KEEPER
Cybersecurity Starts Here

Informe sobre el impacto del ransomware 2021

Contenido

Introducción y metodología

2021 será el año del ransomware. A medida que aumenta la frecuencia de los ataques, las peticiones de rescate, cada vez más llamativas, acaparan los titulares. Los consumidores, que antes estaban relativamente protegidos de cualquier impacto, están experimentando escasez de productos y dificultades para acceder a los servicios a medida que las organizaciones con las que hacen negocios quedan fuera de servicio.

Pero, ¿qué ocurre dentro de una organización después de un ataque? ¿Cómo se ven afectados los procesos internos? ¿Cuál es el impacto en la eficiencia y la productividad de los empleados? Para averiguarlo, Keeper encuestó a 2000 empleados de todo Estados Unidos cuyos empleadores habían sufrido un ataque de ransomware en los 12 meses anteriores.

Keeper Security contrató a Pollfish para realizar esta encuesta a 2000 empleados a tiempo completo en Estados Unidos. Sólo se incluyó a las personas que trabajan a tiempo completo en empresas que habían sido víctimas de ataques de ransomware en los doce meses anteriores. La encuesta finalizó en junio de 2021.

Las consecuencias de una mala formación en ciberseguridad

Casi un tercio de los empleados carecía de formación adecuada en materia de ciberseguridad antes del ataque.

La formación de los empleados en materia de ciberseguridad es crucial para prevenir los ataques de ransomware, sobre todo porque muchos de ellos tienen que ver con la ingeniería social:

- Los encuestados informaron que los correos electrónicos de phishing causaron el 42 % de los ataques de ransomware
- Los sitios web maliciosos representaron otro 23 %
- Las contraseñas vulneradas causaron el 21 %

Sin embargo, el 29 % de los encuestados dijeron a Keeper que no sabían lo que era el ransomware antes de que sus empresas fueran víctimas. Esto indica que se podrían evitar muchos, si no la mayoría, de los ataques de ransomware de la siguiente manera:

- Formar adecuada y rutinariamente a los empleados sobre la concienciación en materia de ciberseguridad, especialmente sobre cómo evitar el phishing y otros esquemas de ingeniería social
- Exigir a los empleados que utilicen contraseñas fuertes y únicas para todas las cuentas y habilitar la autenticación multifactorial siempre que sea compatible

¿A BUENAS HORAS MANGAS VERDES?

Los encuestados nos dijeron que, tras el ataque, el 87 % de las organizaciones aprobaron protocolos de seguridad más estrictos, el 90 % proporcionó a sus empleados formación adicional sobre ciberseguridad y el 67 % aumentó su gasto en ciberseguridad.

Pagar o no pagar

Aunque todo el mundo está de acuerdo en que el pago de rescates fomenta la realización de nuevos ataques, el hecho de si las organizaciones deban ceder a las demandas del cibersecuestro sigue siendo un tema de gran debate incluso dentro de la comunidad de seguridad. Esto se debe a que cuando una organización sufre un ataque activo, sus dirigentes se enfrentan a una enorme presión por parte de los clientes, las partes interesadas de la empresa e incluso las aseguradoras cibernéticas para resolver el problema y volver a estar en línea lo antes posible. La presión es especialmente intensa en las instalaciones sanitarias y en el sector público, donde el tiempo de inactividad del sistema podría poner en riesgo la salud y las vidas humanas.

Como resultado, el 49 % de los encuestados dijo a Keeper que sus empleadores pagaron el rescate. Sin embargo, este dinero no cayó del cielo: el 93 % informó de que sus empleadores redujeron los presupuestos en otras áreas tras el pago del rescate.

Los altos costes indirectos del cibersecuestro

La recuperación de un cibersecuestro supone altos costes indirectos.

