Ransomware en 2025:

Perspectivas claves y estrategias de prevención

Digital Security
Progress. Protected.

El estado del ransomware

El *ransomware* sigue siendo una de las amenazas de ciberseguridad más urgentes en 2025, y continúa evolucionando tanto en sofisticación como en impacto. A pesar de años de avances, organizaciones de todos los tamaños y sectores aún se enfrentan a ataques implacables que penetran sus defensas mediante técnicas cada vez más avanzadas. Una de las últimas es el uso de **EDR killers**, *malware* diseñado para desactivar las soluciones de detección y respuesta de endpoints (EDR) antes de implementar el *ransomware*. Esto demuestra cómo los actores de amenazas se adaptan a los avances de seguridad para explotar las debilidades en las defensas de las empresas.

La motivación detrás de los ataques de ransomware sigue siendo alta, impulsada no solo por incentivos económicos, sino también por objetivos tácticos y estratégicos. Mientras que los grupos cibercriminales implementan ransomware principalmente con fines lucrativos, los grupos APT pueden utilizarlo para ocultar rastros o como herramienta destructiva para interrumpir infraestructuras críticas, a menudo con consecuencias geopolíticas. Estos grupos perfeccionan continuamente sus técnicas, aprovechando las vulnerabilidades de la cadena de suministro, los exploits de día zero y el *phishing* asistido por IA para maximizar su alcance e impacto.

Ante este panorama, la **prevención** sigue siendo la medida más eficaz para reforzar la seguridad. Si bien la respuesta y la recuperación ante incidentes son cruciales, detener el ransomware antes de que se propague reduce tanto las interrupciones operativas como las pérdidas financieras.

$4.91 millones

fue el coste promedio de un ataque de ransomware en 2024.

Fuente: *IBM: Cost of a Data Breach Report 2024*

Una estrategia de seguridad preventiva, con gestión robusta de parches, una arquitectura de confianza cero, protección nativa de IA, políticas de gestión de contraseñas, MFA, concientización y monitoreo continuo, puede reducir el riesgo de infiltración de ransomware.

A medida que avanzamos, la capacidad de anticipar, prevenir y neutralizar las amenazas de ransomware antes de que se materialicen es más crucial que nunca. Incluye contar con una **tecnología de remediación** disponible las 24x7 y 365 días del año.

Observaciones recientes

Uno de los eventos más destacados de 2024 fue el desmantelamiento de LockBit, anteriormente el grupo líder de ransomware como servicio (RaaS), que difundía la variante de ransomware más utilizada en todo el mundo. La disrupción de LockBit ha creado un vacío significativo en el panorama del ransomware. Este vacío fue rápidamente cubierto por otros actores de ransomware, siendo **RansomHub** el más **exitoso hasta la fecha**.

A finales del segundo semestre de 2024, RansomHub había registrado casi 500 víctimas, consolidándose como un actor dominante en el ecosistema del ransomware. Hasta la fecha, RansomHub ha cifrado y exfiltrado datos de víctimas de una amplia gama de sectores: TI, servicios e instalaciones gubernamentales, atención médica, servicios de emergencia, agricultura y alimentación, servicios financieros, instalaciones comerciales, manufactura crítica, transporte o sectores de infraestructura crítica como las comunicaciones.

Aunque RaaS es un entorno cibercriminal altamente competitivo donde las bandas innovan y ajustan continuamente sus programas de afiliados para atraer más socios y aumentar la rentabilidad, ESET espera que RansomHub mantenga su posición dominante a lo largo de 2025. Esto se debe no solo a sus tácticas agresivas y métodos sofisticados para mantener el control sobre las redes comprometidas y explotar las vulnerabilidades en los sistemas, sino también a su capacidad para atraer afiliados anteriormente asociados con LockBit y BlackCat.

A medida que el modelo RaaS continúa evolucionando, los actores de amenazas de ransomware adoptan cada vez más técnicas especializadas para evadir la detección y aumentar el daño. Si bien estos grupos han utilizado durante mucho tiempo herramientas de detección y respuesta en endpoints (EDR), su prevalencia ha aumentado y ahora desarrollan herramientas personalizadas y las ofrecen como parte de sus programas RaaS. Al mismo tiempo, muchos actores de ransomware que entran en el ecosistema RaaS siguen las tendencias de grupos consolidados, a menudo codificando sus cifradores en *Rust o Go* para garantizar la compatibilidad multiplataforma y un mayor alcance.

Lo que demuestra esta tendencia es que **herramientas de seguridad como EDR son un desafío** para los ciberdelincuentes.

