# Funciones de detección de ransomware de Cisco WSA y verificación de la integración de AMP

## Contenido

## Problema

Se ha realizado una consulta sobre si Cisco Secure Web Appliance (WSA) proporciona capacidades de firma o detección específicas para el ransomware Triple X. Esta pregunta también incluía una solicitud de aclaración sobre cómo comprobar si una integración entre la protección frente a malware avanzado (AMP) y Cisco Talos Threat Intelligence funcionaba correctamente en la plataforma WSA.

## Entorno

- Dispositivo Cisco Secure Web Appliance (WSA)
- Integración de protección frente a malware avanzado (AMP)
- Integración de inteligencia de amenazas de Cisco Talos
- Filtrado de URL y reputación web (WBRS)
- Motores de detección de malware (Webroot, McAfee, Sophos)
- Visibilidad y control de aplicaciones (AVC)

## Resolución

Cisco Secure Web Appliance no se basa en una única firma dedicada específicamente denominada Triple X Ransomware. En su lugar, WSA emplea una arquitectura de seguridad de

varios niveles que utiliza diversas técnicas de detección para identificar y bloquear las amenazas de ransomware, incluidas las variantes de ransomware Triple X.

## Métodos de detección de WSA

La plataforma WSA utiliza estas técnicas de detección para la protección frente a ransomware:

- Algoritmos de coincidencia de patrones
- Análisis heurístico
- Técnicas de emulación
- Protección frente a malware avanzado (AMP) integrada con Cisco Talos Threat Intelligence
- Filtrado de URL y reputación web (WBRS)
- Varios motores de análisis antimalware, incluidos Webroot, McAfee y Sophos
- Visibilidad y control de aplicaciones (AVC)

Estas funciones de detección se actualizan continuamente con nuevas reglas que se implementan cada pocos minutos para garantizar la protección frente a las amenazas emergentes.

## Verificación de la integración de AMP y Talos

Para confirmar que la integración entre la protección frente a malware avanzado (AMP) y Cisco Talos Threat Intelligence funciona correctamente en WSA, los administradores pueden revisar estos registros:

Paso 1: Revisar registros de acceso de WSA

Examine los registros de acceso del dispositivo WSA para comprobar que los veredictos de AMP se aplican a los archivos descargados y las solicitudes web.

Paso 2: Comprobar registros de AMP

Revise los registros de AMP para confirmar que se están procesando los resultados del análisis de malware y los datos de inteligencia de amenazas.

Paso 3: Verificar puntuaciones WBRS

Asegúrese de que las puntuaciones de Web Reputation (WBRS) se rellenan y se asocian a las solicitudes web de los registros.

Si los veredictos de AMP y las puntuaciones de WBRS se rellenan y aplican en los registros, esto indica que la integración de AMP y Talos funciona según lo esperado y proporciona decisiones basadas en inteligencia de amenazas en tiempo real.

## Causa

Se trataba de una solicitud informativa sobre las capacidades de detección de ransomware de los WSA, en lugar de un problema técnico que requiriera solución de problemas. La investigación surgió de la necesidad de comprender cómo WSA protege frente a variantes específicas de ransomware y de comprobar que las integraciones de inteligencia de amenazas funcionan correctamente.

## Contenido relacionado

- Características y ventajas de Cisco Secure Web Appliance
- Cisco Talos Threat Intelligence Services
- Ficha técnica de Cisco Secure Web Appliance
- Soporte técnico y descargas de Cisco

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).