HISCOX

Informe de Ciberpreparación de Hiscox 2022

ACTUALIZACION – RANSOMWARE

Cover illustration
www.johnholcroft.com

La lucha contra el ransomware

Los datos muestran que solo el 59% de las empresas que pagaron un rescate recuperaron con éxito todos sus datos.

Gareth Wharton
CEO de ciberseguridad de Hiscox

Lamentablemente, los ciberdelincuentes y las empresas que se defienden de ellos han entrado en el juego del gato y el ratón durante la última década. En 2019, sin embargo, vimos un cambio significativo a favor de los delincuentes. Los ataques de ransomware aumentaron de modo importante, viendo a una serie de grupos como REvil, LockBit y otros pasar a primer plano. Los ataques a Norsk Hydro[1] y a la ciudad de Baltimore[2] son dos de los más destacados.

Durante 2020, las aseguradoras de riesgos ciber empezaron a plantear mayores exigencias de ciberseguridad a sus clientes. En ese momento, el ransomware se centraba en el cifrado de datos, por lo que las aseguradoras exigieron copias de seguridad externas para mitigar el riesgo de que los delincuentes utilizaran el ransomware para cifrar sus datos críticos. Hasta cierto punto, esto niveló el terreno de juego, obligando a las bandas de ransomware a modificar sus técnicas.

A partir de 2020 empezamos a ver la evolución de dos tendencias clave. En primer lugar, el uso de las conocidas como técnicas de doble extorsión, por las que los delincuentes cifran y exfiltran (roban) datos. ¿Por qué supuso esto un cambio en el juego? Incluso si los clientes habían realizado copias de seguridad externas de forma frecuente, los delincuentes podían extorsionarlos por la liberación de los datos sensibles robados. En segundo lugar, la proliferación del ransomware como servicio (RaaS) redujo la barrera de entrada incluso para los ciberdelincuentes menos sofisticados. Al igual que el software como servicio (SaaS), con el que los clientes alquilan una serie de servicios como el correo electrónico o los servidores de colaboración, el RaaS permite a los delincuentes sin conocimientos cibernéticos realizar campañas de ransomware por una modesta cuota mensual.

Estos dos factores han llevado a las aseguradoras a exigir nuevos y mejores controles de seguridad informática. Por ejemplo, no ejecutar servicios de acceso remoto inseguros, garantizar que los servicios remotos estén debidamente protegidos por la autenticación de múltiples factores (MFA) y exigir la aplicación de parches en toda la empresa de los servicios críticos dentro de un número determinado de días después de que el proveedor publique el parche. Ahora, las empresas no sólo tienen un listón más alto para rellenar un formulario de propuesta de seguro ciber, sino que para obtener un presupuesto a menudo es necesario mejorar los controles o procesos de seguridad. Todo ello en un esfuerzo por convertir a la empresa en un objetivo más difícil para los ciberdelincuentes.

Por supuesto, estos controles de seguridad no son las únicas herramientas disponibles para combatir el ransomware. Los principales proveedores y gobiernos tienen interés en defenderse de la amenaza del ransomware. Por ejemplo, una de las técnicas más comunes de las bandas de ransomware son los correos electrónicos de phishing que utilizan archivos adjuntos de Microsoft Office que contienen macros para descargar la primera etapa de un ataque de ransomware. Este mismo año, Microsoft ha anunciado que bloqueará las macros de Office por defecto. Aunque es un paso adelante positivo, ya estamos viendo cómo las bandas de ransomware pivotan a diferentes tipos de archivos, como los .lnk o los .iso. Esto demuestra lo rápido que se mueve el juego del gato y el ratón del que hablábamos al principio.

Los gobiernos también desempeñan un papel fundamental en la lucha contra el ransomware mediante operaciones más ofensivas. En los últimos 18 meses, tanto los gobiernos estadounidenses como los europeos han atacado a estas bandas de ransomware. Por ejemplo, la acción de Interpol contra Clo[3] o la acción de EE.UU. contra la banda Darkside[4] y el desmantelamiento por parte de Interpol de la famosa red de bots Emotet[5]. Además, los gobiernos están tratando de limitar la capacidad de los delincuentes para 'cobrar' criptomonedas. Esto está obligando a las bandas de ransomware a cambiar de tipo de ataque o a desviar su atención de las entidades estadounidenses y europeas. Por último, las agencias gubernamentales, especialmente la CISA en EE.UU. y la NCSC en el Reino Unido, han sido mucho más proactivas a la hora de alertar sobre posibles ataques, como la vulnerabilidad Log4j en diciembre de 2021.

