Cisco Ransomware Defense: Mantenga al ransomware acorralado

Imagine poder mantenerse más a salvo del ransomware, sin importar cuánto intente ingresar. Solo Cisco le ofrece los productos de seguridad y la arquitectura para lograrlo.

Descripción general

Los archivos y la información son el alma de una organización. Mantener esta información (y la productividad de su organización) intactas y seguras no es negociable.

No obstante, puede aparecer ransomware, software malicioso o malware, los cuales bloquean la información en la computadora de un individuo o una organización, como ser documentos, fotografías y música. No liberará estos archivos hasta que el usuario pague una suma (o rescate) para desbloquearlos y recuperarlos. Sin las defensas adecuadas, el ransomware puede causar daños suficiente como para limitar a una organización a operar con bolígrafo y papel.

El ransomware generalmente se envía través de kits de ataque, publicidad maliciosa (anuncios infectados en un sitio web que pueden contener malware), suplantación de identidad (correos electrónicos fraudulentos que se camuflan como confiables), o campañas de correo electrónico no deseado. La infección puede producirse cuando alguien hace clic en un enlace o un archivo adjunto en correos electrónicos de suplantación de identidad. Las infecciones también pueden producirse cuando los usuarios navegan en sitios con anuncios maliciosos que infectan automáticamente las computadoras.

Ingrese en Cisco® Ransomware Defense. Reduce el riesgo de infecciones de ransomware mediante un enfoque por capas, de la capa DNS, pasando por el terminal, a la red, el correo electrónico, y la web. Ofrecemos defensas integradas con un enfoque arquitectónico que combina máxima visibilidad con máxima capacidad de respuesta contra el ransomware.

Beneficios

- **Reduzca el riesgo de ransomware** para poder enfocarse en llevar adelante su empresa
- **Obtenga protección inmediata** con una seguridad que pueda bloquear amenazas antes de que intenten instalarse
- **Obtenga una visibilidad y capacidad de respuesta inigualable** desde un enfoque arquitectónico de la capa DNS, pasando por la red, al terminal
- **Evite que el malware se propague lateralmente** con una sólida segmentación de la red
- **Obtenga investigación de amenazas e inteligencia líderes** en ransomware de Talos

Una amenaza potente y de rápido crecimiento

Éste es el año del ransomware. Y está demostrando ser muy rentable. El ransomware se convirtió rápidamente en el tipo más lucrativo de malware jamás visto.

El FBI afirmó que está camino a convertirse en un mercado anual de USD 1000 millones. La investigación de Cisco Talos muestra que una sola campaña de ransomware puede generar hasta USD 60 millones por año. El ransomware está ganando tanta atención que ya se difundió en programas de televisión.

Los atacantes tienen los fondos y desean continuar innovando en cepas de ransomware que serán mucho más virulentas. Creemos que el ransomware contará con una mayor capacidad de autopropagación, con el objetivo de bloquear extensas redes corporativas. Esto lograría enviar la funcionalidad corporativa de TI nuevamente a la década de 1970.

Las respuestas actuales al ransomware suelen basarse en productos de punto sencillo. Debemos considerar la implementación de un enfoque más arquitectónico, dados los diversos vectores a los que apunta para poder infectar.

Esta descripción general de la solución aborda los diferentes métodos y vectores que utilizan los atacantes. Los defensores deben garantizar la seguridad del correo electrónico y la web, bloquear el acceso a infraestructura maliciosa en Internet, impedir el ingreso de cualquier archivo de ransomware que penetre hasta un terminal, bloquear las rellamadas de comando y control utilizadas y evitar fácilmente el movimiento lateral de ransomware, de producirse una infección.

Qué compra:

Cisco Ransomware Defense reúne todas las piezas necesarias de la arquitectura de seguridad de Cisco para abordar el desafío de ransomware. Puede elegir todas las piezas o seleccionar aquellas que cumplan con una necesidad de seguridad inmediata.

Ransomware Defense comprende:

- Cisco Umbrella, el cual bloquea amenazas en la capa DNS, lejos de su red
- Cisco Advanced Malware Protection (AMP) para Terminales, el cual evita que se ejecuten archivos de ransomware malicioso en los terminales.

- Seguridad de correo electrónico de Cisco, tanto en la nube como en las instalaciones, la cual evita que los mensajes no deseados y de suplantación de identidad intenten enviar ransomware
- Advanced Malware Protection se puede agregar inmediatamente a productos de seguridad de correo electrónico mediante una licencia sencilla para el análisis estático y dinámico (sandboxing) de adjuntos desconocidos que atraviesan la gateway de Seguridad de correo electrónico de Cisco
- Firewall de próxima generación (NGFW) de Cisco Firepower™, el cual impide que el tráfico de comando y control, como también cualquier archivo malicioso, penetren la red
- Cisco ISE, a través de la red Cisco divide su red en forma dinámica, para que el ransomware no pueda propagarse lateralmente

Con Ransomware Defense, las organizaciones pueden usar su red como guardián para contener la propagación de ransomware. No será capaz de propagarse tan fácilmente en la red en el peor de los casos de que se produzca una infección.

Los servicios de seguridad de Cisco pueden proporcionar una clasificación inmediata en caso de respuesta ante los incidentes después de un ataque. También optimizan las implementaciones de AMP, NGFW y demás productos de la solución.

Capacidades clave

- Evite que el ransomware ingrese a la red o se descargue en PC portátiles
- Contenga el ransomware en los peores escenarios, cuando éste ingresa a la red

Los servicios de seguridad ayudan a combatir el ransomware

El equipo de respuesta ante los incidentes de los servicios de seguridad de Cisco puede brindar servicios de preparación de respuesta ante incidentes y respuesta reactiva ante incidentes en caso de ataques de ransomware.

Asimismo, los servicios de integración de seguridad de Cisco abordan desafíos arquitectónicos al nivel de la solución. Optimiza la implementación de tecnologías de solución, como ser, AMP para terminales y NGFW Cisco FirePOWER. Nuestro equipo tiene una vasta experiencia en entregar soluciones de seguridad integrada para agilizar la adopción de la tecnología de seguridad necesaria con poca interrupción.

En términos generales, las organizaciones también deben asegurarse de contar con la tecnología de copias de seguridad y las políticas adecuadas para protegerse contra los impactos de una infección de 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

Cisco Capital

Financiación para ayudarlo a alcanzar sus objetivos

La financiación de Cisco Capital® puede ayudarlo a adquirir la tecnología que necesita para alcanzar sus objetivos y mantener la competitividad. Podemos ayudarlo a reducir los gastos de capital. Acelere su crecimiento. Optimice sus inversiones monetarias y el ROI. La financiación de Cisco Capital le brinda flexibilidad en la adquisición de hardware, software, servicios y equipos complementarios de terceros. Y hay un solo pago previsible. Cisco Capital está disponible en más de 100 países. Más información.

La ventaja que ofrece Cisco

El ransomware encontrará una forma de penetrar su organización valiéndose de cualquier medio necesario. Correos electrónicos de suplantación de identidad, anuncios comprometidos de la web – muchos vectores necesitan protección. Solo Cisco ofrece una arquitectura de seguridad para abordar el desafío de ransomware. Los productos puntuales no son suficientes. Nuestra solución está respaldada por nuestro Grupo de Investigación Talos, líder en la industria, el cual realizó una investigación exhaustiva de amenazas de ransomware, alimentando así nuestra efectiva protección por capas. Bloquearemos el ransomware e incluso lo combatiremos si penetra a través de las grietas y se infiltra en su red, lo cual puede ser muy desafortunado.

C22-737492-01 08/16