MANDIANT

EXTORSIÓN MULTIFACÉTICA: LA EVOLUCIÓN DEL RANSOMWARE

Una amenaza para la seguridad nacional

Los ciberadversarios han propiciado que el ransomware se convierta en el principal vector de ataque en organizaciones de todo tipo y tamaño. Los atacantes de ransomware han intensificado sus misiones amenazando con el cierre de infraestructuras críticas, poniendo en riesgo la salud y la seguridad públicas, desviando recursos públicos vitales, interrumpiendo las instituciones educativas y afectando a la privacidad de los datos hasta tal punto que en algunos casos se considera ahora una amenaza para la seguridad nacional.

Aumento de la agresividad de los atacantes

Desde el primer ataque de ransomware registrado en 1989, los atacantes han ido madurando su técnica, lo que ha creado una industria multimillonaria con la intención y la capacidad de paralizar las operaciones empresariales. Las tácticas de los actores de amenazas han evolucionado para establecer un negocio lucrativo mediante el robo de datos, acompañado de amenazas dañinas de publicar esos datos sensibles si no se satisfacen sus demandas. Estos riesgos tan elevados han hecho que las demandas de extorsión aumenten drásticamente, como ocurrió con una conocida empresa de infraestructuras críticas que pagó una demanda de rescate de USD 4,4 millones en bitcoin[1] para reabrir el suministro de servicios públicos en la costa este de Estados Unidos tras un ataque.

El cambio significativo en la actividad del ransomware se hizo público en 2020, lo que llevó a Mandiant a etiquetar este "nuevo ransomware" como extorsión multifacética. La proliferación de la extorsión multifacética ha sido tan impactante para la industria de la ciberseguridad que fue presentada en el informe M-Trends 2021 de Mandiant.

25 %

El 25 % de los incidentes globales a los que respondió Mandiant estaban relacionados con el ransomware en 2020[2]

2400

Casi 2.400[3] gobiernos, centros sanitarios y escuelas de Estados Unidos fueron víctimas del ransomware

DÍAS

El tiempo de permanencia promedio global de los ataques de ransomware es de cinco días[2]

1. Forbes (julio de 2021). Los hackers del ransomware REvil se han desconectado.
2. FireEye (2021). M-Trends 2021.
3. IST (2021). Un marco de acción integral: Recomendaciones clave del grupo de trabajo sobre ransomware.

Características de la extorsión multifacética

Aunque las amenazas de ransomware y extorsión multifacética están estrechamente relacionadas, la extorsión multifacética presenta un riesgo más profundo para las organizaciones.

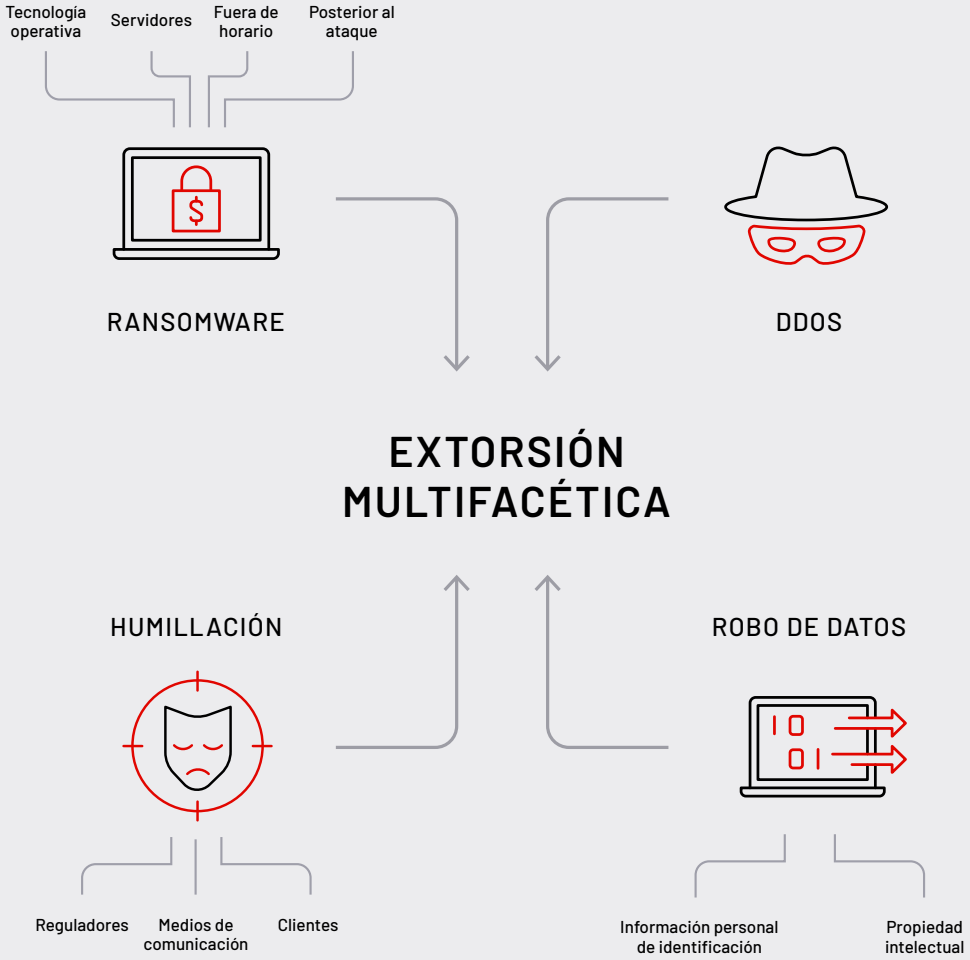
Normalmente, los responsables de las empresas y los gestores de riesgos relacionan el ransomware con los archivos cifrados por el malware que se vuelven inaccesibles para los usuarios legítimos, lo que, en última instancia, da lugar a un nivel de interrupción perjudicial para las empresas. La estrategia de mitigación más común por parte de los equipos de seguridad hoy en día contra un ataque de ransomware es un sólido programa de copias de seguridad fuera de línea. Sin embargo, esto por sí solo no siempre ofrece una recuperación fácil o sin problemas.