Entonces, dada la evolución del ransomware en los últimos años, ¿cuál su estado actual? Utilizando los datos del Informe de Ciberpreparación de Hiscox 2022, podemos comprender mejor a qué se enfrentan realmente los clientes. El informe se basa en los resultados de una encuesta realizada a más de 5.000 empresas de ocho países y de diversos tamaños y sectores.

Es importante entender que pagar por una clave de descifrado no significa que vaya a poder recuperar todos sus datos. En casi todos los casos que vemos, los delincuentes proporcionan una clave de descifrado que funciona, ya que al fin y al cabo se trata de una transacción comercial para ellos. Sin embargo, hay dos cosas que pueden limitar la eficacia incluso de una clave de descifrado que funcione.

[1] https://www.bbc.co.uk/news/business-48661152
[2] https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack
[3] https://www.bleepingcomputer.com/news/security/operation-cyclone-deals-blow-to-clop-ransomware-operation/
[4] https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-operation-shuts-down/
[5] https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

La lucha contra el ransomware
continuación

La primera es la velocidad, ya que a menudo se tarda semanas en descifrar completamente los datos.

En segundo lugar, a medida que la rutina de encriptación maliciosa se ejecuta, lo hace en sistemas transaccionales vivos.

Esto es como desconectar el cable de alimentación de un servidor de base de datos en funcionamiento, siendo probable que el proceso del ransomware pueda dañar la integridad de los datos.

En otras palabras, el hecho de que el ransomware se haya producido, independientemente de una clave de descifrado, significa que todos los datos no se pueden recuperar por completo y deben ser reconstruidos. El 43% de los encuestados que pagaron un rescate dijeron que recibieron la clave de recuperación, pero que aun así tuvieron que reconstruir los sistemas. De forma igualmente alarmante, el 36% que pagó un rescate sufrió otro ataque.

Los sectores más y menos preparados (%)

En la mayoría de los artículos que aparecen en prensa, la razón por la que se mencionan es porque la empresa es de alto nivel o la demanda de rescate notable, por ejemplo, de varios millones de dólares. Sin embargo, nuestra investigación muestra que la mediana de los rescates pagados fue inferior a los 10.000 dólares. Esto demuestra que el ransomware no es sólo un ataque grande y complejo contra grandes empresas por parte de bandas de ransomware conocidas, sino que ahora es un ataque básico utilizado por atacantes mucho menos sofisticados. El punto clave a tener en cuenta es que las pymes no están en absoluto a salvo de este tipo de ataques.

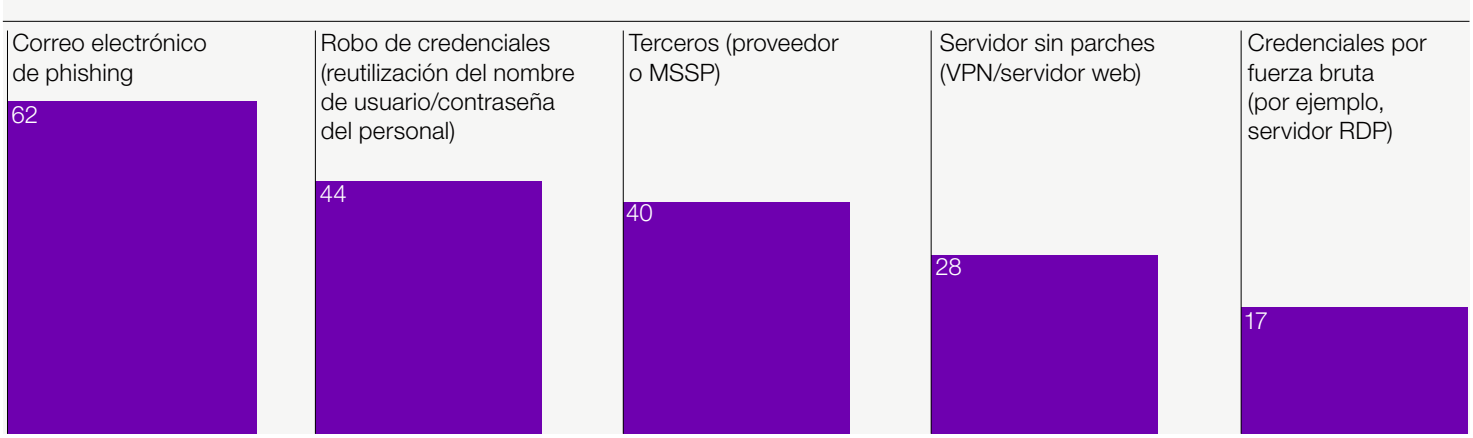
También encontramos que hay una discrepancia en cuanto a que ciertas industrias son más propensas a pagar un rescate. Si observamos el porcentaje de encuestados que pagaron por industria, este nos sugiere qué sectores de la empresa están más y menos preparados.

