Cisco Ransomware Defense

Los ataques son cada vez más sofisticados y recurrentes

Actualmente, los hackers disponen de recursos ilimitados para operar sin límite, aprovechando las vulnerabilidades que las organizaciones y usuarios finales pueden tener. Estos ataques, pueden permanecer activos e inadvertidos durante días, meses o incluso más tiempo. Los defensores, mientras tanto, se enfocan en obtener visibilidad de la actividad en torno a las amenazas y reducir el tiempo de detección (TTD) de las amenazas nuevas y conocidas.
Se están realizando grandes progresos, pero aún hay mucho por recorrer para debilitar verdaderamente la capacidad de los adversarios en sentar las bases para realizar ataques, a fin de contrarrestarlos con un impacto alto y rentable.

Un nuevo malware

El ransomware viene tomando impulso y dominando el mercado desde el 2015, apoderándose de muchos documentos e información relevante que no serán liberados hasta que el usuario pague una suma de dinero para desbloquearlos y recuperarlos.
Este malware se está convirtiendo en uno de los más rentables jamás visto, y va en camino a convertirse en un mercado de USD 1 billón anuales, según el FBI. Sin las defensas adecuadas en la red, el ransomware puede causar grandes daños, al punto de limitar las operaciones de una organización por un tiempo prolongado.

¿Cómo puede ingresar el malware a las redes de su organización?

Correo electrónico
Mensajes de suplantación de identidad y correo electrónico no deseado con enlaces o adjuntos maliciosos.

Servidores Web
Puntos de ingreso para acceso a la red.

Web 2.0
Archivos cifrados propagados por redes sociales y mensajería instantánea.

Publicidad maliciosa
Descargas desapercibidas a través de un sitio confiable infectado.

La evolución del Ransomware

En octubre de 2016 el mundo entero fue víctima de alrededor de 10 tipos de Ransomware nuevos y casi 5 variantes, los mismos con capacidades de propagación más avanzados.

En función de las tendencias y los avances observados a la fecha, los investigadores de seguridad de Cisco, anticipan que la autopropagación del ransomware será el siguiente paso para los innovadores en el área, quienes asesorarán a los usuarios para que puedan tomar medidas en su seguridad y estar preparados frente a estos ataques.

La autopropagación de malware no es algo nuevo. De hecho, viene implementándose desde hace décadas en la forma de gusanos. Muchas de estas amenazas aún son dominantes y siguen siendo eficaces.

Las características de la autopropagación del malware pueden incluir lo siguiente:

- **Tomar ventaja de la vulnerabilidad de un producto popular:** Con el tiempo, se ha detectado que los gusanos exitosos se filtraban en las vulnerabilidades de productos que habían sido implementados a través de Internet.
- **Replicarse en dispositivos y redes disponibles:** Los malware detectan los dispositivos locales y remotos y se autocopian en dichas unidades, así logran persistir en el tiempo. Esto permite la infección de sistemas sin conexión y de sistemas no accesibles mediante Internet pública.
- **Infecciones de archivos:** El malware se añade a ejecutables que no están protegidos mediante el comprobador de archivos de sistema (SFC) o el Protector de archivos de Windows (WFP) de Windows. Algunos gusanos pueden autoañadirse a archivos no ejecutables y propagarse a través de estos.
- **Comando y control resistentes:** Algunos gusanos tienen registrados los movimientos de cada usuario para interrumpir la infraestructura de comando y control, e implementan medidas preventivas para evitar dichas interrupciones.
- **Uso de otras puertas traseras:** Algunos creadores de malware, conscientes de haber logrado que otras infecciones hayan tenido impacto en un sistema, aprovechan esas puertas traseras para propagar su malware en la red y llevan a cabo el ataque.

Para defenderse de este malware, se necesita una solución integral de seguridad en sus redes. Cisco le ofrece una arquitectura completa e integrada que logra mitigar al mínimo el riesgo, logrando acercarse al 100% de prevención contra este tipo de ataques, protegiendo cada una de las capas más vulnerables.