EDR KILLERS: malware especializado, diseñado para desactivar soluciones de seguridad mediante técnicas BYOVD. Los atacantes primero instalan controladores legítimos pero vulnerables y luego los explotan para ejecutar acciones privilegiadas desde el kernel. Esto les permite eludir los controles de seguridad, finalizar procesos de seguridad y desactivar los mecanismos de detección y protección.

No se debe hablar de RaaS ni de técnicas avanzadas sin reconocer la participación y el papel de los grupos de amenazas persistentes avanzadas (APT). Estos grupos utilizan el ransomware no solo para obtener beneficios económicos, sino también para alcanzar objetivos estratégicos más amplios. Los siguientes grupos de APT se han involucrado recientemente en mayor medida en ataques de ransomware:

ChamelGang (China-aligned)

Este grupo utiliza ransomware para distraer la atención de sus operaciones encubiertas, lo que dificulta que los defensores detecten sus actividades principales.

Este grupo, también llamado CamoFei, ha estado utilizando la cepa de *ransomware* CatB en ataques que afectan a organizaciones de alto perfil en todo el mundo, incluidas organizaciones gubernamentales como la Presidencia de Brasil o infraestructura crítica como el Instituto de Ciencias Médicas (AIIMS), una universidad pública de investigación médica y hospital.

Moonstone Sleet (North Korea-aligned)

Conocido por desarrollar e implementar su propio ransomware, FakePenny, Moonstone Sleet utiliza el ransomware principalmente para obtener beneficios económicos. Anteriormente conocido como Storm-17, Moonstone Sleet ha sido identificado atacando tanto al sector financiero como al ciberespionaje. Sus métodos incluyen el uso de software troyanizado como PuTTY para el acceso inicial, la distribución de juegos maliciosos y paquetes de Node Package Manager (NPM), la implementación de cargadores de malware personalizados y la creación de empresas de desarrollo de software falsas como StarGlow Ventures y C.C. Waterfall.

➜ Estas empresas falsas interactúan con víctimas potenciales a través de plataformas como LinkedIn, Telegram, redes de trabajo independiente y correo electrónico.

Pioneer Kitten (Iran-aligned) y Andariel (North Korea-aligned)

Estos grupos han sido vinculados a ataques de ransomware, principalmente como proveedores de acceso inicial. Probablemente vendan este acceso a otros ciberdelincuentes para obtener beneficios económicos. Los primeros atacan principalmente sectores como defensa, educación, finanzas y salud, mientras que los segundos atacan infraestructuras críticas y organizaciones sanitarias, especialmente en Estados Unidos.

Pioneer Kitten también se conoce con los nombres de Fox Kitten, UNC757, Parisite, RUBIDIUM y Lemon Sandstorm, y utiliza una amplia gama de técnicas. Andariel se considera un subgrupo del Grupo Lázaro y se le atribuye a la Oficina General de Reconocimiento de Corea del Norte.

Se espera que las empresas y diversas organizaciones no sean el único objetivo de los ataques de ransomware. Los actores de amenazas están explorando y atacando sistemáticamente a los **usuarios domésticos**. En agosto de 2024, el ransomware Magniber lanzó una campaña global a gran escala dirigida a usuarios finales comunes y cifrando sus dispositivos en todo el mundo.

Aunque tales acciones se han observado en el pasado, esta campaña marcó un cambio significativo en las estrategias de ataque del ransomware, principalmente debido a la escala y amplia distribución del ataque, que se centra en usuarios individuales que a menudo carecen de medidas sólidas de ciberseguridad.

El ransomware Magniber se distribuyó mediante descargas de software malicioso, actualizaciones falsas y generadores de claves, exigiendo rescates de entre 1000 y 5000 dólares por el descifrado. Los métodos empleados para distribuir Magniber incluyen ataques de día cero de Windows, actualizaciones falsas de Windows y del navegador, y cracks de software troyanizados y generadores de claves.

Por lo tanto, los usuarios domésticos deben mantenerse alerta y proactivos en sus prácticas de ciberseguridad. Al adoptar medidas preventivas, pueden reducir significativamente el riesgo de ser víctimas de ataques de ransomware.

Las demandas de rescate dirigidas a usuarios individuales aumentaron hasta

$5,000

in 2024.

Fuente: *BleepingComputer: Surge in Magniber ransomware attacks impact home users worldwide*

Prevenir más, gestionar menos

El ransomware suele ser la carga útil final, precedida por otras amenazas, como phishing, explotación, ataques de fuerza bruta, credenciales comprometidas, descargadores o malware personalizado. Muchos posibles ataques de ransomware se detectan en las primeras etapas del ciclo de vida del ataque, y solo si los atacantes logran evadir las defensas de sus víctimas y finalmente intentan implementar el ransomware, podemos hablar de un ataque de ransomware.

