Comprender la protección frente a malware y spyware de los dispositivos web seguros

Contenido

Introducción

En este documento se describen las completas funciones de protección frente a software malicioso y software espía de Cisco Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Cisco SWA se ha diseñado para ofrecer mecanismos de defensa de gateway sólidos y completos frente a un amplio espectro de spyware y malware basado en la Web. Combate de forma eficaz amenazas que van desde el adware, que es conocido por causar una fuga de recursos de red significativa y desafíos de compatibilidad, hasta amenazas más graves, como troyanos, secuestradores de navegadores, objetos de ayuda del navegador, suplantación de identidad, pharming, monitores del sistema, registradores de teclas y gusanos.

Diferenciadores clave de los SWA

Monitor de tráfico de capa 4 integrado (L4TM)

El monitor de tráfico L4 es capaz de analizar todos los puertos de red (65 535 en total) a velocidad de cable, lo que garantiza una detección y un bloqueo exhaustivos del malware y los intentos de comunicación no autorizados. Esta funcionalidad impide de forma eficaz que el malware intente eludir los puertos habituales, como los puertos 80 y 443, y también suprime las actividades de comunicación punto a punto (P2P) y de chat de retransmisión de Internet (IRC) desconocidas.

Procesamiento de la capa de proxy

El SWA incorpora un proxy web de alto rendimiento con almacenamiento en caché integrado y capacidades de aceleración de contenido. Con la tecnología AsyncOS propiedad de Cisco, este proxy web puede gestionar hasta diez veces más conexiones que los servidores proxy basados en UNIX convencionales. Como proxy web, facilita una inspección exhaustiva del contenido en la capa de aplicaciones, lo que resulta esencial para una defensa precisa frente al malware basado en la Web.

Filtros de reputación de Web

A medida que los filtros de reputación web pioneros en el sector, estos proporcionan una capa adicional de defensa. Utilizando SenderBase®, estos filtros evalúan más de 50 parámetros de tráfico web y relacionados con la red para determinar la fiabilidad de una URL. Se emplean técnicas avanzadas de modelado de seguridad para asignar pesos individuales a cada parámetro, lo que culmina con una puntuación de reputación que oscila entre -10 y +10. Las políticas configuradas por el administrador se adaptan dinámicamente en función de estas puntuaciones.

Motor de transmisión y vectorización dinámica (DVS)

El motor DVS introduce un análisis de firmas acelerado en el SWA, que se diferencia de las arquitecturas heredadas que dependen del protocolo de adaptación de contenidos de Internet (ICAP) y de las implementaciones de varios paquetes para el análisis de malware. Esta plataforma de vanguardia utiliza sofisticadas técnicas de vectorización, análisis de flujos y

almacenamiento en caché de veredictos, lo que permite multiplicar por diez el rendimiento del análisis en comparación con las soluciones basadas en ICAP de primera generación.

Sistema anti-malware de Cisco

Este sistema aprovecha el motor DVS junto con varios tipos de firmas procedentes de Webroot, lo que ofrece una protección incomparable frente a una amplia gama de amenazas basadas en la Web. El espectro de amenazas incluye adware, secuestradores de navegadores, suplantación de identidad (phishing), ataques de pharming y más entidades maliciosas como troyanos, monitores de sistemas y registradores de teclado. SWA cuenta con la base de datos de firmas de malware más grande del sector en el gateway, lo que garantiza una protección completa.

Por tanto, el dispositivo de seguridad Cisco Web Security Appliance se posiciona como líder en la protección de gateways de red frente a una amplia gama de amenazas basadas en la Web, lo que garantiza una protección sólida y un rendimiento de red de alto rendimiento.

Información Relacionada

- Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).