> "En función de las tendencias y los avances observados a la fecha, los investigadores de seguridad de Cisco anticipan que la auto-propagación del ransomware será el siguiente paso para los innovadores en el área y exhortan a los usuarios a tomar medidas ahora para estar preparados".
>
> Informe semestral de Ciberseguridad 2016 - Cisco

Soluciones destacadas

> Cisco Ransomware Defense

Reduce el riesgo de ataques mediante un enfoque por capas, desde la capa DNS, pasando por el dispositivo, la red, el correo electrónico y la web. Ofrecemos defensas integradas con un enfoque arquitectónico que combina máxima visibilidad y capacidad de respuesta contra el ransomware.

Beneficios obtenidos

Reduzca el riesgo de infecciones de ransomware bloqueando amenazas antes de que intenten instalarse.

Las defensas integradas y por capas le otorgan una visibilidad y capacidad de respuesta inigualable desde el DNS al EndPoint.

La inteligencia líder en la industria es suministrada por el grupo de investigación e inteligencia de seguridad Cisco Talos.

Una protección inmediata le permite mantenerse enfocado en llevar adelante su empresa.

Segmentación dinámica para tener el ransomware acorralado en la red.

Productos destacados

Cisco Ransomware Defense reúne todos los componentes necesarios para abordar el desafío de ransomware. Puede elegir todos los componentes o seleccionar aquellas que cumplan con una necesidad de seguridad inmediata para sus negocios.

> Protección de Malware Avanzado (AMP)

Inteligencia global de amenazas

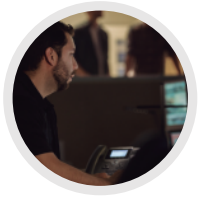
La inteligencia AMP se basa en los estudios realizados por el equipo de expertos de Cisco Talos, quienes analizan millones de muestras de malware y crean soluciones para ello. AMP correlaciona archivos, datos de telemetría y el comportamiento de los archivos, así podrá brindar una defensa proactiva contra amenazas conocidas y emergentes con esta base de conocimientos e información contextual.

Sandboxing avanzado

Se realizan análisis estáticos y dinámicos automatizados de archivos con respecto a más de 700 indicadores de comportamiento, cuyo objetivo es descubrir las amenazas furtivas. De esta manera, el equipo de seguridad puede entender, priorizar y bloquear los ataques sofisticados.

Detección y bloqueo puntuales de malware

Bloquee el malware que intenta entrar en su red en tiempo real con AMP, el cual utiliza diversas técnicas de entrada (motor antivirus, patrón de firmas, huella digital del archivo y mecanismos de inteligencia artifical). AMP analiza los archivos en el ingreso para detectar el malware conocido y desconocido, permitiendo detectar y proteger el ataque en menos tiempo y de forma automática.



Análisis continuos y seguridad retrospectiva

Una vez que un archivo ingresa a la red, AMP hace un seguimiento de éste, supervisando, analizando y registrando las actividades que realiza. Si detecta un comportamiento malicioso posteriormente, AMP envía un alerta retrospectiva al equipo de seguridad donde se le indica el lugar de origen y cómo se está desarrollando para poder contenerlo y corregirlo de una forma muy rápida.

100%

Detección líder de vulnerabilidades

Fuente: NSS Labs

Cisco
-13 horas

SECTOR
-100 DÍAS

Tiempo de detección

Fuente: Informe semetral sobre ciberseguridad 2016

1,5
MILLONES

Muestra de malware por día

Fuente: Grupo de investigación e inteligencia de seguridad Cisco Talos

Productos destacados

> Cisco Umbrella

Medio de seguridad que protege a los empleados que se encuentren dentro y fuera de la VPN. Bloquea las solicitudes DNS antes de que un dispositivo pueda conectarse a sitios maliciosos. Obtendrá una protección continua contra malware, suplantación de identidad y devoluciones de llamadas de comando y control donde sea que sus usuarios vayan. Lo único que se necesita para obtener una protección continua es habilitar la funcionalidad integrada en Cisco AnyConnect.

