* es un tipo de malware que proporciona al atacante privilegios de administrador en el sistema infectado. Normalmente, también se diseña de modo que permanezca oculto del usuario, de otro software del sistema y del propio sistema operativo.

*Otros Tipos de Malware*

Un [registrador de pulsaciones de teclas](https://blog.malwarebytes.com/glossary/keylogger/) es malware que graba todas las pulsaciones de teclas del usuario, almacena la información recopilada y se la envía al atacante, que busca información confidencial, como nombres de usuario, contraseñas o detalles de la tarjeta de crédito.

La [minería de criptomonedas maliciosa](https://blog.malwarebytes.com/101/2018/02/how-to-protect-your-computer-from-malicious-cryptomining/), denominada también minería fortuita o [cryptojacking](https://es.malwarebytes.com/cryptojacking/" \t "_blank), es un malware cada vez más prevalente instalado por un troyano. Permite que otras personas utilicen su ordenador para hacer minería de criptomonedas como bitcoin o monero. Los programas maliciosos de minería de criptomonedas utilizan los recursos de su ordenador, pero envían los coins obtenidos a sus propias cuentas, no a las del propietario del equipo. En pocas palabras, un programa de minería de criptomonedas malicioso, le roba recursos para hacer dinero.

* Los *[exploits](https://blog.malwarebytes.com/glossary/exploit/" \t "_blank)* son un tipo de malware que aprovecha los errores y [vulnerabilidades](https://blog.malwarebytes.com/glossary/software-vulnerability/) de un sistema para que el creador del exploit pueda asumir el control. Los exploits están vinculados, entre otras amenazas, a la [publicidad maliciosa](https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/), que ataca a través de un sitio legítimo que descarga contenido malicioso inadvertidamente desde un sitio peligroso. A continuación, el contenido dañino intenta instalarse en el ordenador tras una descarga involuntaria. Ni siquiera es necesario hacer clic. Todo lo que tiene que hacer es visitar un sitio bueno el día equivocado.
* Una *botnet* es una red de dispositivos infectados con malware conectados a internet bajo el control de un pirata informático. Las botnets pueden incluir PC, dispositivos móviles, dispositivos de Internet de las cosas (IoT) y más. A menudo, las víctimas no se dan cuenta de que sus dispositivos forman parte de una botnet. Los piratas informáticos suelen utilizar botnets para lanzar ataques DDoS, que bombardean una red objetivo con tanto tráfico que se ralentiza o se apaga por completo.

**RANSOM-WARE & CRYPTO-WARE**

***Ransomware y criptomalware***

El ransomware es malware diseñado para bloquear el acceso de los usuarios a su sistema o denegar el acceso a los datos hasta que se pague un rescate. El criptomalware es un tipo de ransomware que cifra los archivos del usuario y reclama un pago antes de una fecha específica y, a menudo, a través de una criptomoneda como el Bitcoin.

El ransomware es una amenaza persistente para las organizaciones de muchas industrias desde hace varios años. Ya que cada vez más empresas adoptan la transformación digital, la probabilidad de ser el objetivo de un ataque de ransomware crece considerablemente.

*Ejemplos de ransomware:*

***CryptoLocker:*** es una forma de malware predominante en 2013 y 2014 que los ciberdelincuentes usaron para obtener acceso y cifrar archivos en un sistema. Los ciberdelincuentes usaron tácticas de ingeniería social con el fin de engañar a los empleados para que descargaran ransomware en sus computadoras, lo que infectó la red. Una vez descargado, CryptoLocker mostraba un mensaje de rescate en el que ofrecía descifrar los datos si se realizaba un pago en efectivo o con Bitcoins antes de la fecha indicada. Aunque se destruyó el ransomware de CryptoLocker, se cree que los operadores consiguieron alrededor de tres millones de dólares extorsionando organizaciones desprevenidas.

***Phobos malware:*** Una forma de ransomware que apareció en 2019. Esta variedad de ransomware se basa en la familia de ransomware anteriormente conocida como Dharma (también llamada CrySis).

**COMO EVITAR UN ATAQUE DE RANSOMWARE**

***1. Necesitas las herramientas correctas para entender tus vulnerabilidades***

Tu departamento de seguridad de TI necesita de herramientas para investigar qué pasó en cada ataque y qué partes de infraestructura tienen que ser actualizadas o sustituidas. ¿No está ejecutando una aplicación o endpoint suelto? ¿Tienes puntos de red abiertos y no monitoreados? ¿Los accesos escalonados a contenidos restringidos son monitoreados?