Esto coincide en gran medida con nuestra propia experiencia. Tanto los servicios profesionales como los financieros suelen disponer de fondos para programas de seguridad más completos y, por tanto, están mejor protegidos y con la capacidad de responder a un ataque si éste se produce.

Además, los menos preparados son también los sectores con algunas de las ventanas de la cadena de suministro más estrechas y con menos regulaciones exigidas en materia de seguridad. En el caso de que se produzca un ataque, este tipo de empresas no pueden estar fuera de línea mucho tiempo, siendo a menudo, el pago de rescate, la última opción.

Cuando miramos los datos sobre cómo los atacantes entraron en los sistemas de los encuestados, los resultados son similares año tras año. Hay cinco métodos de entrada clave y, según nuestros datos internos, vemos que se utilizan todos ellos. Aunque estos vectores de ataque hayan sido probados y testados por las bandas de ransomware, no es imposible defenderse de ellos.

Método de entrada más común (%)



La lucha contra el ransomware
continuación

Este verano, Hiscox llevó a cabo un nuevo análisis sobre la amenaza del phishing. Según una prueba reciente en cinco empresas, vemos que una prueba genérica de phishing no es suficiente para detener el ransomware.

Realizamos dos pruebas con estas cinco empresas. En la primera se utilizó un conocido proveedor de pruebas de phishing y ganchos de phishing estándar (por ejemplo, un paquete de Amazon, una alerta de LinkedIn, etc.). La tasa global de clics en los correos electrónicos masivos de la primera simulación fue del 9%. Lo más interesante es que el más efectivo de los cinco ganchos fue un correo electrónico temático de Office 365 sobre el restablecimiento de una contraseña. Aunque no es sorprendente con una base de instalación de Office 365 tan grande, el hecho de que se hiciera clic en él cuatro veces más que en los otros ganchos, se considera alarmante.

En la segunda simulación, utilizamos un correo electrónico dirigido, diseñado de forma única y específica para cada empresa, pero con un esfuerzo de ingeniería social limitado. También nos dirigimos a los altos directivos, en lugar de a la población general de empleados. En este caso, el porcentaje de clics se multiplicó por cuatro, hasta el 36%. Lo que demuestra que, si bien la formación sobre phishing es una parte fundamental de los requisitos de seguridad de cualquier empresa, la formación específica para los altos cargos también debería formar parte del apoyo adicional al personal directivo.

Dado que no hay un resultado perfecto una vez que una empresa ha sido atacada con ransomware, la situación ideal es mitigar el riesgo tanto como sea posible.

Los pasos para prevenir un ataque de ransomware incluyen:

La ruta de los atacantes en	Mitigaciones
Correo electrónico de phishing	Formación general y personalizada del personal, fuerte seguridad del correo electrónico
Robo de credenciales (reutilización del nombre de usuario/contraseña del personal)	Formación del personal sobre el uso de contraseñas únicas, autenticación multifactorial (MFA)
Terceros (proveedor o MSSP)	Comprensión de las cadenas de suministro, auditorías periódicas
Servidor sin parches (VPN/servidor web)	Lista de materiales del software (SBoM) para saber qué hay en su patrimonio, parches regulares
Servidor sin parches (credenciales de VPN/servidor de fuerza bruta, por ejemplo, servidor RDP)	Formación del personal sobre el uso de contraseñas únicas, MFA, control "justo a tiempo" de los puertos de acceso a Internet

Si ocurre lo peor, ¿cómo se puede mitigar un ataque de ransomware?

