proofpoint.

# Informe sobre amenazas: **ransomware**

## Datos básicos

**Descripción:**

El ransomware cifra datos esenciales o bloquea a los usuarios el acceso a sus dispositivos hasta que paguen un rescate al atacante, que suele ser una organización criminal.

**Herramientas en el mercado:**

Cryptolocker, WannaCry, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw, Locky, Petya, Conti, Sodinokibi y Ryuk

**Origen:**

Troyano AIDS creado en 1989 por Joseph Popp. Popp envió 20 000 disquetes infectados con el texto "AIDS Information—Introductory Diskettes" (Información sobre sida: disquetes de introducción) a los asistentes a la conferencia internacional sobre sida de la OMS y llevó a cabo lo que ahora se considera el primer ataque de ransomware de la historia.

**Tipos:**

- **Crypto ransomware**
  Los ciberdelincuentes cifran los archivos de un ordenador de manera que a los usuarios les resulta imposible acceder a ellos.
- **Locker ransomware**
  Se trata de un malware que impide a la víctima acceder al ordenador hasta que paga un rescate.
- **Scareware**
  Es un tipo de malware diseñado para hacer creer a las víctimas que sus ordenadores se han infectado con ransomware y conseguir que paguen un rescate al atacante. Aunque técnicamente el scareware no es un tipo de ransomware, tiene el mismo efecto en las víctimas.

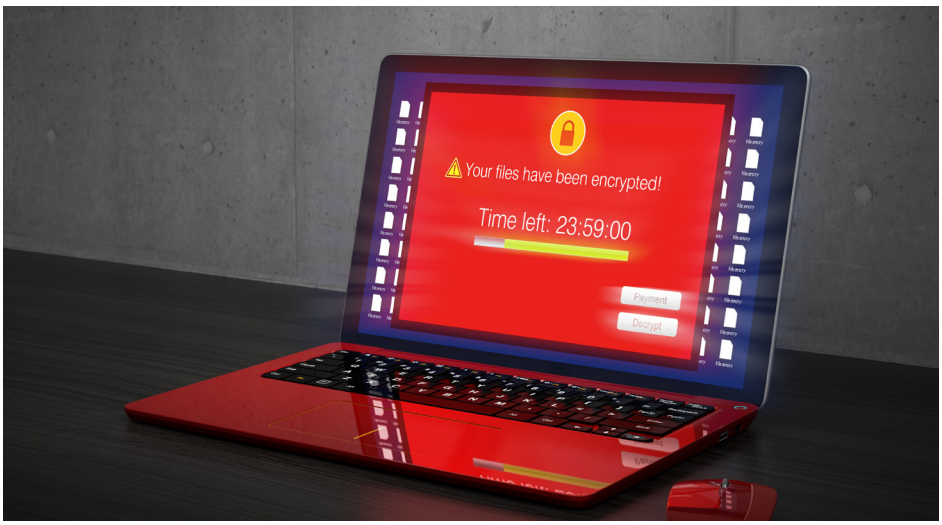
**Factores de riesgo:**

- Software y sistemas vulnerables
- Copias de seguridad de difícil acceso
- Ciberseguridad ineficaz o inexistente
- Usuarios sin formación y vulnerables

**Posibles daños:**

- Pérdidas económicas
- Pérdida de datos confidenciales o propiedad intelectual
- Posible deterioro de la reputación
- Interrupción de las operaciones y disminución de la productividad

El ransomware o secuestro de datos, que recibe su nombre del rescate (*ransom* en inglés) que se exige tras impedir a las víctimas el acceso a sus archivos, es un problema grave para cualquier empresa actual. Hoy por hoy, es uno de los tipos de ciberataque más destructivos: deja a sus víctimas en la quiebra, obliga a los hospitales a rechazar pacientes y paraliza órganos de gobierno de ciudades enteras. La mejor forma de librarse del ransomware es evitar que penetre en su entorno. Aquí encontrará un manual básico sobre esta amenaza que cada vez es más preocupante.




## Casos de ataques de ransomware señalados

### Universal Health Services pierde 67 millones de dólares por el ataque de un ransomware Ryuk

Un ataque de ransomware dirigido a Universal Health Services (UHS) supuso a la empresa cerca de 67 millones de dólares por el tiempo que permaneció inactiva y por los gastos derivados de ello. Esta organización del sector sanitario y miembro de la lista Fortune 500 tiene decenas de miles de empleados en EE. UU. y Reino Unido, y percibe unos ingresos anuales superiores a los 10 000 millones de dólares.[1]

