Contenido

Introducción

Este documento proporciona una descripción de la reputación Web de Cisco (WBRS) para el dispositivo de seguridad de la red de Cisco (WSA).

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

Descripción WBRS

WBRS es un método innovador que analiza el comportamiento y las características de un servidor Web y proporciona la última defensa de la lucha contra el Spam, los virus, el phishing, y las amenazas del spyware.

WBRS utiliza el análisis en tiempo real en un grupo de datos extenso, diverso, y global para detectar los URL que contienen una cierta forma de malware. WBRS es una parte crítica de la base de datos de seguridad de Cisco, que protege a los clientes contra las amenazas mezcladas del correo electrónico o del tráfico de la Web.

Uso WBRS de SenderBase

WBRS leverages los datos de la base de datos de la seguridad común de Cisco (red del ® de SenderBase), que es red el correo electrónico del mundo y de la supervisión de tráfico de la Web más grandes. Sigue sobre 50 parámetros distintos que sean indicadores excelentes de la reputación URL. Con los agentes sofisticados de la detección del modelado y del malware de la Seguridad, Cisco evalúa estos URL basados en estas entradas.

Algunos de los parámetros incluyen:

- Datos de la clasificación URL
- Presencia de código transferible
- Presencia de largo, acuerdos de licencia de usuario final ofuscados (EULA)
- Volumen y cambios en el volumen globales
- Información del titular de la red
- Historial de un URL
- Edad de un URL

- Presencia de virus/de Spam/de spyware/de listas negras del phishing/del pharming
- Errores tipográficos URL de los dominios populares
- Información del secretario del dominio
- Información de la dirección IP

Granularity WBRS

WBRS diferencia de una lista negra tradicional o de la lista blanca URL porque analiza a un conjunto de datos amplio y produce una calificación altamente granular de -10 a +10, en vez de las **buenas** o **malas** clasificaciones binarias de la mayoría de las aplicaciones de la detección del malware. Esta calificación granular ofrece a administradores la mayor flexibilidad; diversas políticas de seguridad se pueden implementar sobre la base de diversos rangos que anotan WBRS.