

CS-014 · Malware

Ransomware

Malware que cifra los datos o bloquea el acceso a ellos y exige un pago para devolverlos.

[Read this reference sheet in English](#)

[← CS-013](#)

Ficha 14 de 15

[CS-015 →](#)

Resumen ejecutivo

El ransomware es malware que cifra los archivos de la víctima o bloquea sus sistemas y después exige un pago, por lo general en criptomoneda, a cambio de devolver el acceso. Los ataques actuales suelen añadir una segunda capa de presión: roban los datos primero y amenazan con publicarlos. Es una de las amenazas más disruptivas y costosas que enfrentan las organizaciones hoy.

Qué es

El ransomware es una categoría de malware construida alrededor de la extorsión. En su forma más común, cifra los archivos de un dispositivo o de una red entera para que su dueño no pueda abrirlos, y después muestra una nota de rescate que exige un pago por la clave de descifrado. Algunas variantes bloquean en cambio la pantalla o el dispositivo completo. El ransomware se vende y se opera con frecuencia como servicio, donde quienes lo desarrollan proporcionan el malware y los afiliados ejecutan los ataques, lo que ha bajado la barrera de entrada y aumentado el volumen. Muchas campañas usan hoy la doble extorsión: los atacantes roban datos sensibles antes de cifrarlos y amenazan con filtrarlos o venderlos si no se paga el rescate, lo que presiona incluso a las víctimas que tienen buenas copias de seguridad.

Por qué importa

Un ataque de ransomware puede detener una organización entera en horas: tumba la operación, corta el acceso a registros críticos y obliga a una recuperación costosa. Más allá del rescate en sí, las víctimas enfrentan tiempo de inactividad, gastos de recuperación, posible exposición regulatoria por los datos robados y un daño duradero a su reputación. Servicios críticos como la salud, el gobierno y la infraestructura han sido golpeados, lo que plantea preocupaciones reales de seguridad para las personas. Pagar un rescate no garantiza la recuperación y puede financiar más delito, así que las autoridades en general lo desaconsejan. Eso vuelve la prevención, las copias de seguridad resistentes y un plan de recuperación probado mucho más valiosos que cualquier pago.

■ Cómo funciona

Un ataque de ransomware suele empezar con el acceso inicial, a menudo por phishing, credenciales robadas o una vulnerabilidad explotada. El atacante se mueve entonces por la red, escala privilegios e identifica los sistemas y los datos valiosos. En muchas campañas roba datos durante esa etapa para habilitar la doble extorsión. Cuando está listo, despliega el ransomware de forma amplia y cifra archivos en tantos sistemas como pueda, a veces borrando o desactivando antes las copias de seguridad para impedir una recuperación sencilla. Después una nota de rescate explica cómo pagar y recibir la clave de descifrado. Como tanto depende de las etapas iniciales, los controles de acceso fuertes, la monitorización y la capacidad de detectar al intruso antes de que empiece el cifrado son decisivos para limitar el daño.

■ Diagrama de arquitectura



■ Flujo de trabajo

Un atacante obtiene el acceso inicial por phishing, credenciales robadas o una vulnerabilidad.

→ Se mueve de forma lateral, escala privilegios y mapea los sistemas y los datos valiosos.

→ A menudo roba datos sensibles para habilitar la doble extorsión. →

Localiza las copias de seguridad y puede borrarlas o desactivarlas. →

Despliega el ransomware, que cifra archivos en todo el entorno. →

Una nota de rescate exige el pago por la clave y por no divulgar los datos robados.

■ Ataques frecuentes

- Correos de phishing que entregan el malware o roban las credenciales usadas para entrar
- Explotación de vulnerabilidades sin parchear expuestas a internet para irrumpir
- Abuso de servicios de acceso remoto expuestos o mal protegidos
- Doble extorsión, que roba datos antes de cifrar y amenaza con filtrarlos
- Localizar y borrar las copias de seguridad para empujar a la víctima a pagar

■ Errores frecuentes

- Mantener las copias de seguridad en línea, donde el mismo ataque puede alcanzarlas y destruirlas
- No probar nunca si las copias de seguridad de verdad restauran bajo presión
- Dejar el acceso remoto expuesto sin autenticación multifactor
- Demorar los parches en sistemas expuestos a internet que los atacantes buscan de forma activa
- No tener un plan de respuesta a incidentes, así que la primera reacción se improvisa

■ Buenas prácticas

- Mantener copias de seguridad fuera de línea o inmutables y probar las restauraciones con regularidad
- Exigir autenticación multifactor, sobre todo en el acceso remoto y el correo
- Parchear sin demora, con prioridad a los sistemas expuestos a internet y explotables de forma remota
- Aplicar el mínimo privilegio y segmentar las redes para limitar el movimiento lateral
- Vigilar las señales tempranas de intrusión antes de que pueda empezar el cifrado
- Preparar y ensayar un plan de respuesta a incidentes específico para ransomware