Mientras las estratosféricas peticiones de rescate son tendencia en las redes sociales, las organizaciones incurren en numerosos costes indirectos después de un ataque, sobre todo en lo que se refiere a las interrupciones de los sistemas. Además de frustrar a los clientes y socios, estas interrupciones impiden a los empleados realizar su trabajo.

- El 77 % de los encuestados no pudieron acceder temporalmente a los sistemas o a las redes después del ataque
- El 28 % de las interrupciones duraron una semana o más
- El 26 % de los encuestados no pudieron desempeñar plenamente sus funciones laborales durante al menos una semana

Incluso una vez que los sistemas vuelven a estar en línea, las organizaciones deben realizar cambios para evitar nuevos ataques. La abrumadora mayoría de los encuestados (83 %) dijo que sus organizaciones instalaron nuevo software o realizaron otras actualizaciones importantes, como la migración de algunos activos a la nube.

En la mayoría de los casos, el despliegue de estos cambios perjudicó aún más la productividad y se sumó al balance de los costes indirectos de recuperación; el 71 % de los encuestados afirmó que el proceso de instalación de nuevos programas y actualizaciones resultó incómodo o perturbó la productividad.

- El 64 % de los encuestados perdió credenciales de acceso o documentos
- El 38 % dijo haber experimentado fallos en el programa o en la aplicación
- El 33 % se enfrentó a una pronunciada curva de aprendizaje sobre los nuevos protocolos
- El 40 % perdió tiempo por los frecuentes reinicios y actualizaciones del ordenador
- El 43 % tuvo que iniciar sesión repetidamente en programas/cuentas (frente a permanecer conectado continuamente)
- El 21 % dijo que sus herramientas y aplicaciones habituales en línea ya no estaban disponibles

Desgraciadamente, justo cuando los empleados más necesitaban el apoyo de las TI para restablecer sus contraseñas, intentar recuperar documentos perdidos y obtener ayuda con las nuevas aplicaciones y protocolos, los departamentos de TI a menudo estaban muy ocupados. Más de un tercio (36 %) de los encuestados afirmó tener un acceso limitado al soporte informático para cuestiones no relacionadas con la seguridad post-ataque.

Porcentaje de ataques que no se comunican

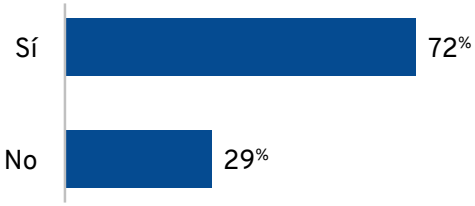
Los ataques de ransomware están más generalizados de lo que se piensa porque muchos de ellos no se dan a conocer.

Además de la presión que sienten los líderes de las organizaciones para pagar el rescate y seguir adelante, el 64 % de los encuestados consideró que sufrir un cibersecuestro tuvo un impacto negativo en la reputación de su organización. Además, el 63 % de los empleados informó de que el ataque les hizo perder personalmente la confianza en su organización.

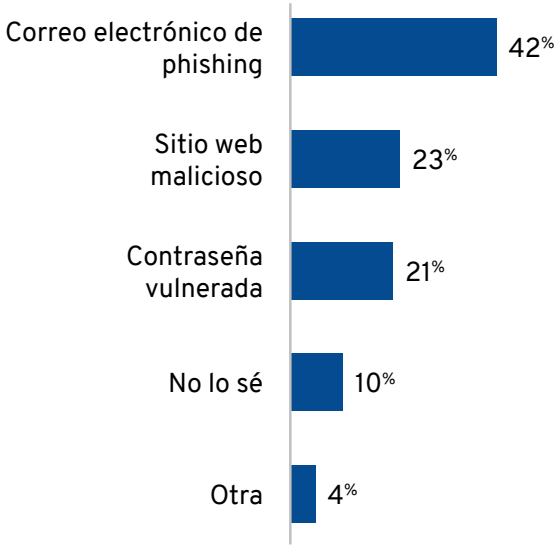
Teniendo esto en cuenta, no es de extrañar que el 26 % de los encuestados informara de que sus empleadores sólo revelaron el ataque a socios y clientes (no al público en general), mientras que el 15 % no se lo dijo a nadie. Esto indica que los cibersecuestros están probablemente mucho más generalizados de lo que se cree.