Para prevenir eficazmente los ataques de ransomware, las organizaciones deben adoptar un enfoque de seguridad multicapa que incorpore automatización para abordar cada etapa del ciclo de vida del ataque. Esto puede considerarse un **enfoque preventivo** que muchas organizaciones y empresas reconocen cada vez más como una estrategia con un gran potencial, y las razones son indudables.

Primero: **la formación y la concienciación de los empleados** son cruciales, ya que el phishing sigue siendo uno de los principales vectores del ransomware. Los empleados deben estar al tanto de las señales comunes de phishing y comprender la importancia de no hacer clic en enlaces desconocidos ni descargar archivos adjuntos no solicitados.

La capacitación sobre cómo reconocer intentos de phishing, usar contraseñas seguras y habilitar la autenticación multifactor puede reducir los riesgos. La protección de endpoints con AV robustos, soluciones antimalware y herramientas de Detección y Respuesta de Endpoints (EDR) también es importante, ya que es esencial para detectar y bloquear actividades maliciosas.

Ninguna solución EDR es totalmente inmune a los controladores EDR killers, ya que

los atacantes explotan vulnerabilidades en controladores legítimamente firmados para ejecutar código malicioso en el espacio del kernel. Estos controladores, una vez instalados en Windows, pueden utilizarse para desactivar las herramientas de seguridad. Los productos de ESET bloquean eficazmente muchos de estos controladores vulnerables, y tanto ESET como los administradores pueden ayudar a los clientes a reforzar aún más sus defensas. Al configurar ajustes estrictos de PUA, solo se permiten los controladores más recientes, un enfoque que se beneficia de la orientación de expertos.

Fortalecer el sistema operativo con reglas WDAC también es importante, lo que contribuye a una estrategia de prevención a largo plazo, necesaria de por sí. Esta orientación experta puede ser clave a la hora de lidiar con los controladores EDR killers.

Otras medidas que se deben dominar incluyen **medidas de seguridad de red** como firewalls, sistemas de detección de intrusiones (IDS) y segmentación de red, que ayudan a controlar y supervisar el tráfico, evitar el acceso no autorizado y limitar la propagación del ransomware.

67%

de los CISO informaron haber aumentado sus presupuestos de ciberseguridad en 2024 en comparación con 2023.
Fuente: *IANS, 2024 Security Budget Benchmark Report*

Prácticamente ninguna medida de este tipo se puede ejecutar sin una gestión regular de parches que garantice que todos los sistemas y el software estén actualizados con los últimos **parches de seguridad**, cerrando las vulnerabilidades que los atacantes podrían explotar.

Implementar controles de acceso basados en el principio del mínimo privilegio y adoptar un **modelo de seguridad de confianza cero** minimiza aún más el riesgo de acceso no autorizado y se ha convertido en un estándar común en la prevención de la ciberseguridad. Esto también aplica al **backup** de datos críticos, almacenados sin conexión o en entornos seguros en la nube, que son vitales para la recuperación en caso de ataque. Estas copias de seguridad deben, por supuesto, probarse periódicamente para garantizar su eficacia.

Al hablar de las operaciones diarias y la utilidad de la prevención, las medidas de **seguridad del correo electrónico**, como el filtrado y la protección contra spam, ayudan a bloquear correos electrónicos y archivos adjuntos maliciosos antes de que lleguen a los usuarios.

Dado que existen muchas otras aplicaciones que se utilizan en el día a día, la **lista blanca de aplicaciones** también es fundamental. Garantiza que solo las aplicaciones aprobadas puedan ejecutarse en la red, impidiendo la ejecución de software no autorizado.

Contar con un plan de respuesta a incidentes y realizar simulacros periódicos garantiza que las organizaciones estén preparadas para responder a los ataques de ransomware.

¿Por qué no pagar?

Los actores de amenazas perfeccionan constantemente sus tácticas, explotando vulnerabilidades de día cero, debilidades en la cadena de suministro o errores humanos para eludir incluso las mejores defensas. Las organizaciones que actúan con rapidez, implementan planes de respuesta a incidentes y confían en copias de seguridad seguras pueden recuperarse sin ceder a la extorsión. Esto nos lleva a un punto crítico: por qué pagar el rescate no es la solución adecuada.

