Descripción general de Cisco Web Reputation de WSA

Contenido

Introducción

Este documento proporciona una descripción general de Cisco Web Reputation (WBRS) para Cisco Web Security Appliance (WSA).

Contribuido por Josh Wolfer y Stephan Fiebrandt, Ingenieros del TAC de Cisco.

Descripción general de WBRS

WBRS es un método innovador que analiza el comportamiento y las características de un servidor Web y proporciona la última defensa en la lucha contra el spam, los virus, la suplantación de identidad y las amenazas de spyware.

WBRS utiliza análisis en tiempo real en un conjunto de datos amplio, diverso y global para detectar las URL que contienen algún tipo de malware. WBRS es una parte esencial de la base de datos de seguridad de Cisco, que protege a los clientes de amenazas combinadas del tráfico web o del correo electrónico.

Uso de WBRS de SenderBase

WBRS aprovecha los datos de Cisco Common Security Database (SenderBase ® Network), que es la red de control de tráfico web y de correo electrónico más grande del mundo. Hace un seguimiento de más de 50 parámetros distintos que son indicadores excelentes de la reputación de una URL. Con sofisticados agentes de detección de malware y modelado de seguridad, Cisco evalúa estas URL basándose en estas entradas.

Algunos de los parámetros incluyen:

- Datos de categorización de URL
- Presencia de código descargable

- Presencia de contratos de licencia de usuario final (EULA) largos y confusos
- Volumen global y cambios en el volumen
- Información del propietario de la red
- Historial de una URL
- Antigüedad de una URL
- Presencia de virus / spam / spyware / phishing / lista(s) negra de pharming
- Tipos de URL de dominios populares
- Información del registrador de dominios
- información de dirección IP

Granularidad de WBRS

WBRS difiere de una lista negra de URL tradicional o una lista blanca porque analiza un amplio conjunto de datos y produce una puntuación granular de -10 a +10, en lugar de las categorías binarias **buenas** o **malas** de la mayoría de las aplicaciones de detección de malware. Esta puntuación granular ofrece a los administradores una mayor flexibilidad; se pueden implementar diferentes políticas de seguridad en función de diferentes rangos de puntuación de WBRS.