Entender y verificar las raíces de problemas significa saber tu postura de defensa, o sea, el status de seguridad de tu red y de tus datos y la capacidad que tienes de defenderlos, reaccionar a cualquier tipo de cambios y monitorear tu respuesta a incidentes.

***2. Mantente atento al patching y a las actualizaciones***

Los invasores de hoy en día buscan por toda la internet para encontrar servidores y aplicaciones desactualizadas. Con eso, muchos ataques de ransomware ocurren rápidamente, solo días después de que esas vulnerabilidades sean atacadas por esos criminales.

Los retrasos son invitaciones a los invasores. Por eso, para evitar ataques, asegúrate de que tus programas de patching cubran todos los endpoints, sean físicos o en la nube.

***3. Pon a prueba regularmente tus procedimientos de recuperación y respuesta***

Crea un backup con tus datos esenciales y asegúrate de que ese backup esté intacto y que sea recuperable. Practica los procedimientos de recuperación y desarrolla una orden correcta para restablecer los datos en caso de que haya problemas e invasiones. Identifica tus archivos más valiosos y garantiza que estén resguardados. Por fin, revisa regularmente esta lista para asegurar que no te olvidaste de nada.

Los backups de datos y los procedimientos de recuperación deben ser el punto de partida para cualquier plan de respuesta de emergencia. Ese plan debe incluir ejercicios y entrenamientos regulares y programados, desde el

“table top” (reuniones organizadas donde cada persona cumple un determinado rol) hasta la resolución de problemas organizacionales y la simulación de ataques. Todo eso puede ser utilizado para encontrar enlaces débiles y obstáculos que puedan bloquear la vuelta de la infraestructura.

Además de todo eso, tu plan de respuesta también debe considerar un seguro digital para protegerse en casos de filtración. Analiza con cuidado todas las opciones para saber cuál es el seguro ideal para tu negocio.

***4.Mejora tu programa de seguridad y el nivel promedio de tus contraseñas***

Las contraseñas débiles han sido la causa de cerca de un tercio de todos los intentos de ataques de ransomware en el 2019. Hacer entrenamientos regulares sobre ciberseguridad es la mejor manera de ayudar a los usuarios a mejorar la intensidad de sus contraseñas. Instala un gerente de contraseñas para toda la empresa o una herramienta de verificación personal y activa un sistema de multiplicación de múltiples factores (MFA) para que los usuarios manejen datos privados y tareas relacionadas con dinero.

**CÓMO DETECTAR EL RANSOMWARE**

Un ataque de ransomware normalmente procede de un archivo ejecutable o de un script que descarga el archivo ejecutable y lo ejecuta. No todos los ataques de ransomware son inmediatos. Algunos ransomwares se mantienen inactivos hasta que llega una fecha concreta.

La prevención efectiva de ransomware necesita una combinación de buenas aplicaciones de supervisión, copias de seguridad frecuentes de los archivos, software anti-malware y formación del usuario. Aunque ninguna ciberdefensa reduce completamente el riesgo, puede limitar enormemente la posibilidad de que los atacantes tengan éxito.

***Conclusión***

Mientras que la lista de estrategias utilizadas por cibercriminales para apuntar a usuarios desprevenidos es larga y puede ser aún más extensa -ya que los cibercriminales siguen desarrollando nuevas tácticas maliciosas-, puedes descansar asegurándote de que hay formas de mantener tus datos seguros y dispositivos protegidos. Estas amenazas pueden ser controladas mediante buenas prácticas de ciberseguridad, que incluye la utilización de [soluciones de seguridad con buena reputación](https://www.eset.com/latam/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotagging&utm_content=seguridad-digital&utm_term=es) y mantener tus sistemas parcheados y actualizados.

**BIBLIOGRAFIA**

<https://es.malwarebytes.com/malware/>

<https://www.ibm.com/es-es/topics/malware>

<https://www.welivesecurity.com/la-es/2021/01/05/formas-comunes-dispositivos-pueden-infectarse-con-malware/>

<https://latam.kaspersky.com/resource-center/threats/types-of-malware>

<https://latam.kaspersky.com/blog/secure-futures-magazine/how-to-ransomware/20480/>

<https://www.trendmicro.com/es_es/what-is/ransomware/how-to-prevent.html>