Desglose de la cadena de exterminio del ransomware

Cinco pasos para bloquear el movimiento lateral

El ransomware no se propaga con el ataque a un solo equipo o dispositivo. Los ciberdelincuentes utilizan esta cepa de malware para cifrar el mayor número posible de sistemas de una red y asegurarse de que las víctimas paguen el rescate.

Cada 2 segundos

Se prevé que para 2031 el ransomware ataque a una empresa, un consumidor o un dispositivo cada dos segundos.

Cybersecurity Ventures Ransomware Market Report

¿Confía en su seguridad de red actual?

Si confía en los firewalls heredados para la segmentación, no podrá evitar que el ransomware se extienda por su red y bloquee las aplicaciones e infraestructuras fundamentales.

Cadena de exterminio del ransomware

1. **Acceso inicial**
   (Spear) Phishing o servicios vulnerables
2. **Movimiento lateral**
   Difusión por la red para lograr el mayor impacto posible
3. **Exfiltración**
   Búsqueda y robo de datos valiosos
4. **Cifrado**
   PKI para cifrado para evitar grietas
5. **Extorsión**
   Fondo de pantalla, correo electrónico, archivo .txt de rescate, etc.
6. **Impacto**
   Datos, financiero, reputación, etc.

Las filtraciones son inevitables

Necesita una solución de seguridad que sea capaz de detectar amenazas en el tráfico este-oeste del centro de datos y bloquear el movimiento lateral.

Rompa la cadena

Preparación mediante la identificación de todas las aplicaciones y activos que se ejecutan en su entorno de TI

Prevención mediante la creación de reglas para bloquear las técnicas más comunes de propagación de ransomware

Detección mediante la recepción de alertas sobre cualquier intento de obtener acceso a las aplicaciones segmentadas y las copias de seguridad

Corrección mediante la activación de medidas de cuarentena y contención de amenazas cuando se detecta un ataque

Recuperación mediante capacidades de visualización con estrategias de recuperación por fases

En 2022, los ataques de ransomware aumentaron casi un 13 %, un aumento tan grande como el de los últimos cinco años combinados.

Informe de 2022 de investigación sobre filtración de datos de Verizon

Si no está preparado para defenderse de ataques más frecuentes y extorsiones más costosas, ahora es el momento de incorporar la segmentación y la visibilidad a su estrategia de defensa.

Más información