Datos completos

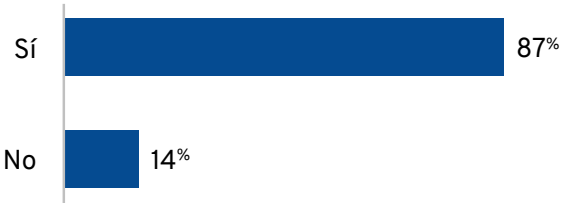
P1. Antes del ataque, ¿Ud. sabía lo que era el cibersecuestro de datos o ransomware?



P2. ¿Cuál fue la causa del ataque de ransomware a su empresa?

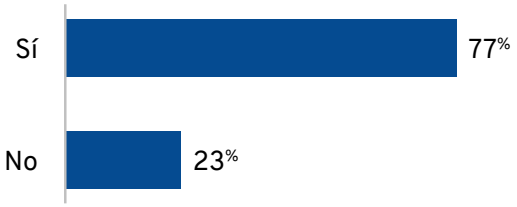


P3. ¿Ha adoptado su empresa protocolos de seguridad más estrictos como consecuencia del cibersecuestro de datos?

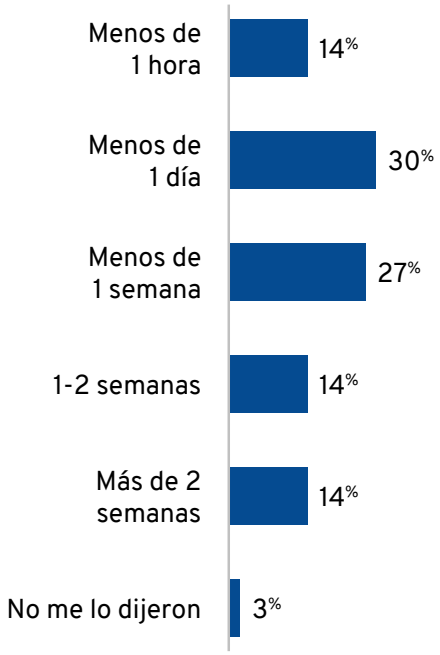


Resultados de las respuestas (Algunas respuestas pueden ser superiores al 100 % debido al redondeo)

P4. ¿Su empresa estuvo fuera de línea (por ejemplo, no pudo acceder a los sistemas o redes) durante algún período de tiempo debido al cibersecuestro de datos?

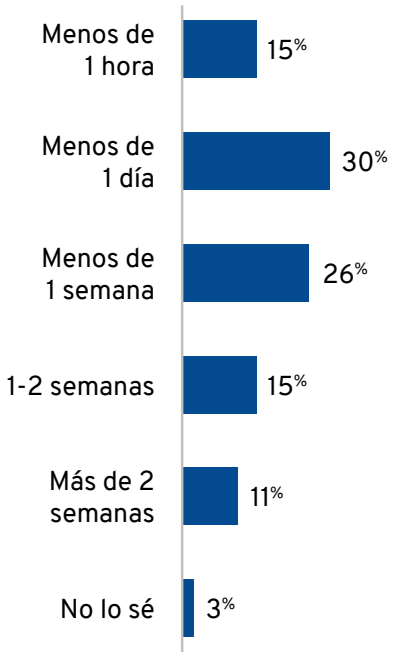


P5. En caso afirmativo, ¿durante cuánto tiempo estuvo paralizada su empresa?