### La UCSF paga 1,14 millones de dólares de rescate por recuperar los datos de sus investigaciones

Los ciberdelincuentes atacaron la Universidad de California en San Francisco (UCSF) bloqueando los sistemas informáticos de la Facultad de Medicina. Los administradores actuaron con rapidez y lograron aislar la infección estableciendo un perímetro de seguridad en torno a ciertos sistemas. Con ello evitaron que el ransomware llegase a la red principal de la UCSF y causase daños mayores.[2]

### Los ingresos de Cognizant se reducen entre 50 y 70 millones de dólares debido a un rescate de ransomware

En abril de 2020 Cognizant, proveedor de servicios de TI, fue víctima de un ataque de ransomware que mermó sus ingresos del segundo trimestre. El incidente se saldó con importantes costes legales, de consultoría y de otra índole destinados a investigar los hechos, restaurar el servicio y reparar los sistemas.[3]

1 Phil Muncaster (*Infosecurity*), "Universal Health Services Estimates $67 Million in Ransomware Losses", marzo de 2021.
2 Charlie Osborne (*ZDNet*), "University of California SF pays ransomware hackers $1.14 million to salvage research", junio de 2020.
3 Catalin Cimpanu (*ZDNet*), "Cognizant expects to lose between $50m and $70m following ransomware attack", mayo de 2020.

### Un ataque de ransomware interrumpe el suministro de combustible en EE. UU.

En mayo de 2021, uno de los oleoductos más grandes de EE. UU. tuvo que interrumpir su actividad por un ataque de ransomware, lo que supuso parar un sistema de 8850 km que da suministro a casi la mitad de los distribuidores de combustible de la costa este del país.[4] La empresa que gestiona el oleoducto entregó a los atacantes 4,4 millones de dólares para poder recuperar el acceso a los datos, pero según la empresa eso no bastó para restaurar de inmediato los sistemas del oleoducto.[5]

### La empresa de elaboración de productos cárnicos más importante del mundo suspende la producción de vacuno por un ataque de ransomware

La empresa, con sede en Brasil, cerró sus plantas de envasado de Colorado, Iowa, Minnesota, Pensilvania, Nebraska y Texas por un ataque que, según las autoridades estadounidenses, se lanzó desde Rusia.[6] La empresa comunicó mediante una nota de prensa que detectó el ataque en sus redes informáticas de Norteamérica y Australia. Por suerte, el ataque no afectó a sus servidores de copias de seguridad.[7]

## Anatomía de un ataque de ransomware

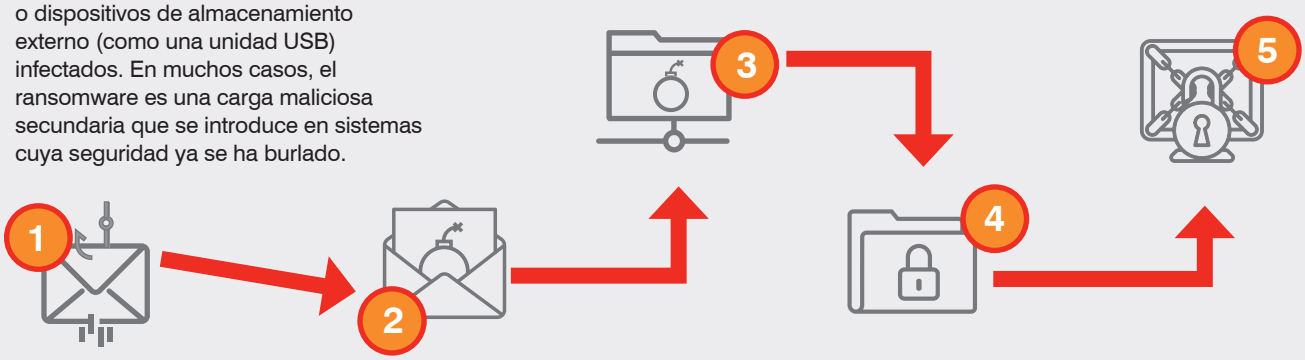
En las últimas tres décadas, el ransomware ha evolucionado hasta convertirse en una de las ciberamenazas que más preocupan. Las criptomonedas como el Bitcoin han facilitado a los ciberdelincuentes el cobro de los rescates. Además, los ciberdelincuentes se están haciendo expertos en atacar sistemas antiguos y obsoletos.

**Así se perpetran la mayoría de los ataques de ransomware:**

**1. Distribución |** Los atacantes engañan a los usuarios para que accedan a software malicioso mediante mensajes de correo que emplean el phishing, o mediante ingeniería social, sitios web falsos con enlaces maliciosos o dispositivos de almacenamiento externo (como una unidad USB) infectados. En muchos casos, el ransomware es una carga maliciosa secundaria que se introduce en sistemas cuya seguridad ya se ha burlado.

**3. Ejecución |** La carga de ransomware que se ha copiado desde el archivo se oculta y se integra en el sistema.

**5. Nota de rescate |** Por último, se le muestra a la víctima una nota en la que se le solicita el pago por desbloquear los archivos.