■ Lista de verificación

- ✓ Copias de seguridad fuera de línea o inmutables en su lugar y con restauración probada hace poco
- ✓ Autenticación multifactor exigida en el acceso remoto y el correo
- ✓ Sistemas expuestos a internet parcheados según un calendario definido y breve
- ✓ Mínimo privilegio y segmentación de red que limiten el movimiento lateral
- ✓ Monitorización y detección afinadas para atrapar al intruso antes del cifrado
- ✓ Plan de respuesta y de comunicación específico para ransomware, ya probado

■ Herramientas recomendadas

Detección y respuesta en endpoints (EDR)

Detecta la intrusión y el comportamiento del ransomware y permite contenerlo rápido

Copias de seguridad inmutables o fuera de línea

Dan una vía de recuperación que el atacante no puede alterar ni borrar con facilidad

Autenticación multifactor

Bloquea el abuso de credenciales que da acceso a buena parte del ransomware

Segmentación de red

Limita hasta dónde puede extenderse el ransomware en el entorno

■ Normas del sector

NIST SP 800-61

Ciclo de manejo de incidentes para contener un ataque y recuperarse

NIST SP 800-83

Guía para prevenir y manejar malware, incluido el ransomware

Controles Críticos de Seguridad del CIS

Salvaguardas de copias de seguridad, accesos y parches, centrales en esta defensa

Relevancia profesional

El ransomware está en el centro del trabajo de seguridad actual. El personal de respuesta a incidentes dirige la contención y la recuperación, los analistas de SOC buscan las señales tempranas de intrusión que anteceden al cifrado, y los ingenieros de seguridad construyen los controles de copias de seguridad, accesos y segmentación que reducen el impacto. Los analistas de malware estudian las familias de ransomware y los profesionales de GRC evalúan la resiliencia y la preparación para recuperarse. Para el público de GRC Careers, dominar el tema es esencial en puestos de seguridad y de gobernanza.

Preguntas de entrevista

- ¿Qué es la doble extorsión y por qué presiona incluso a quien tiene copias de seguridad?
- ¿Por qué quienes trabajan en el área suelen aconsejar no pagar el rescate?
- ¿Qué hace tan importantes las copias de seguridad fuera de línea o inmutables para recuperarse?
- ¿Cómo avanza un atacante del acceso inicial hasta el cifrado?
- ¿Qué señales tempranas podría atrapar un SOC antes de que el ransomware se dispare?

Certificaciones relacionadas

CompTIA Security+
(GREM)

ISC2 Certified in Cybersecurity (CC)

GIAC Reverse Engineering Malware

Para profundizar

- [CISA StopRansomware \(en inglés\)](#)
- [NIST SP 800-61: guía de manejo de incidentes de seguridad \(en inglés\)](#)
- [MITRE ATT&CK \(en inglés\)](#)

Puntos clave

- El ransomware cifra o bloquea los datos y exige un pago para devolver el acceso.
- Los ataques actuales suelen robar los datos primero, para la doble extorsión.
- Pagar no garantiza la recuperación y puede financiar más delito.
- Las copias de seguridad fuera de línea o inmutables, y probadas, son el control de recuperación más fuerte.
- La prevención y la detección temprana, antes del cifrado, limitan el mayor daño.

Preguntas frecuentes

► ¿Una organización debería pagar el rescate?

► ¿Qué es la doble extorsión?

► ¿Cuál es la defensa más importante?

Carreras relacionadas

PUESTOS RELACIONADOS

[Incident Responder](#)

[Soc Analyst](#)

[Security Engineer](#)

CERTIFICACIONES RELACIONADAS

[CompTIA Security+](#)

[ISC2 Certified in Cybersecurity \(CC\)](#)

[GIAC Reverse Engineering Malware \(GREM\)](#)

[VACANTES ACTUALES](#)

[GUÍAS Y SALARIOS](#)

Las vacantes vigentes están en la bolsa de empleo.

[Ver todas las vacantes](#)

[Vacantes en español](#)

[Glosario GRC](#)

[Empezar en privacidad](#)

[Cumplimiento por país](#)

RUTA DE APRENDIZAJE SUGERIDA

- 1 Afiance las bases con [CS-001 Ciberseguridad](#)
- 2 Estudie esta ficha: **Ransomware**
- 3 Profundice: [Virus informáticos](#)
- 4 Profundice: [Troyanos](#)
- 5 Valídelo: trabaje hacia **CompTIA Security+**
- 6 Encuentre el puesto: [vea las vacantes disponibles](#)

Las vacantes se publican en el idioma del empleador, por lo general en inglés.

FICHAS RELACIONADAS

[CS-011 Virus informáticos](#)

[CS-012 Troyanos](#)

[CS-013 Gusanos](#)

[CS-001 Ciberseguridad](#)

MÁS DE MALWARE

[CS-011 Virus informáticos](#)

[CS-012 Troyanos](#)

[CS-013 Gusanos](#)

[CS-015 Spyware](#)

[← CS-013](#)

Ficha 14 de 15

[CS-015 →](#)

Compartir

[LinkedIn](#)

[Facebook](#)

[X](#)

[Correo](#)