La extorsión multifacética lleva lo que hemos llegado a conocer como ransomware tradicional a un nivel superior, al publicitar el robo de datos críticos, convirtiendo la interrupción del servicio en una vulneración de datos completa. Como demuestra el diagrama a continuación, la extorsión multifacética implica múltiples puntos de ataque, incluyendo el cifrado del ransomware, el robo de datos y el "señalar y avergonzar" públicamente a la organización víctima.

> *Una vulneración de datos puede dar lugar a un mayor nivel de daños a la reputación, multas normativas, demandas judiciales colectivas e iniciativas de transformación digital entorpecidas. Estas consecuencias no se solían ver con el ransomware antes de 2019.*
>
> — M-Trends 2021

La extorsión “multifacética”

Durante un evento de extorsión multifacética, las copias de seguridad de los datos siguen siendo relevantes para la interrupción. Sin embargo, no ayudan con el robo de datos real; el objetivo permanece a merced tanto del atacante que aplica tácticas de coerción y amenaza con amplificar las noticias de la vulneración a menos que se cumplan las demandas, como de los organismos reguladores que pueden multar a la organización por no proteger adecuadamente los datos de sus clientes. La organización también puede sufrir un daño en su reputación extremo.



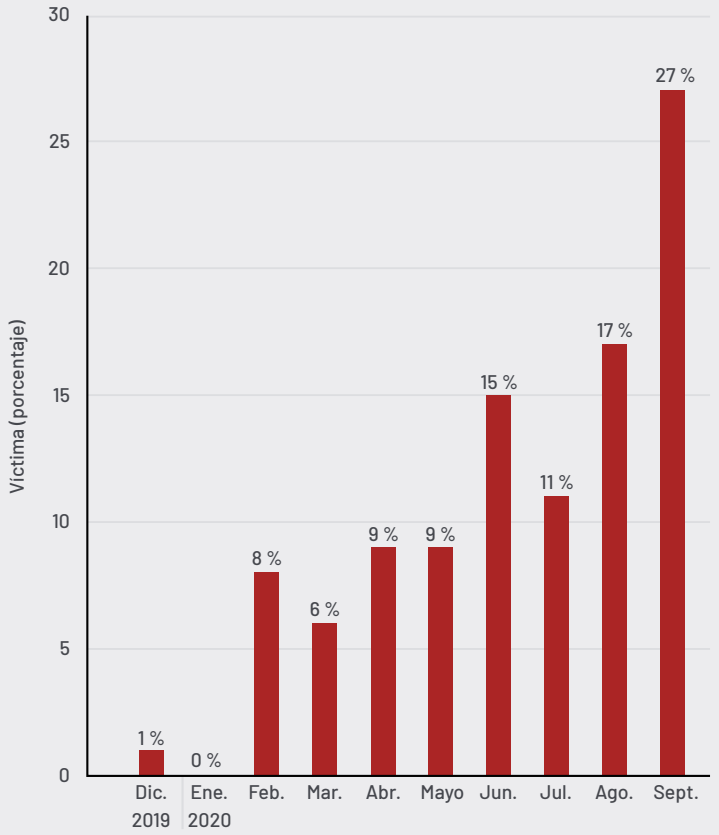
Tácticas de gran presión

Las víctimas de extorsión multifacética tienen poco control sobre la divulgación de su incidente de robo de datos. Los atacantes utilizan la posible divulgación de los datos durante las negociaciones para aumentar el monto del rescate solicitado o incitar al pago inmediato por parte de la organización víctima. Para causar la máxima interrupción el atacante recurre a:

- Acosar a los empleados
- Notificar a los socios comerciales
- Enviar campañas de spam por correo electrónico
- Informar a los operadores de valores para que puedan vender en corto antes de que se filtren los datos
- Contactar a organizaciones de noticias y medios de comunicación
- Utilizar anuncios en las redes sociales para humillar a las víctimas
- Crear y mantener sitios web del tipo nombrar y humillar

Los sitios web del tipo "nombrar y humillar" han demostrado ser exitosos para algunas operaciones de extorsión multifacética. De marzo a septiembre de 2020, Mandiant registró una media de al menos un nuevo sitio web de humillación al mes.[4] Esta cifra continúa creciendo constantemente. Si bien las víctimas abarcan casi todas las industrias, el sector manufacturero ha tenido una representación desproporcionada.