Pagar a los delincuentes que han cifrado tus datos significa:

63%

Fue la proporción de víctimas de ransomware que involucraron a las fuerzas del orden y evitaron pagar un rescate en 2024.
Fuente: *IBM, Cost of a Data Breach Report 2024*

Pagar el rescate no garantiza que los ciberdelincuentes proporcionen una clave de descifrado

- Validas el modelo de negocio detrás del crimen.
- Fomentas más actividades delictivas al financiarlas inadvertidamente.
- Permites que las bandas de *ransomware* investiguen vulnerabilidades de día cero y desarrollen nuevos exploits.
- Es posible que en el futuro sufras ataques y nuevas exigencias de dinero.

funcional; después de todo, no hay forma de exigirles responsabilidades ni emprender acciones legales contra ellos. Hay varias razones por las que pagar podría no permitir la recuperación de datos.

- Posiblemente algunos datos se hayan dañado durante el cifrado, haciéndolos irrecuperables.
- La herramienta de descifrado podría contener malware adicional, funcionar mal o ser más lenta que la restauración desde copias de seguridad.
- El proceso de entrega de la clave de descifrado puede fallar: errores en el código de descifrado, un esquema de cifrado complicado, problemas con el procesamiento de pagos o tácticas de doble extorsión que exigen pagos adicionales.
- El atacante puede simplemente actuar de mala fe, sin intención de proporcionar una clave de descifrado.

En la práctica, suelen existir 2 argumentos principales para pagar el rescate: 1) La imposibilidad de restaurar los datos cifrados a partir de las copias de seguridad, ya sea porque estas no existen, están incompletas o han sido dañadas. Antes de realizar cualquier pago, consulte con su proveedor de software de seguridad:

(a) para verificar si hay una herramienta de descifrado disponible para la variante específica de ransomware, lo que podría permitir la recuperación sin pago, y

(b) para verificar si el pagar el rescate es ineficaz para esa variante en particular.

2) Pagar resulta más económico que restaurar desde copias de seguridad. Si bien esto podría ser técnicamente cierto en términos de tiempo y trabajo, sigue siendo una decisión fundamentalmente errónea por varias razones.

Como se mencionó anteriormente, las promesas de descifrado no son fiables, existe una alta probabilidad de ser atacado nuevamente después de realizar el primer pago (recuerda, no estás tratando con personas que cumplen la ley) y, al pagar, estás apoyando una operación criminal, lo que en última instancia aumenta la probabilidad de nuevos ataques contra terceros. Pagar a veces es incluso ilegal, y una de las razones es que los atacantes podrían estar sujetos a sanciones.

Ransomware & remediation: ¿Cómo ayuda ESET?

Una herramienta de **remediación confiable**, como parte de una estrategia proactiva que prioriza la prevención, puede ser tu mejor defensa ante decisiones difíciles, ya sea invertir una gran cantidad de dinero en la recuperación de datos o incluso considerar pagar un rescate.

El *Ransomware & remediation de ESET* es una capa de seguridad automatizada dentro del módulo de protección de endpoints de la plataforma ESET PROTECT. Diseñada para mejorar la defensa contra el ransomware, funciona junto con el Escudo de ransomware, que detecta y bloquea comportamientos sospechosos. Combina prevención y remediación, ofreciendo un enfoque integral de varias etapas para combatir el cifrado.

94%

de las organizaciones encuestadas, el 100% reportó intentos de ciberdelincuentes de comprometer sus copias de seguridad durante el ataque de 2024.
Fuente: *SC World, Compromised backups send ransomware recovery costs soaring*

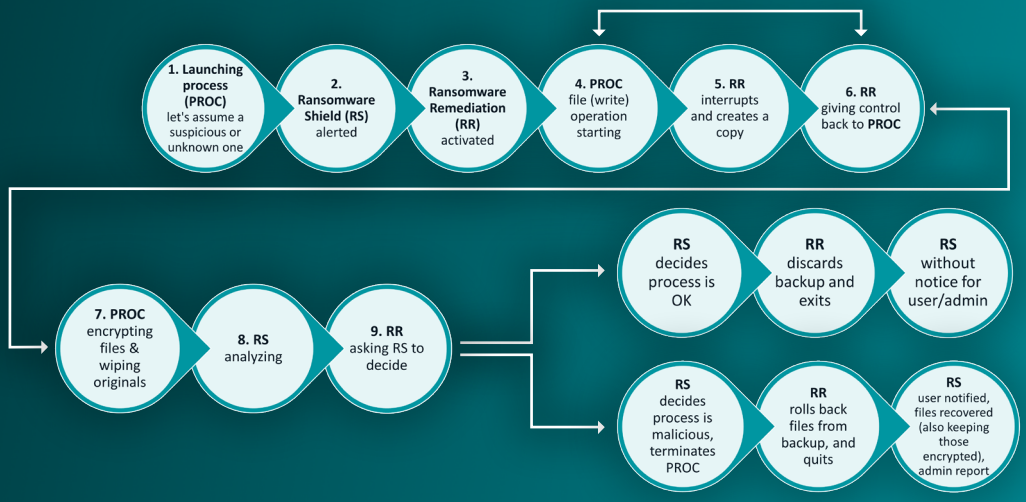
A diferencia de las soluciones tradicionales de remediación y reversión que dependen del *Servicio de Instantáneas de Volumen* del sistema operativo, ESET utiliza una solución propietaria de almacenamiento en caché de archivos que ofrece mayor flexibilidad y fiabilidad. Los operadores de ransomware suelen eliminar o sobrescribir las instantáneas para impedir la recuperación, haciendo que los métodos tradicionales sean ineficaces.