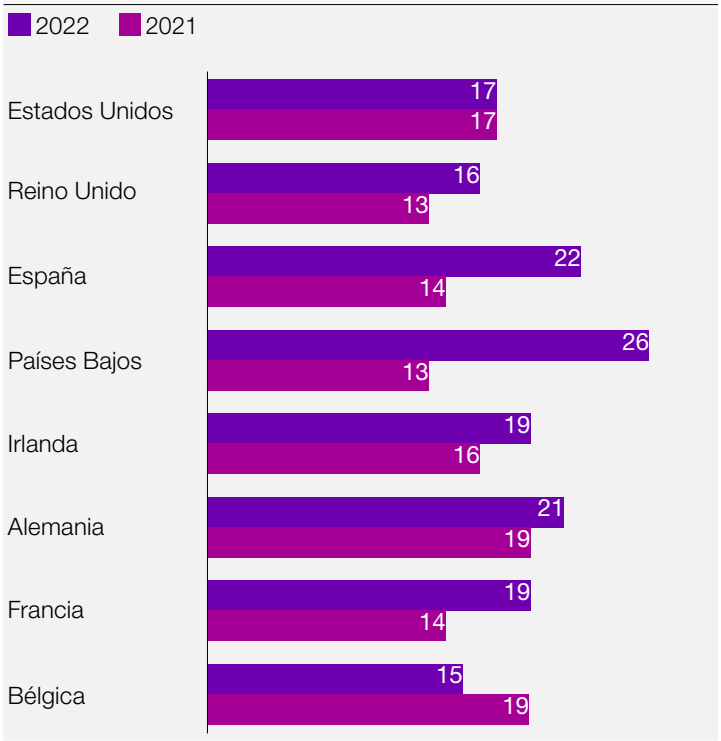
- Asegúrate de que tienes copias de seguridad offline fiables, frecuentes y probadas: en el caso de las pequeñas empresas, esto podría ser tan sencillo como llevar las unidades de copia de seguridad a casa o almacenarlas fuera de las instalaciones.
- Prepárate para lo peor: asegúrate de tener un plan de respuesta ante el ransomware y ponlo a prueba con frecuencia. ¿A quién llamarías, cómo te comunicarías con el personal, los clientes, las partes interesadas, los medios de comunicación, etc.?
- Obtén ayuda de tu proveedor de TI: ¿necesitas contratar a una empresa especializada en respuesta a incidentes (IR)?
- Seguro ciber: utiliza las ventajas de una empresa de respuesta a través de tu proveedor de seguros para gestionar el incidente y volver a funcionar.
- No te dejes llevar por el pánico: tómate tu tiempo para evaluar la situación y las opciones que tienes antes de actuar.

El ransomware es una amenaza para todas las empresas, independientemente de su tamaño, sector o ubicación. Todas las partes, clientes, aseguradoras y gobiernos deben tomársela en serio. La acción coordinada ha demostrado ser eficaz, pero hay mucho más que hacer. Es una amenaza de la que puedes y debes protegerte, ya que, como hemos explicado, una vez que has sido atacado, no hay forma fácil de volver a la normalidad.