Número de víctimas que aparecen en los sitios web del tipo "nombrar y humillar"



4. FireEye (Abril de 2021). M-Trends 2021.

El precio de pagar rescates

La divulgación pública de un ataque de extorsión multifacética puede afectar significativamente a la reputación de la organización víctima, lo que se traduce en una pérdida de confianza de socios, accionistas y clientes. El efecto dominó puede extenderse a la cotización de las acciones, las relaciones comerciales estratégicas, la fidelidad de los clientes, la facturación, la rentabilidad y la retención de los empleados. Muchas organizaciones escarban en sus bolsillos para pagar la demanda de extorsión, con lo que se realiza una maliciosa, pero lucrativa transacción a favor del atacante. Pagar un rescate es un juego de azar: las organizaciones no conocen a su atacante ni saben si cumplirá con su palabra.

> *En última instancia, que una organización pague o no un rescate depende de sus circunstancias individuales, teniendo en cuenta factores como el tiempo de recuperación con o sin pago, la fiabilidad del actor de la amenaza y la sensibilidad de los datos que fueron robados.*

Mandiant ha observado que los atacantes modernos de ransomware pueden adoptar cualquiera de las siguientes estrategias o características:

No pueden volver a encriptar los datos, pero suelen tener suficiente ventaja para extorsionar aún más

Son fiables, su modelo de negocio depende de ello, por lo que es probable que lleven a cabo las consecuencias perjudiciales en caso de que no reciban el pago

Suelen pasar al siguiente objetivo cuando se les paga

No garantizan la eliminación de los datos robados (a pesar de recibir una "prueba" de eliminación)

Acción preventiva

Ante el aumento de los ataques de extorsión multifacética, los equipos de seguridad deben adoptar un enfoque proactivo para proteger sus entornos. Los expertos de Mandiant han comprobado que en muchos casos se podría haber contenido o evitado rápidamente un evento si se hubieran aplicado las mejores prácticas de configuraciones de seguridad y de validación continua de la seguridad antes de un incidente de extorsión multifacética.

Realice una corrección previa de su entorno

La "corrección previa" es la práctica de implementar proactivamente mejoras en los controles y la seguridad que se aplican comúnmente como parte de los esfuerzos de recuperación después de una vulneración de la ciberseguridad.

Los expertos de Mandiant que trabajaron en las operaciones de respuesta a incidentes a lo largo de 2020 observaron los siguientes puntos en común entre las organizaciones víctimas:

Priorizar las acciones para abordar estos problemas puede ayudarle a mitigar el riesgo de un incidente de ransomware o extorsión multifacética.

Una gran cantidad de cuentas con un gran nivel de privilegios en Active Directory

Cuentas que no son informáticas con un gran nivel de privilegios configuradas con nombres principales del servicio (SPN)

Controles de seguridad no configurados para minimizar la exposición y el uso de las cuentas con privilegios en los endpoints

Los atacantes modifican los objetos de la política de grupo (Group Policy Objects, GPO) para implementar ransomware

Conozca las amenazas que afectan a su organización

El acceso a la última versión de Threat Intelligence para la primera línea de defensa le permite a su organización mejorar sus defensas ayudándole a comprender la identidad, los objetivos, el momento, la motivación y los métodos de los últimos actores de la amenaza. Se puede utilizar Threat Intelligence para priorizar y centrar los esfuerzos en las amenazas específicas a las que se enfrentan su industria y organización, probando los procedimientos de seguridad y solucionando las vulnerabilidades.

Pruebe sus defensas

El poner a prueba de forma segura a su organización contra escenarios de ataques de extorsión multifacética del mundo real puede ayudar a identificar los errores de configuración existentes en un entorno y a mejorar o desarrollar una postura de seguridad más sólida.

La buena noticia es que es posible minimizar significativamente el impacto general de un ataque. Una vez identificados los activos que pueden ser objeto de ataques de extorsión multifacética en su entorno, puede darse cuenta de forma proactiva de sus puntos débiles en materia de seguridad y realizar mejoras tanto estratégicas como tácticas evaluando su capacidad para detectar, contener y neutralizar el ransomware y las amenazas relacionadas con él con servicios de seguridad creados a tal efecto.

Más información en **www.mandiant.com**

Mandiant
833.3MANDIANT (362.6342)
info@mandiant.com

Acerca de Mandiant

Desde 2004, Mandiant® ha sido un socio de confianza para las organizaciones preocupadas por la seguridad. En la actualidad, la inteligencia y la experiencia de Mandiant, líderes en el sector, impulsan soluciones dinámicas que ayudan a las organizaciones a desarrollar programas más eficaces e infundir confianza en su preparación cibernética.

MANDIANT