> Cisco Cloud Email Security (CES)

Ofrece protección al correo electrónico frente a las amenazas constantes y dinámicas que afectan la información del correo electrónico. La solución, también ofrece una constante actualización de los avances que se dan en la industria gracias a los estudios de Cisco Talos. Cisco Cloud Email Security, está disponible con la nueva versión de Office 365.

> Cisco FirePower - Firewall de próxima generación (NGFW)

Logre bloquear más amenazas y mitigue en el menor tiempo posible aquellas que traspasen sus defensas con NGFW centrado en amenazas del sector, combinando el firewall Cisco de red probado con el sistema de prevención de NGIPS, la protección avanzada contra el malware de día cero y filtrado URL. Logrando obtener mayor visibilidad, flexibilidad, ahorro y mejor protección de su red.

> Stealthwatch

StealthWatch es líder de visibilidad de red para defenderse de las amenazas avanzadas. Mediante la recopilación y el análisis de NetFlow, Sflow, IPFIX y otros tipos de datos de flujo, convertimos la red en un sensor de monitoreo y seguridad, así ayudamos a detectar rápidamente una amplia gama de ataques: APT, DDoS, Malware de día cero, amenazas internas, comportamientos sospechosos, ex filtración de datos así como proveer visibilidad de amenazas en la capa de acceso, distribución, core y borde.

Logre los siguientes beneficios con Stealthwatch:

- ✔ Detecte amenazas en tiempo real
- ✔ Respuesta ante incidentes e informática forense
- ✔ Segmentación de la red
- ✔ Planificación de la capacidad y rendimiento de la red
- ✔ Cumplimiento reglamentario

> Cisco ISE – Identity Services Engine

Obtenga una plataforma de administración de políticas de seguridad que automatiza y aplica a los recursos de la red acceso de seguridad sensible al contexto. Cisco ISE, ofrece una visibilidad superior de los usuarios y dispositivos para respaldar experiencias de movilidad empresarial y controlar el acceso. Comparte datos con soluciones integradas de partners para acelerar sus funcionalidades de identificación, mitigación y corrección de amenazas.

1. PREVENCIÓN RÁPIDA BASADA EN LA NUBE | Prevención y protección de e-mail, web y endpoints. Logre detener las amenazas antes que el malware ingrese a su red.

Umbrella bloquea la solicitud

NGFW bloquea la conexión

E-mail Security con AMP, bloquean el e-mail

Umbrella bloquea la solicitud

NGFW bloquea la conexión

AMP para dispositivos, bloquea el archivo malicioso

Umbrella bloquea las solicitudes de llaves a las infraestructuras PKI de los atacantes

Cisco Umbrella + **Next-Gen Firewall (NGFW)** + **Cloud E-mail Security (CES)** + **AMP para Endpoints**

Proteja sus dispositivos que se encuentran dentro y fuera de la VPN, bloqueando las solicitudes DNS antes de conectarse a sitios maliciosos.

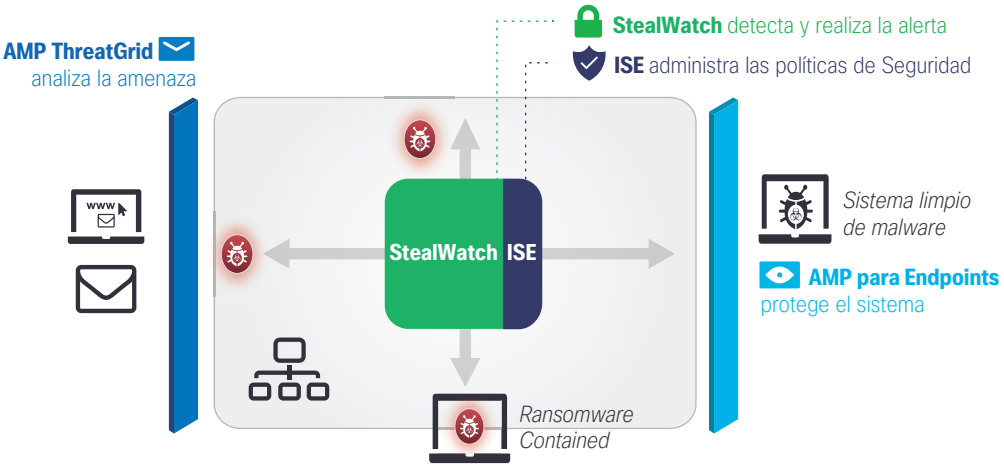
Logre bloquear las amenazas y solucionar las infecciones en el menor tiempo posible.