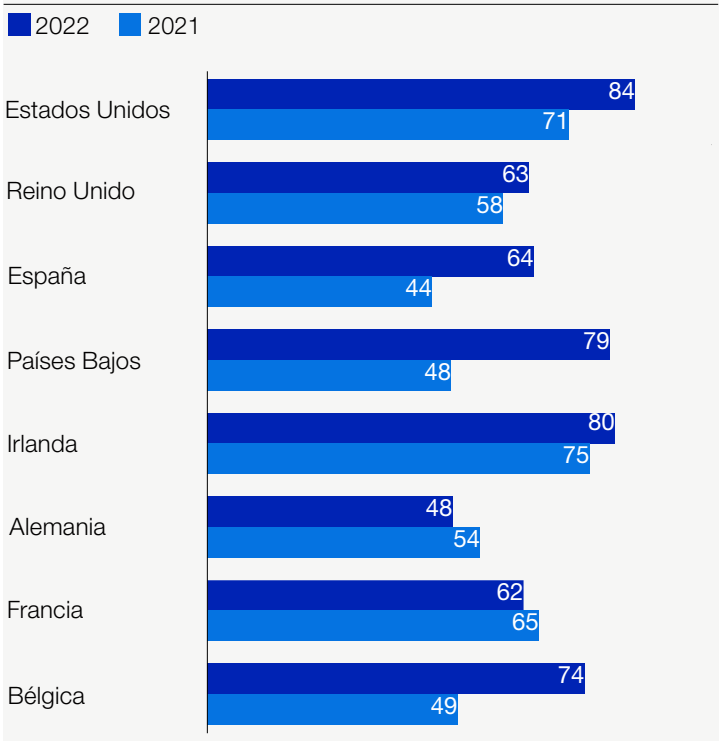
La mayoría de las empresas son objetivo del ransomware básico, no de los actores estatales de alto perfil, por lo que las empresas deberían centrarse en dificultar su ataque. Sin embargo, es igualmente importante tener un plan en caso de que ocurra lo peor: tener un plan probado y buenas copias de seguridad. Un punto de partida útil es **'Exercise in a box'** del NCSC, una herramienta en línea que permite a las empresas practicar su respuesta a los ciberataques. **(https://www.ncsc.gov.uk/information/exercise-in-a-box).**

¿A quién se ataca? ¿Quién paga?

Han sido víctima de un ataque de ransomware (%)



Víctimas de ransomware que pagaron (%)



¿Por qué pagaron las empresas un rescate?

En muchos ataques, parece que las bandas de ransomware se dirigen deliberadamente a las copias de seguridad, lo que refuerza la necesidad de que las copias de seguridad estén segregadas para volver a operar. Las empresas necesitan proteger los datos de los clientes cuando se produce una exfiltración de datos y los delincuentes amenazan con publicarlos.

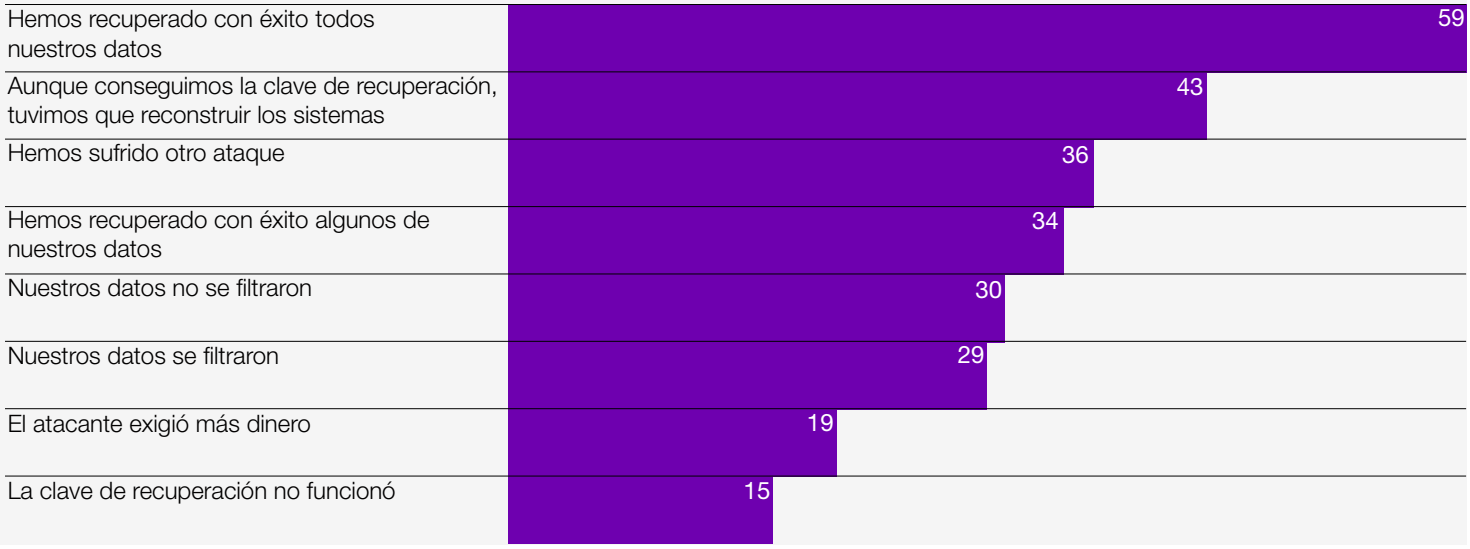
Razones de las empresas para pagar un rescate (%)

