¿Cómo afecta el ransomware a mi negocio?

v¿Cómo afecta el ransomware a mi negocio? GandCrab, SamSam, WannaCry, NotPetya, son diferentes tipos de ransomware y están afectando a las empresas. De hecho, los ataques de ransomware a las empresas aumentaron un 88% en la segunda mitad de 2018, ya que los ciberdelincuentes se alejaron de los ataques centrados en el consumidor.

Los ciberdelincuentes reconocen que las grandes empresas se traducen en grandes beneficios, dirigidos a hospitales, agencias gubernamentales e instituciones comerciales. En total, el costo promedio de una violación de datos , que incluye remediación, sanciones y pagos de ransomware, asciende a $ 3.86 millones (todas las cifras dadas en dólares de los Estados Unidos).

La mayoría de los casos de ransomware últimamente se han identificado como GandCrab . Detectado por primera vez en enero de 2018, GandCrab ya ha pasado por varias versiones a medida que los autores de amenazas hacen que su ransomware sea más difícil de defender y fortalecer su cifrado. Se ha estimado que GandCrab ya ha recaudado alrededor de $ 300 millones en rescates pagados , con rescates individuales establecidos de $ 600 a $ 700,000.

En otro ataque notable ocurrido en marzo de 2018, el ransomware SamSam paralizó la ciudad de Atlanta al anular varios servicios esenciales de la ciudad, incluida la recolección de ingresos y el sistema de registros de la policía. En total, el ataque de SamSam le costó a Atlanta $ 2.6 millones para remediarlo .

Teniendo en cuenta la gran cantidad de ataques de ransomware y el tremendo costo asociado con ellos, ahora es un buen momento

para ser inteligente en cuanto a la protección de su empresa contra el ransomware. Anteriormente, hemos cubierto el tema con gran detalle, pero aquí hay una breve descripción de cómo proteger su empresa contra el malware.

Copia de seguridad de sus datos

Suponiendo que tiene copias de seguridad disponibles, la remediación o cura de un ataque de ransomware es tan simple como limpiar y volver a crear imágenes de los sistemas infectados. Es posible que desee escanear sus copias de seguridad para asegurarse de que no se hayan infectado, ya que algunos ransomware están diseñados para buscar recursos compartidos de red. En consecuencia, haría bien en almacenar copias de seguridad de datos en un servidor de nube seguro con cifrado de alto nivel y autenticación de múltiples factores.

Parche y actualiza tu software

El ransomware a menudo se basa en kits de explotación para obtener acceso ilícito a un sistema o red (por ejemplo, GandCrab). Siempre que el software de su red esté actualizado,