Protéjase ante amenazas que pueden llegar a través de un correo electrónico e infectar toda su información.

⚠ Versión disponible con el Office 365.

Realice una defensa proactiva contra amenazas conocidas y emergentes, utilizando información contextual en sus dispositivos.

2. PREVENCIÓN AVANZADA | Detección y contención del ransomware dentro de la red para detener su propagación y evitar la exfiltración de datos y afectación de servicios.



AMP ThreatGrid + **StealthWatch** + **ISE** + **AMP de dispositivos**

Realice un análisis dinámico (sandboxing) sobre los archivos recibidos.

Identifique las amenazas, analizando el comportamiento del tráfico de la Red.

Logre una orquestación centralizada de las políticas de control de acceso seguro a la red.

Realice una defensa proactiva contra amenazas conocidas y emergentes, utilizando información contextual en sus dispositivos.

> Servicios Técnicos

Cisco Threat Management Service

Servicio de inteligencia de amenazas basado en un portal de fácil uso. Aumenta la visibilidad de las amenazas para los clientes de *Smart Net Total Care (SNTC)*, ya que el usuario tiene acceso las 24 horas del día a la información básica de seguridad.

Conozca los beneficios:

- ✓ Permite detectar en forma oportuna las actividades maliciosas en función de la experiencia de inteligencia de amenazas y de visibilidad de la extensa red de Cisco.
- ✓ Ayuda a las empresas a identificar rápidamente los sistemas comprometidos mediante la implementación de marcas en dichas redes y comportamientos sospechosos.
- ✓ Ayuda a los equipos de seguridad y TI a reconocer las amenazas y brinda inteligencia procesable.
- ✓ Posibilita la mejora continua del estado general de seguridad mediante el análisis del tráfico de red desde fuera de ella.

> Servicios de Consultoría de Seguridad

Respuesta ante Incidentes

Si su organización está experimentando un incidente de cyberseguridad, desde una exfiltración de datos confidenciales hasta un ataque que puede impactar en la operaciones de su empresa, Cisco Security Incident Response Services puede ayudarlo a lograr una rápida detección del problema para detener el ataque, responder ante el incidente y crear una estrategia a largo plazo para controlar el problema desde el punto cero.

El servicio de Cisco se basa en inteligencia de última generación frente a incidentes, años de experiencia y mejores prácticas realizadas. El equipo especializado primero seleccionará la situación, después lo ayudará a construir un plan de respuesta personalizado para poder identificar al atacante, conocer el alcance del ataque, determinar su causa y así logrará que la empresa pueda recuperar su información lo más rápido posible.

Acceso inmediato a incidentes calificados, dando respuestas en base a las experiencias obtenidas con diferentes tipos de ataque.

Mayor confianza en los resultados de las respuestas a través de metodologías probadas con inteligencia y un equipo existoso.

Acceso completo a las herramientas de Cisco durante el incidente. Una mayor visibilidad, rapidez y comprensión más amplia de todas las amenazas en la red.

Evaluación del programa de seguridad

Como asesor estratégico y técnico, los servicios de consultoría de Cisco lo ayudan a identificar las oportunidades fundamentales en materia de seguridad de la información para proteger el rendimiento, crear ventaja competitiva y capturar el valor comercial sostenible a largo plazo. Asimismo, lo ayudamos a comprender, definir, priorizar y mitigar los riesgos para aprovechar al máximo sus inversiones.