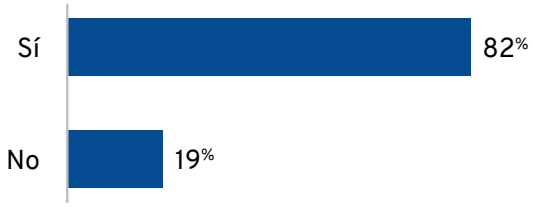


Resultados de las respuestas (Algunas respuestas pueden ser superiores al 100 % debido al redondeo)

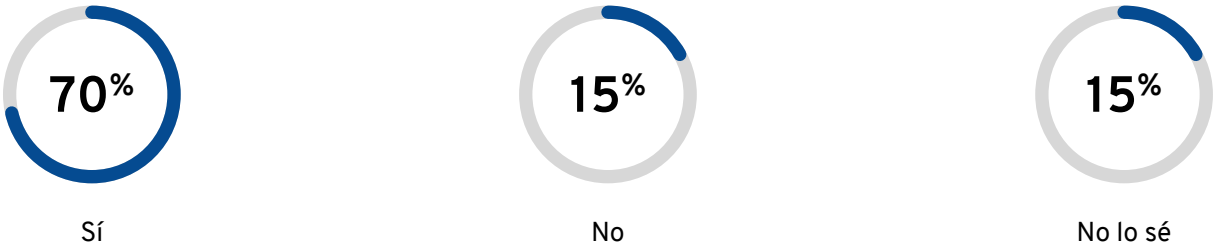
P6. En caso afirmativo, ¿durante cuánto tiempo no pudo trabajar plenamente?



P7. ¿Cree que la dirección de su organización se comunicó eficazmente con los empleados tras el ataque de ransomware?

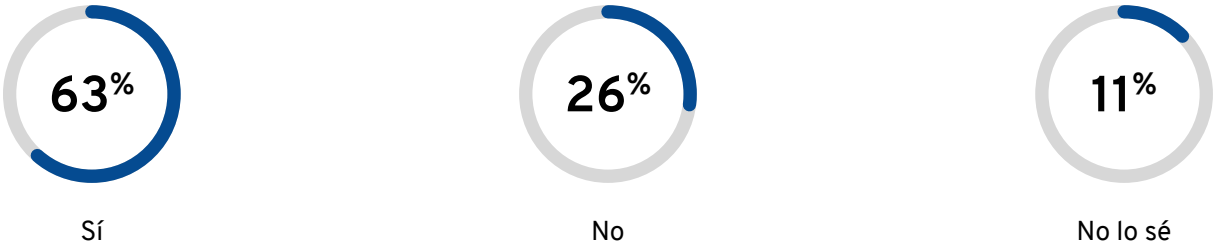


P8. ¿Avisó su empresa a los clientes y socios del ataque?

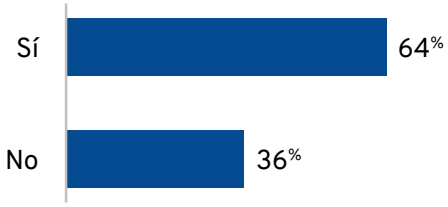


Resultados de las respuestas (Algunas respuestas pueden ser superiores al 100 % debido al redondeo)

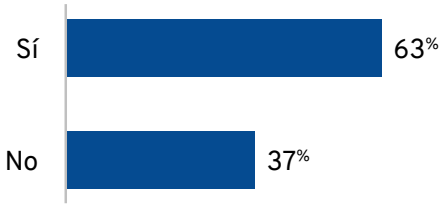
P9. ¿Emitió su empresa una declaración pública como reacción al ataque?



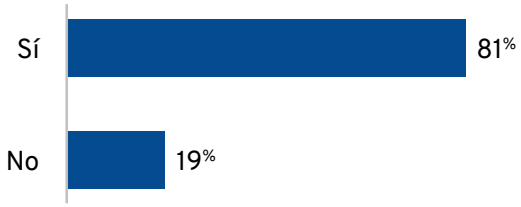
P10. ¿Considera que el ataque de ransomware impactó negativamente en la reputación de su empresa?