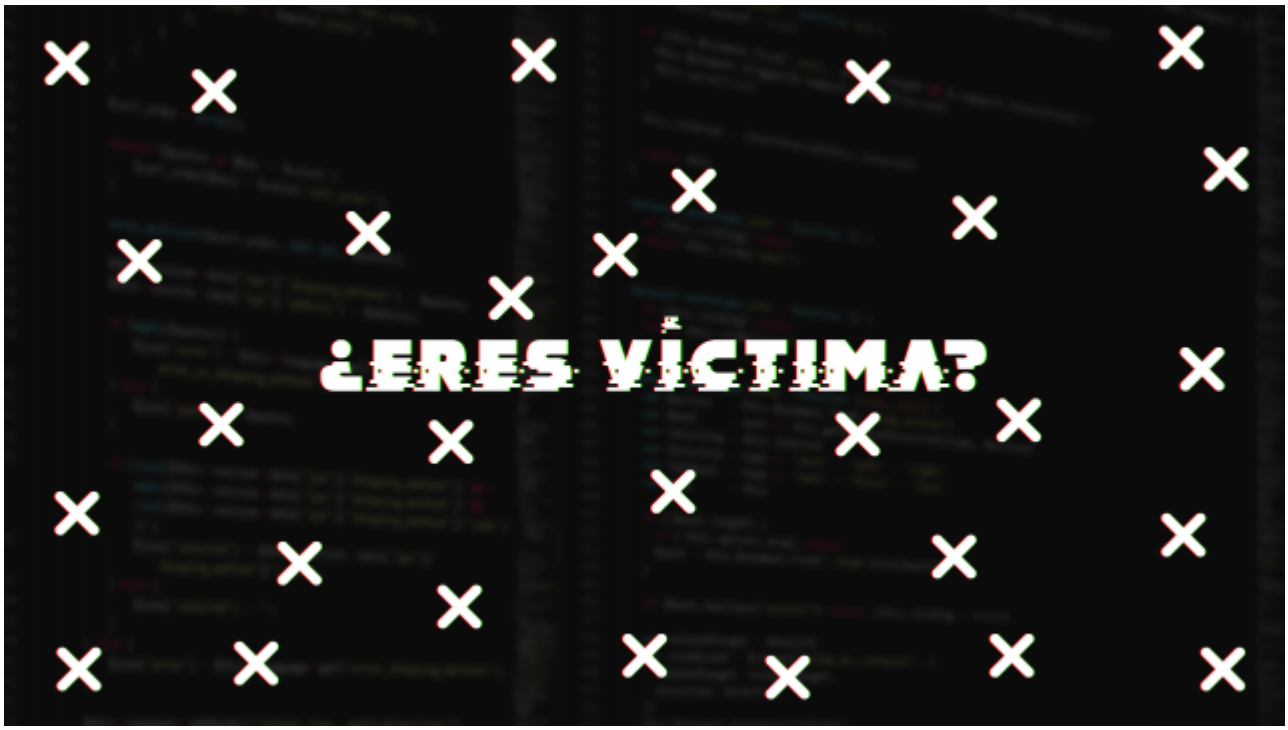
los ataques de ransomware basados en exploits no pueden perjudicarlo. En esa nota, si su negocio funciona con software obsoleto u obsoleto, entonces está en riesgo de ransomware, ya que los fabricantes de software ya no están publicando actualizaciones de seguridad. Desháguese de abandonware y reemplácelo con el software que aún es compatible con el fabricante.

Educa a tus usuarios finales en malspam y crea contraseñas seguras

Los ciberdelincuentes emprendedores detrás de Emotet están utilizando el antiguo troyano bancario como un vehículo de entrega de ransomware. Emotet confía en malspam para infectar a un usuario final y obtener un punto de apoyo en su red. Una vez en su red, Emotet muestra un comportamiento similar a un gusano, extendiéndose de un sistema a otro utilizando una lista de contraseñas comunes. Al aprender a detectar malspam e implementar la autenticación multifactor, sus usuarios finales estarán un paso por delante de los cibercriminales.
Invertir en una buena tecnología de ciberseguridad. Malwarebytes Endpoint Protection and Response, por ejemplo, le brinda capacidades de detección, respuesta y remediación a través de un agente conveniente en toda su red.

¿Qué haces si ya eres víctima de

ra



Nadie quiere lidiar con el ransomware después del hecho.

1. Compruebe y vea si hay un descifrador. En algunos casos excepcionales, puede descifrar sus datos sin pagar, pero las amenazas de ransomware evolucionan constantemente con el objetivo de hacer que cada vez sea más difícil descifrar sus archivos, así que no se fíe.
2. No pague el rescate. Durante mucho tiempo hemos abogado por no pagar el rescate y el FBI (después de un tiempo) está de acuerdo. Los cibercriminales no tienen escrúpulos y no hay garantía de que recupere sus archivos. Además, al pagar el rescate, está mostrando a los ciberdelincuentes que los ataques de ransomware funcionan.

Otros recursos del blog para complementar esta información de malware: ¿Ransomware puede afectar a servidores web Linux ?; Ransomware, mejores prácticas para prevenir daños irrecuperables; Ransomware en Windows server, características y patrones de ataque, qué hacer