Por el contrario, el proceso de copia de seguridad de *ransomware remediation* de ESET funciona dentro de su propia sección de almacenamiento protegida en la unidad, donde los archivos no pueden ser modificados, dañados o eliminados por los atacantes.

La tecnología monitoriza continuamente todos los procesos e intercepta las modificaciones de archivos en tiempo real. En cuanto se detecta un proceso que altera archivos, el sistema de copias de seguridad instantáneas de ESET crea copias de los archivos originales, incluso antes de que sistemas de reputación de comportamiento

como Ransomware Shield determinen si la actividad es maliciosa. Todo funciona en conjunto con las tecnologías ESET LiveSense, analizando el malware hasta su núcleo.

El ransomware & remediation de ESET garantiza que las empresas puedan recuperar sus archivos al instante sin pagar un rescate. Está incluida en todos los niveles de la plataforma ESET PROTECT, a partir de ESET PROTECT Advanced.



Esquema de procesos complejo de ESET Ransomware Shield y Ransomware Remediation

BENEFICIOS DE RANSOMWARE & REMEDIATION DE ESET

- La herramienta proporciona una reversión integral a través de una restauración de archivos automatizada y simple desde un caché seguro.
- Solo protege los archivos afectados por un proceso sospechoso, por lo tanto, el espacio en disco es un problema mucho menor.
- ESET utiliza su propia tecnología exclusiva y no depende de la función VSS (Servicio de instantáneas de volumen) proporcionada en los sistemas operativos Windows de Microsoft, como lo hacen otras soluciones.
- La función está activada de forma predeterminada en los niveles de suscripción de ESET PROTECT; no se requiere interacción del usuario y los administradores pueden configurar carpetas y tipos de archivos protegidos.

Conclusión

El ransomware sigue siendo una formidable amenaza de ciberseguridad en 2025, con tácticas en constante evolución y una creciente sofisticación. La caída de LockBit y el auge de RansomHub ponen de relieve la dinámica cambiante del ecosistema RaaS, donde el éxito a menudo se mide por la capacidad de atraer y fidelizar afiliados.

Tras el desmantelamiento de LockBit por parte de las fuerzas del orden, muchos afiliados perdieron la confianza y migraron a RansomHub, lo que debilitó significativamente la escala operativa de LockBit. Mientras tanto, técnicas avanzadas como los asesinos EDR, junto con la participación de grupos APT, siguen añadiendo capas de complejidad a estas amenazas.

Las organizaciones deben adoptar un enfoque de seguridad multicapa y preventivo para combatir eficazmente el ransomware y las amenazas que lo preceden. Esto incluye la formación de los empleados, una sólida protección de endpoints y datos, copias de seguridad periódicas y soluciones de seguridad avanzadas como MDR o XDR.

Con la completa suite de ciberseguridad de ESET, que incluye la tecnología de remediación de ransomware, una solución proactiva que te permite recuperarte rápidamente y minimizar el impacto de los ataques, puedes gestionar incluso las amenazas de ransomware más sofisticadas.

MÁS INFORMACIÓN

Somos ESET

Defensa proactiva. Nuestra misión es minimizar la superficie de ataque.

Anticípate a las ciberamenazas conocidas y emergentes con nuestro **enfoque preventivo, impulsado por IA y experiencia humana**. Experimenta la mejor protección gracias a nuestra IA sobre ciberamenazas, recopilada y analizada durante más de 30 años, que impulsa nuestra extensa red de I+D, liderada por **investigadores de renombre del sector**.

ESET protege tu empresa para que puedas aprovechar al máximo el potencial de la tecnología.

Multicapa, enfoque preventivo

IA de vanguardia con experiencia humana

Inteligencia de amenazas de renombre mundial

Soporte hiperlocal y personalizado

eset®
Digital Security
Progress. Protected.