P11. ¿El ataque de ransomware afectó a su confianza en su organización?

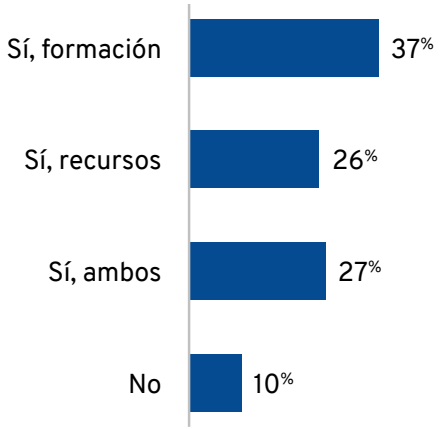


P12. Antes del ataque del ransomware, ¿instalaba regularmente las actualizaciones de software cuando se le pedía?

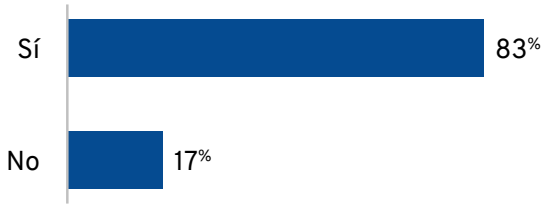


Resultados de las respuestas (Algunas respuestas pueden ser superiores al 100 % debido al redondeo)

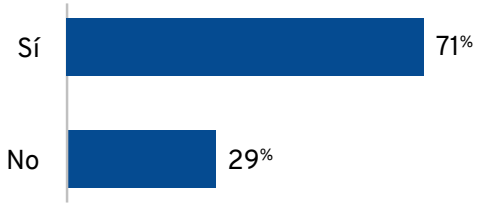
P13. Tras el ataque, ¿ofreció su empresa formación o recursos de ciberseguridad?



P14. Tras el ataque, ¿su empresa instaló software o realizó otras actualizaciones tecnológicas importantes (por ejemplo, trasladando cosas a la nube)?

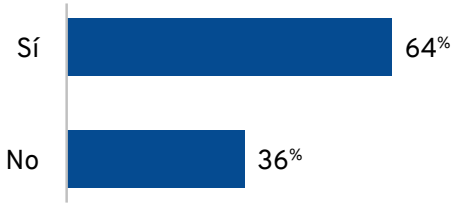


P15. En caso afirmativo, ¿considera que el proceso de instalación de nuevos programas/ actualizaciones le causó alguna molestia o interrumpió la productividad?

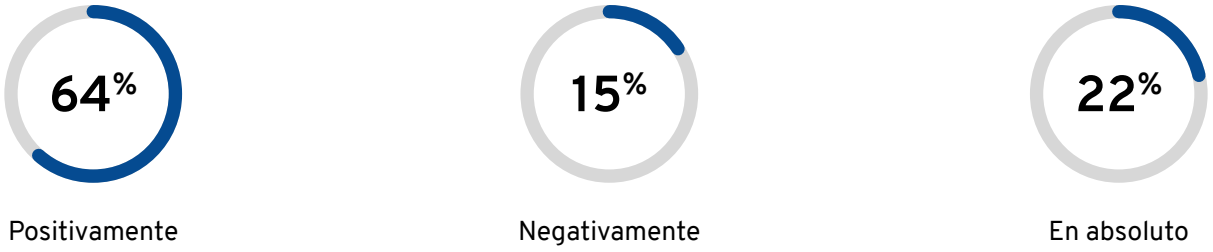


Resultados de las respuestas (Algunas respuestas pueden ser superiores al 100 % debido al redondeo)

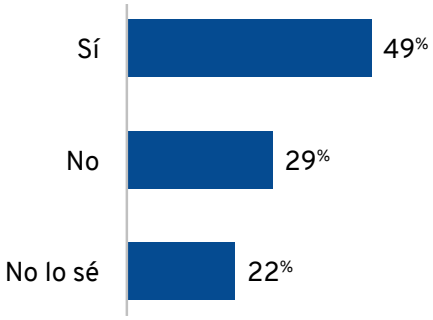
P16. En caso afirmativo, ¿perdió alguna información, como credenciales de acceso o documentos, en el proceso de actualización de sus dispositivos?