- Conozca cómo utilizar la nube y los servicios móviles para incorporarlos a su estrategia de negocio.
- Aprenda a implementar un nuevo servicio en la nube.
- Analice la viabilidad de su estrategia de seguridad existente.

Logre identificar y mitigar las vulnerabilidades, creando una línea de base de riesgo y encontrando soluciones para reducir o eliminar los riesgos inaceptables.

Entienda y administre las inseguridades de terceros para equilibrar los riesgos y la oportunidad.

Cumpla el ISO: ya sea su primer intento para obtener la certificación o si solo quiere mantener los requisitos de generación de informes.

Evaluación de diseño de seguridad de la red

Si el objetivo es construir una sólida defensa para la red de la empresa, es necesario conocer primero cuál es su estado actual. El diseño y la implementación de una solución de defensa de varias capas requieren algo más que solo conocer los productos de seguridad y las prácticas principales. Es indispensable entender cómo es la infraestructura de red sobre la que funcionan las soluciones de seguridad.

Cisco Security Advisory Services asesora técnica y estratégicamente a las organizaciones líderes y a los equipos de ejecutivos para que puedan:

- Identificar las mejores oportunidades en materia de seguridad de la información para proteger el rendimiento del negocio.
- Crear una ventaja competitiva y capturar el valor comercial sostenible a largo plazo.

Respaldados por una combinación inigualable de recursos, extensa investigación e inteligencia de amenazas, metodologías maduras y expertos en diversas disciplinas de operaciones de seguridad, nube, movilidad, colaboración y centro de datos, nuestros clientes administrarán mejor el riesgo y el cumplimiento al controlar el costo, y así podrán alcanzar sus objetivos estratégicos.

Cree una arquitectura de seguridad sólida y escalable mediante un enfoque de prevención de riesgos ideal para negocios.

Logre correlacionar los datos sobre las vulnerabilidades con la información de la topología de red e identifique los riesgos que representan para las redes y los recursos críticos.

Mejore del cumplimiento de las regulaciones y las obligaciones del sector, identificando los controles internos necesarios para proteger mejor los datos confidenciales.

Oficinas locales

» Cisco Costa Rica

Centro Corporativo Plaza Roble
Edificio Los Balcones A, Primer Nivel
Escazú, Costa Rica

Tel: +506 2201-3600
Preventas: 2519-6767

» Cisco Panamá

Edificio World Trade Center
Piso 17, Oficina 1701, Área Comercial
Marbella, República de Panamá

Tel: +507 265-4040
Preventas: 001-800-507-3649

» Cisco República Dominicana

Torre Piantini, Piso 5, Local 5OA
Ensanche Piantini
Santo Domingo

Tel: +1 888-156-1464 Ext. 6214 Preventas:
1-888-751-9317

» Cisco Puerto Rico y Bermuda

Parque Las Américas 1
235 Calle Federico Costa. Oficina 415
San Juan, Puerto Rico. 00918-1912

Puerto Rico: +787 620-1888
Bermuda: 1-877-841-6599 Ext 6214
Preventas: 866-441-8405

» Cisco Venezuela

Avenida La Estancia, Centro Banaven,
Torre C, Piso 7, Chuao
Caracas, Distrito Federal 1064A

Tel: +58 212 9020221
Preventas: 0800-100-4573

» Cisco Perú

Av. Víctor Andrés Belaunde 147,
Vía Principal 123, Edificio Real Uno,
Piso 13, San Isidro, Lima

Tel: +511 215-5100
Preventas: 0800-54927

» Cisco Ecuador

Eurocenter Diursa Building, Piso 6
Avenida Amazonas 37-29 entre
Villalengua y UNP, Quito, Pichincha

Tel: +593 2397-8700

» Oficina Regional Cisco Latinoamérica

8200 NW 41st Street, Suite 400
Miami, Florida 33166-6204

Phone: 305-718-2600

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**