En resumen

Beneficios

- **Reduzca el riesgo** de infecciones de ransomware con una seguridad que pueda bloquear amenazas antes de que intenten instalarse.
- **Una protección inmediata** contra ransomware le permite mantenerse enfocado en llevar adelante su empresa.
- **Las defensas integradas y por capas** le otorgan una visibilidad y capacidad de respuesta inigualable de la capa DNS, pasando por la red, al terminal.
- **Segmentación dinámica** para mantener el ransomware acorralado en la red.
- **La inteligencia líder en la industria** es suministrada por el grupo de investigación e inteligencia de seguridad Cisco Talos.

Cisco Ransomware Defense

El auge del ransomware

El ransomware es software malicioso o malware que cifra la información en la computadora de un individuo, como ser documentos, fotografías y música. No liberará estos archivos hasta que el usuario pague una suma (o rescate) para desbloquearlos y recuperarlos.

El ransomware se convirtió rápidamente en el tipo más rentable de malware jamás visto, y va camino a convertirse en un mercado de USD 1000 millones anuales.

Generalmente se infiltra en una computadora o red a través de la web o el correo electrónico. En un sitio web, el ransomware puede infiltrarse a través de anuncios infectados que pueden propagar malware, conocidos como “publicidad maliciosa”. Los usuarios navegan en sitios con anuncios maliciosos que descargan malware automáticamente o los redirige a equipos de ataque. En el correo electrónico, el ransomware utiliza suplantación de identidad o mensajes de correo electrónico no deseado para infiltrarse. Los usuarios solo tienen que hacer clic en enlaces en correo electrónico no deseado o de suplantación de identidad, o abrir archivos adjuntos para que el ransomware se descargue y se comunique con su servidor de comando y control.

El ransomware también puede tomar el control de sistemas utilizando kits de ataque. Los kits de ataque son kits de software diseñados para identificar vulnerabilidades del software en sistemas finales. Luego, cargan y ejecutan un código malicioso, como ransomware, en los sistemas vulnerables.

En el futuro, el ransomware no solo apuntará a usuarios individuales, sino también a redes enteras. Con más métodos semiautomáticos de propagación, los creadores de ransomware aprovecharán las oportunidades de penetrar en una red y moverse lateralmente para controlar sectores de la red para maximizar el impacto y la probabilidad de recibir el pago.

Reduzca el riesgo de ransomware con una seguridad más eficaz

Dado que el ransomware puede infiltrarse en organizaciones de varias maneras, reducir el riesgo de infecciones de ransomware requiere un enfoque basado en una cartera, en lugar de un solo producto. El ransomware se debe evitar siempre que sea posible, y se lo debe detectar si obtiene acceso a sistemas y contener para limitar daños.

Cisco® Ransomware Defense aplica la arquitectura de seguridad de Cisco para proteger empresas mediante defensas que abarcan desde redes, pasando por la capa DNS y el correo electrónico, hasta el terminal. Está respaldado por las investigaciones líderes de amenazas de Talos por la última capacidad de respuesta con ransomware.

“Hemos cubierto un gran riesgo en el vector de ataque de red de ransomware, y hemos mejorado significativamente nuestra experiencia de usuario con respecto a conectividad a Internet”

Octapharma

La solución comprende los siguientes componentes:

- **Cisco Umbrella** protege los dispositivos dentro y fuera de la red corporativa. Bloquea las solicitudes DNS antes de que un dispositivo siquiera pueda conectarse a sitios maliciosos que alojan ransomware.
- **Cisco Advanced Malware Protection (AMP) para terminales** evita que los archivos de ransomware se ejecuten en terminales.
- **La seguridad de correo electrónico de Cisco con Advanced Malware Protection (AMP)** bloquea correos electrónicos no deseados y de suplantación de identidad y adjuntos de correo electrónico y URL maliciosos. La tecnología AMP es la misma que la que se aplica en el terminal, pero se implementa en la gateway de correo electrónico.
- **El firewall de próxima generación Cisco FirePOWER** con Advanced Malware Protection (AMP) y la tecnología de sandboxing Threat Grid bloquea las amenazas y rellamadas de comando y control conocidas a la vez que proporciona análisis dinámico de malware y amenazas desconocidos.
- **Cisco ISE a través de la red de Cisco** para segmentar su red en forma dinámica, de manera que el acceso a los servicios y las aplicaciones permanezca muy seguro y el ransomware no pueda propagarse lateralmente.
- **Los servicios de seguridad de Cisco** proporcionan una clasificación inmediata en el caso de respuesta ante los incidentes. También optimizan las implementaciones de AMP, NGFW y demás productos de la solución.

Próximos pasos

Mantenga su negocio enfocado en lo mejor que puede ofrecer entrando en contacto con su representante de ventas de Cisco para obtener más información sobre Cisco Ransomware Defense.

C45-737465-00 07/16