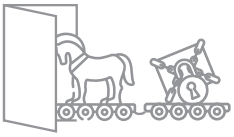



**2. Infección |** A continuación, el usuario descarga sin saberlo un archivo ejecutable llamado "cargador" (o "descargador") que instala el ransomware.

**4. Análisis y cifrado |** Posteriormente, el malware analiza el sistema y la red, y cifra los archivos.

Los ciberdelincuentes se han dado cuenta de que la mayoría de las víctimas de ransomware tienen copias de seguridad de sus datos y se niegan a pagar los rescates que piden, por lo que ahora plantean amenazas más sofisticadas. Empiezan robando y cifrando archivos, y luego amenazan a los propietarios con publicar sus datos. Esa información puede ser sumamente confidencial y personal, y puede ocasionar daños devastadores si sale a la luz. Las variantes de ransomware más sofisticadas también buscan y cifran incluso las copias de seguridad.

4 David E. Sanger, Clifford Krauss y Nicole Perlroth (*The New York Times*), "Cyberattack Forces a Shutdown of a Top U.S. Pipeline", mayo de 2021.
5 Collin Eaton y Dustin Volz (*The Wall Street Journal*), "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom", mayo de 2021.
6 Jacob Bunge (*The Wall Street Journal*), "Meat Buyers Scramble After Cyberattack Hobbles JBS", junio de 2021.
7 Hamza Shaban, Ellen Nakashima y Rachel Lerman (*The Washington Post*), "JBS, world's largest meat processor, shut down U.S. beef plants amid cyberattack", junio de 2021.



### EVOLUCIÓN DE LOS ATAQUES DE RANSOMWARE

Inicialmente, el ransomware era la payload principal de las campañas de mensajes de correo maliciosos, pero ahora es más frecuente observarlo como una infección secundaria.

Los ciberdelincuentes distribuyen troyanos y otro tipo de malware que permiten a los grupos de ransomware usar puertas traseras por las que colarse en sistemas infectados a cambio de una parte de los beneficios.

Por lo tanto, para la mayor parte de las empresas la primera línea de defensa contra el ransomware es evitar la infección inicial a toda costa. Es decir, si son capaces de bloquear el cargador, se habrán librado del ransomware.

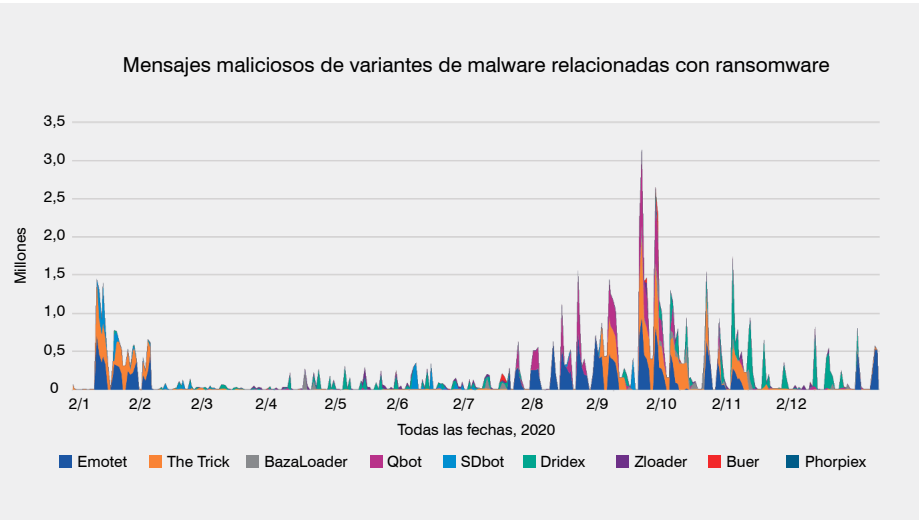
## Información extraída de las investigaciones

Por lo general, el ransomware se introduce como infección secundaria cuando la seguridad de un sistema ya se ha vulnerado mediante un mensaje de correo malicioso. Según nuestra experiencia y la de otros investigadores, muchas de las variantes del malware más prolífico están estrechamente relacionadas con infecciones de ransomware posteriores.

En esta lista se recogen las variantes de malware más habituales y el ransomware que más se asocia con ellas.

| MALWARE/DESCARGADOR | RANSOMWARE ASOCIADO |
|---|---|
| Emotet | Ryuk |
| The Trick | Conti |
| Dridex | BitPaymer/DoppelPaymer |
| Qbot | Egregor |
| SDBbot | Clop |
| ZLoader | Egregor y Ryuk |
| Buer (Buer Loader) | Ryuk |
| Phorpiex/Trik | Avaddon |

Emotet, The Trick, Dridex y Qbot fueron las variantes de malware más prolíficas en 2020, con volúmenes constantes durante todo el año y repuntes importantes en otoño.