¿Funcionó pagar un rescate?

Sólo el **59%** recupera totalmente sus datos porque en muchos casos no se pueden recuperar todos los datos.

Se trata de una transacción comercial, por lo que a las bandas de ransomware no les beneficia no dar claves de descifrado que funcionen. Eso no significa, sin embargo, que sea fácil volver a trabajar de inmediato con la clave. Para el 36% de los que pagaron un rescate, el ransomware inicial siguió dando lugar a nuevos ataques.

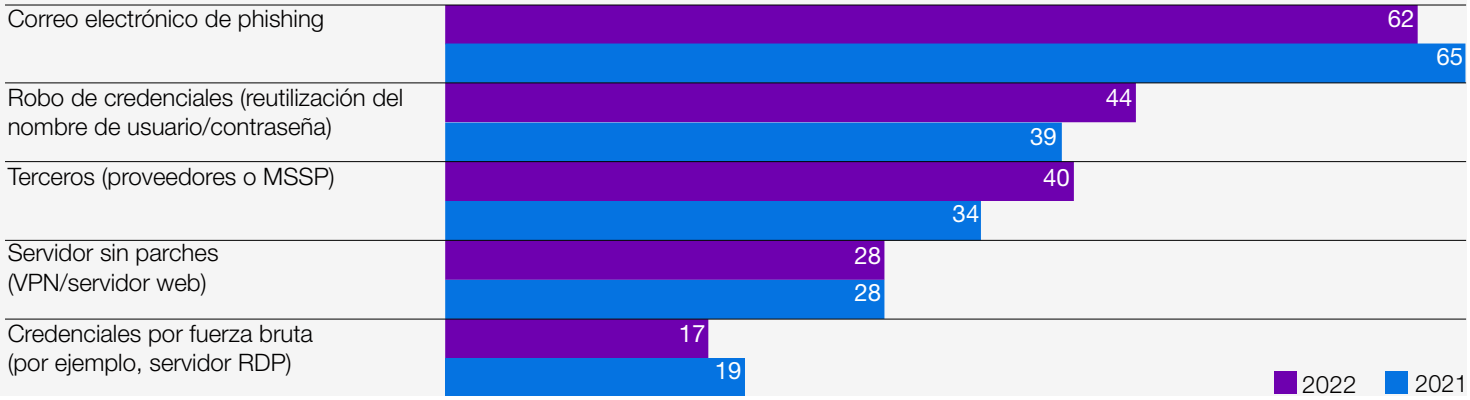
El resultado de pagar un rescate (%)



¿Cómo acceden los atacantes?

Se están utilizando cinco métodos de entrada clave. Son métodos probados por las bandas de ransomware, pero no es imposible defenderse de ellos.

Métodos de entrada (%)



Según una pequeña prueba reciente realizada por Hiscox en cinco empresas, una prueba genérica de phishing no es suficiente para detener el ransomware.

Según Beauceron Security, los informes sobre el porcentaje medio de clics de los proveedores de phishing globales oscilan entre el 3,4% y el 12%. La tasa de clics de los correos electrónicos masivos en una prueba de phishing genérica fue del 9%. En una aproximación más específica a los altos cargos, éstos hicieron clic en el 36% de las ocasiones. Esto es más del doble de la media y entre un grupo de personas de más alto perfil. La formación específica para los altos cargos es especialmente importante.

Hiscox España

c/ Miguel Ángel, 11 4º planta
28010 Madrid

+34 915 15 9900
info_spain@hiscox.com
hiscox.es/hiscox-cyber-readiness-report-2022

22161 11/22