P17. En caso afirmativo, ¿cómo cree que las actualizaciones han afectado a sus rutinas de trabajo diarias?

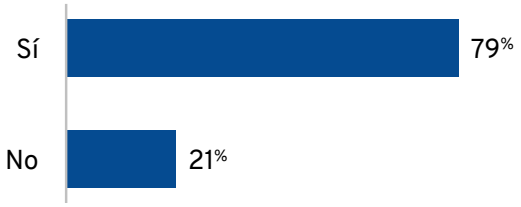


P18. ¿Su empresa pagó el rescate?



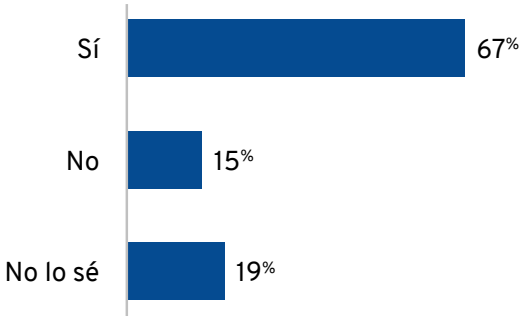
Resultados de las respuestas (Algunas respuestas pueden ser superiores al 100 % debido al redondeo)

P19. En caso afirmativo, ¿se comunicó la cantidad a los empleados?



P20. En caso afirmativo, ¿ha notado que su organización haya ajustado los presupuestos en otras áreas tras el pago?

P21. ¿Aumentó el gasto en ciberseguridad en su empresa tras el ataque?



Resultados de las respuestas (Algunas respuestas pueden ser superiores al 100 % debido al redondeo)

Sobre Keeper

Keeper protege a las organizaciones contra los ataques de ransomware gracias a una sólida administración, a controles y visibilidad sobre la seguridad de contraseñas fuertes y la supervisión de la Dark Web en tiempo real.

La plataforma de seguridad y encriptación de contraseñas de grado empresarial y con un marco de conocimiento cero de Keeper ayuda a miles de empresas de todo el mundo a prevenir los ciberataques relacionados con las contraseñas, a mejorar la productividad y a cumplir con la normativa.

Keeper ofrece a los administradores de TI una visibilidad completa de las prácticas de contraseñas de los empleados, lo que les permite supervisar la adopción de los requisitos de las contraseñas y hacer cumplir las políticas de seguridad de las contraseñas en toda la organización, incluidas las contraseñas fuertes y únicas y la autenticación multifactorial (2FA). Los exhaustivos controles de acceso permiten a los administradores establecer los permisos de los empleados en función de sus funciones y responsabilidades, así como configurar carpetas compartidas para grupos individuales, como las clasificaciones de los puestos de trabajo o los equipos de proyectos.

Para una mayor protección, las organizaciones pueden desplegar valiosos complementos como Keeper Secure File Storage, que permite a los empleados almacenar y compartir de forma segura documentos, imágenes, vídeos e incluso certificados digitales y claves SSH, y BreachWatch™, que escanea los foros de la Dark Web y notifica a los administradores de TI si alguna de las contraseñas de los empleados se ha visto comprometida en una filtración de datos pública.

Keeper cuenta con las certificaciones SOC-2, FIPS 140-2 e ISO 27001, y también está incluida en la lista para ser utilizada por el gobierno federal a través del Sistema para la Administración de Subvenciones (System for Award Management - SAM). Keeper protege a empresas de todos los tamaños en todos los sectores industriales importantes.

Para saber más visite **keeper.io/ransomware-impact**.