## Cada vez más organizaciones acaban pagando (y los resultados varían)

Según el informe State of the Phish 2021 de Proofpoint, el 68 % de las organizaciones estadounidenses encuestadas reconocieron haber pagado un rescate en 2020, lo que supone el doble de la media mundial. Por otra parte, el 41 % de las organizaciones españolas se negaron a pagar el rescate tras sufrir un ataque. A nivel global, se consideró que se prestaban menos a negociar con los atacantes.

Tras hacer un pago único como rescate, el 78 % de las organizaciones francesas recuperaron el acceso a sus datos. Las estadounidenses, con un 76 %, fueron las segundas con mayor porcentaje de éxito.

Los profesionales de Infosec revelaron que en 2020 el 34 % de las organizaciones sufrieron un ataque y decidieron pagar el rescate. Otro 32 % fueron víctimas de algún ataque, pero no pagaron el rescate, y el 34 % restante aseguraron no haber sufrido ningún ataque de ransomware.

# Cómo proteger su organización

Ante todo, la mejor forma de librarse del ransomware es evitarlo.

## Antes del ataque

Empiece por asumir que será víctima de un ataque de ransomware. Después, su plan deberá girar en torno a la prevención, la detección y la respuesta al ataque. Por ejemplo:

- Haga copias de seguridad de los datos más importantes, guárdelas aparte de los sistemas de archivos principales y haga simulacros de los procedimientos de restauración de datos.
- Actualice los sistemas y aplique los parches que correspondan.
- Forme e instruya a los usuarios.
- Invierta en soluciones de seguridad centradas en las personas.
- Separe los ámbitos de red para limitar la propagación.
- Decida si su organización pagaría el rescate, y la cantidad y las circunstancias en las que lo haría.

## Durante el ataque

Ante un ataque, lo primordial es evitar daños mayores y contar con un plan de respuesta. Por ejemplo:

- Alerte a las autoridades.
- Desconecte los sistemas de la red.
- Determine el alcance del problema sirviéndose de la inteligencia de amenazas.
- Prepare su respuesta.
- Separe los ámbitos de red para acotar la propagación.
- Detecte puntos débiles, malware o vulneraciones del sistema que suelen ir de la mano del ransomware.
- Olvídese de las herramientas de descifrado de ransomware gratuitas.
- Restaure los datos más importantes y asegúrese de que no haya malware que se haya colado en la copia de seguridad de otros datos.

## Tras el ataque

Después del ataque de ransomware, inicie la restauración de los datos y solucione los problemas que el incidente haya causado. Por ejemplo:

- Limpie y repare los sistemas.
- Lleve a cabo una revisión de seguridad.
- Evalúe el nivel de concienciación de los usuarios.
- Aplique controles centrados en las personas y basados en los posibles riesgos.
- Replantéese su postura ante la seguridad y adecúe la inversión pensando en las principales áreas de riesgo.

## ¿Debería pagar el rescate?

Pagar un rescate supone financiar una actividad delictiva. No obstante, las consecuencias de un ataque pueden ser graves tanto para la empresa como para sus clientes. La respuesta no siempre está clara.

Antes de decidir cómo actuar, las organizaciones deben tener en cuenta ciertos factores:

- La seguridad de los clientes y de los empleados
- El tiempo y los recursos que se deben recuperar
- Las responsabilidades para con los accionistas de mantener la empresa en funcionamiento
- El tipo de actividad delictiva que el pago terminaría financiando

La decisión, sea cual sea, debe tomarse antes de un ataque, cuando los ejecutivos no se encuentren bajo la presión que supone la amenaza de un ultimátum y la interrupción grave de la actividad de la empresa. Más allá de que la organización esté dispuesta a pagar un rescate, sus líderes deben decidir cuánto están dispuestos a desembolsar y en qué circunstancias. Tenga presente que algunos pagos —como los que se entregan a los atacantes que figuran en las listas de sanciones que mantiene Estados Unidos— pueden ser ilegales.

## MÁS INFORMACIÓN

La mejor forma de detener el ransomware es evitarlo mediante un plan proactivo. Un buen plan de prevención de ransomware supone contar con un sistema de seguridad centrado en las personas que incluya medidas para concienciar a los empleados mediante formación basada en técnicas de ataque reales, que detecte y bloquee los descargadores de ransomware y malware que atenten contra las personas de su organización, y que le permita reaccionar rápido y adoptar las medidas necesarias antes de que la cosa vaya a peor.

Para informarse mejor sobre cómo detener un ataque de ransomware, descargue nuestra guía de supervivencia frente al ransomware

Para obtener más información, visite **proofpoint.com/es**.