Contenido

Pregunta

¿El dispositivo de seguridad de la red de Cisco (WSA) proporciona la protección de Malware/del Spyware?

El dispositivo de seguridad de la red de Cisco (WSA) proporciona la defensa más completa del gateway de la industria contra el spyware y el malware basado en web. Esto incluye todo del adware (que causa la mayoría de los problemas de la posibilidad de entretenimiento y consume a los recursos de red significativos) a amenazas más malévolas tales como Trojans, objetos del ayudante de los secuestradores del navegador, del navegador, phishing, pharming, monitores de sistema, registradores de pulsaciones, gusanos, etc.

Los diferenciadores de claves de la solución acerca de la seguridad de la red de Cisco incluyen:

1. Un control de tráfico de la capa integrada 4 (L4) analiza todos los puertos en la velocidad de cable, detectando y bloqueando el malware y llamada a casa la actividad. Siguiendo los 65,535 puertos de red, el control de tráfico L4 para con eficacia el malware que las tentativas de desviar el puerto 80 y también previenen el P2P rogue y el IRC actividad relacionada.
2. Proceso de la Proxy-capa: El dispositivo de seguridad de la red de Cisco también incluye un funcionamiento de la extremadamente alta Web Proxy (Proxy Web), junto con el almacenamiento en memoria inmediata integrado y las capacidades contentas de la aceleración. Empleado el sistema operativo propietario de Cisco, AsyncOS, el dispositivo de Cisco Web Proxy (Proxy Web) puede soportar hasta 100,000 conexiones simultáneas tanto como los servidores proxy en lenguaje Unix más que tradicionales 10x. El ser a Web Proxy (Proxy Web) permite el examen contento completo en la capa de la aplicación - un requerimiento crítico hacia asegurar la exactitud contra el malware basado en web.
3. Los primeros filtros de la reputación Web de la industria proporcionan una capa externa potente de defensa. El ® Leveraging de SenderBase, los filtros de la reputación Web de Cisco analiza sobre diverso tráfico de la Web 50+ y los parámetros relacionados a la red para evaluar exactamente la fiabilidad URL. La Seguridad sofisticada que modela las técnicas se utiliza para pesar individualmente cada parámetro y para generar una sola calificación en una escala de -10 a +10. Las directivas configuradas administrador son dinámicamente aplicadas, sobre la base de las calificaciones de la reputación.
4. Exploración acelerada de la firma usando el motor Vectoring y que fluye dinámico (motor DV). A diferencia de las soluciones de la arquitectura de la herencia que confían en el ICAP y un despliegue del multi-cuadro para asegurar la exploración del malware, el WSA de Cisco ha introducido el motor DV para una solución integrada de la exploración del en-cuadro. Esta plataforma innovadora emplea el objeto sofisticado que analiza y vectoring las técnicas, junto con la exploración de la secuencia y el veredicto que ocultan, dando por resultado hasta un aumento de la producción de la exploración 10x sobre las soluciones ICAP-basadas de primera generación.

5. El sistema anti-Malware de Cisco del conducir de la industria leverages el motor DV y la firma múltiple teclea de Webroot para proporcionar el mejor de la protección de la raza contra la variedad más amplia de amenazas basadas en web. Estas amenazas pueden extenderse del adware, de los secuestradores del navegador, del phishing y de los ataques del pharming a amenazas más malévolas tales como monitores de los Trojans, de sistema y registradores de pulsaciones. WSA ofrece la base de datos más grande de la firma del malware de la industria en el gateway.